

No. 25-__

IN THE
Supreme Court of the United States

DETRINA SOLOMON,

Petitioner,

v.

FLIPPS MEDIA, INC., DBA FITE, DBA FITE TV,

Respondent.

On Petition for Writ of Certiorari to the
United States Court of Appeals for the Second Circuit

PETITION FOR WRIT OF CERTIORARI

NICOMEDES S. HERRERA
HERRERA KENNEDY LLP
5072 Annunciation Circle
Suite 207
Ave Maria, FL 34142
(510) 422-4700

JASON HARROW
Counsel of Record
CHARLES GERSTEIN
GERSTEIN HARROW LLP
400 7th Street NW, Suite 304
Washington, DC 20004
jason@gerstein-harrow.com

CHRISTOPHER J. CORMIER
BURNS CHAREST LLP
4725 Wisconsin Ave. NW,
Suite 200
Washington, DC 20016
(202) 577-3977

(323) 744-5293
Counsel for Petitioner

QUESTION PRESENTED

The Video Privacy Protection Act forbids a “video tape service provider” from disclosing without consent “personally identifiable information,” which the Act defines to “include[] information which identifies a person as having requested or obtained specific video materials or services” 18 U.S.C. § 2710(a)(3), (b).

The question presented is whether information can be “personally identifiable” if it is “reasonably . . . foreseeable[]” to the person sending the information that it will be used to identify someone’s video choices, as the First Circuit held in *Yershov v. Gannett Satellite Info. Net., Inc.*, 820 F.3d 482, 486 (1st Cir. 2016), or whether information can be “personally identifiable” only if an “ordinary person” could use it to identify someone’s video choices, as the Second, Third, and Ninth Circuits have held, Pet. App. 19a; *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 290 (3d Cir. 2016); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 985 (9th Cir. 2017).

PARTIES TO THE PROCEEDING

Petitioner in this Court is Plaintiff-Appellant Detrina Solomon. Respondent in this Court is Defendant-Appellee Flipps Media, Incorporated, doing business (and referred to here) as FITE or FITE TV.

TABLE OF CONTENTS

	PAGE
QUESTION PRESENTED	i
PARTIES TO THE PROCEEDING	ii
TABLE OF CONTENTS	iii
TABLE OF AUTHORITIES	v
OPINIONS BELOW	1
JURISDICTION	1
STATUTE INVOLVED	1
INTRODUCTION	2
STATEMENT OF THE CASE	4
A. Statutory Background	4
B. Technological Background	7
C. This Case	8
D. Subsequent Developments	10
REASONS FOR GRANTING THE PETITION	11
I. The Circuits Are Split on The Meaning of “Personally Identifiable Information,” and That Issue Is Case-Dispositive	11
II. The Second Circuit’s Rule Is Incorrect and Divorced from the Statutory Text	15

III.	This Case Is an Ideal Vehicle to Resolve an Important Question.....	24
IV.	This Court Should Grant This Case And Hold <i>Salazar</i>	25
	CONCLUSION	28

APPENDIX

	APPENDIX A — OPINION OF THE U.S. COURT OF APPEALS FOR THE SECOND CIRCUIT	1a
	APPENDIX B — MEMORANDUM AND ORDER OF THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF NEW YORK.....	29a
	APPENDIX C — SECOND CIRCUIT ORDER DENYING REHEARING EN BANC.....	43a
	APPENDIX D — COMPLAINT.....	45a
	APPENDIX E — 18 U.S.C. § 2710.....	79a

TABLE OF AUTHORITIES

PAGE

CASES

<i>Bartnicki v. Vopper</i> , 532 U.S. 514 (2001).....	6
<i>Bostock v. Clayton County</i> , 590 U.S. 644 (2020)...	15, 20
<i>Carpenter v. United States</i> , 585 U.S. 296 (2018)	6
<i>Eichenberger v. ESPN, Inc.</i> , 876 F.3d 979 (9th Cir. 2017)	i, 3, 10, 12, 14, 16, 20, 21, 22
<i>Hughes v. Nat’l Football League</i> , No. 24-2656, 2025 WL 1720295 (2d Cir. June 20, 2025)..	3, 10, 24, 27
<i>In re Hulu Priv. Litig.</i> , No. C 11–03764 LB, 2014 WL 1724344 (N.D. Cal. Apr. 28, 2014).....	16
<i>In re Nickelodeon Consumer Priv. Litig.</i> , 827 F.3d 262 (3d Cir. 2016).....	i, 3, 5, 10, 12, 13, 14
<i>In re Vizio, Inc., Consumer Privacy Litigation</i> , 238 F. Supp. 3d 1204 (C.D. Cal. 2017).....	21
<i>Kurowski v. Rush Sys. for Health</i> , No. 22-CV-5380, 2023 WL 8544084 (N.D. Ill. Dec. 11, 2023)	8
<i>Lee v. Springer Nature Am., Inc.</i> , 769 F. Supp. 3d 234 (S.D.N.Y. 2025)	16
<i>Manza v. Pesi, Inc.</i> , No. 24-CV-690-JDP, 2025 WL 1445762 (W.D. Wis. May 20, 2025)...	11, 12, 14, 16, 17, 18, 21

<i>United States v. Archer-Daniels-Midland Co.</i> , 785 F.2d 206 (8th Cir. 1986)	19
<i>United States v. John Doe, Inc. I</i> , 481 U.S. 102 (1987)	19, 20
<i>Yershov v. Gannett Satellite Info. Net., Inc.</i> , 820 F.3d 482 (1st Cir. 2016)	i, 4, 10, 12, 13, 14, 16

STATUTES

18 U.S.C. § 2710	i
18 U.S.C. § 2710(a)(1)	5
18 U.S.C. § 2710(a)(3)	2, 5, 15
18 U.S.C. § 2710(a)(4)	5
18 U.S.C. § 2710(b)(1)	4, 15, 19
18 U.S.C. § 2710(b)(2)	2, 3, 5, 9, 24
Pub. L. 98–353 (H.R. 5174), 98 Stat. 333 (July 10, 1984)	18

RULES

Supreme Court Rule 10(a)	11
--------------------------------	----

OTHER AUTHORITIES

Anjali C. Das, WILSON ELSER, <i>Courts Continue to Grapple with VPPA Class Actions</i> , https://perma.cc/D5R3-2Q7A (June 16, 2025)	24
---	----

BLACK’S LAW DICTIONARY, <i>Disclose</i>	19
BLOCKBUSTER, <i>About Us</i> , https://bendblockbuster.com/	25
Br. in Opp., <i>Nat’l Basketball Ass’n v. Salazar</i> , No. 24-994 (June 30, 2025).....	10, 27
Br. of Nat’l Football League, <i>Nat’l Basketball Ass’n v. Salazar</i> , No. 24-994 (May 2, 2025)	8, 21, 24
CENTRAL TIBETAN ADMINISTRATION, BASELINE STUDY OF THE TIBETAN DIASPORA COMMUNITY OUTSIDE SOUTH ASIA (2020).....	23
CRYPTII, https://cryptii.com/pipes/caesar-cipher	19
D. Daniel Sokol & Feng Zhu, Essay, <i>Harming Competition and Consumers Under the Guise of Protecting Privacy: An Analysis of Apple’s iOS 14 Policy Updates</i> , 107 Cornell L. Rev. Online 94 (2022).....	24
GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949)	6
LOKKER, <i>Online Data Privacy Report: March 2024</i> (March 2024), https://lokker.com/online- data-privacy-report-march-2024/	8
MERRIAM-WEBSTER, <i>Information</i> , https://www. merriam-webster.com/dictionary/information	18
Michael Dolan, <i>The Bork Tapes</i> , WASH. CITY PAPER (Sept. 25–Oct. 1, 1987).....	2, 18

Pet. for Cert., <i>Nat’l Basketball Ass’n v. Salazar</i> , No. 24-994 (Mar. 14, 2025).....	26
Pet’r Reply, <i>Nat’l Basketball Ass’n v. Salazar</i> , No. 24-994 (July 16, 2025).....	11, 26
S. REP. No. 100-599, 2, 1988 U.S.C.C.A.N. 4342-12, 6, 22	
Supp. Br. of Resp. in <i>Nat’l Basketball Ass’n v. Salazar</i> , No. 24-994 (Aug. 13, 2025).....	26
SUPREME COURT OF THE UNITED STATES, CIRCUIT ASSIGNMENTS (Sept. 28, 2022).....	23

OPINIONS BELOW

The Second Circuit’s opinion affirming the district court’s grant of FITE’s motion to dismiss is reported at 136 F.4th 41 and reproduced at Pet. App. 1a–28a. The Second Circuit’s order denying Solomon’s petition for rehearing en banc is not reported and is reproduced at Pet. App. 43a–44a. The district court’s opinion dismissing Solomon’s complaint is not reported but is available at 2023 WL 6390055 and reproduced at Pet. App. 29a–42a.

JURISDICTION

The Second Circuit issued an order denying en banc review on July 24, 2025. Pet. App. 43a. This Court has jurisdiction under 28 U.S.C. § 1254(1).

STATUTE INVOLVED

The full text of the Video Privacy Protection Act (VPPA) is reproduced at Pet. App. 79a. It reads, in relevant part:

A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person.

* * *

[T]he term “personally identifiable information” includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.

INTRODUCTION

This petition asks the Court to resolve a clear, acknowledged, and case-dispositive circuit split about the meaning of the phrase “personally identifiable information” in the VPPA, a federal statute protecting Americans’ video-viewing choices from unauthorized disclosure.

In 1987, after President George H.W. Bush nominated Judge Robert Bork to serve on this Court, the Washington *City Paper* published a list of the videos he and his family rented from a local store. Michael Dolan, *The Bork Tapes*, WASH. CITY PAPER (Sept. 25–Oct. 1, 1987). In response, Congress passed the VPPA, which creates a cause of action against any “video tape service provider” who “knowingly discloses, to any person, . . . information which identifies a person as having requested or obtained specific video materials . . .” 18 U.S.C. § 2710(a)(3), (b)(2).

Since then, the technology Americans use to watch videos has changed and the problem Congress addressed has worsened. Congress was concerned in 1987 that because consumer activities are “all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what . . . sort of television programs they watch.” S. REP. No. 100-599, at 5–6, *as reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4352-6. We have reached that predicted future point. Today, online video providers use pieces of computer code called “pixels” to send their customers’ video-viewing history to large social media companies, who use that information to create a “profile of a person and tell what . . . sort of [videos] they watch.” *Id.*

The text of the law Congress passed straightforwardly forbids, without relevant qualification, disclosing

information that “identifies a person as having requested or obtained specific video materials” 18 U.S.C. § 2710(b)(1), (a)(3). And yet the Second, Third, and Ninth Circuits have taken it upon themselves to add a new clause to that sentence. These courts hold that “personally identifiable” information must not only “identify a person as having requested or obtained specific video materials,” but also must be such that a hypothetical “ordinary person” who comes into possession of the information could instantly use it to identify a person as having requested or obtained specific video materials. Pet. App. 19a; *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 290 (3d Cir. 2016); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 985 (9th Cir. 2017). By doing so, these courts create a clear, and acknowledged, split with the First Circuit. Pet. App. 19a (rejecting *Yershov v. Gannett Satellite Info. Net., Inc.*, 820 F.3d 482, 486 (1st Cir. 2016)); *see also Hughes v. Nat’l Football League*, No. 24-2656, 2025 WL 1720295, at *2 (2d Cir. June 20, 2025) (“*Solomon* effectively shut the door for Pixel-based VPPA claims.”).

There is a reason Congress did not add the “ordinary person” clause to the law. Under the “ordinary person” rule, the video clerk who inspired the Act’s passage by disclosing Judge Bork’s video-rental history to the *Washington City Paper* need only have used a simple code, or a foreign language, to fully subvert the function of the law with trivial ease. Because an “ordinary person” would not know the code or speak the language, but the *City Paper* reporter would, the clerk could send information to the *City Paper* enabling it to identify every video Judge Bork rented without sending any “personally identifiable information.” That cannot be, and is not, right. Instead, people “knowingly disclose” information that is “personally identifiable” when they send information to

someone who will use it to identify who watched what videos. *See Yershov*, 820 F.3d at 486.

This case presents an ideal opportunity for this Court to resolve this circuit split on an important legal issue. Because this case arises from the district court’s grant of a motion to dismiss, there is no dispute here that FITE disclosed information, without Solomon’s consent, that the recipient, Meta Platforms, Inc. (Facebook), could use to identify Solomon as having watched specific videos. And Solomon conceded below that any “ordinary person” reading the message FITE sent to Facebook would find it incomprehensible. *E.g.* Pet. App. 58a ¶ 53 (example code). Moreover, as internet technology makes it easier than ever for large tech companies to obtain more data about ordinary Americans, this Court should spell out when those disclosing such information may do so without fear of liability. Indeed, this interpretive issue determines whether a plaintiff has a viable VPPA action in any case involving online video viewing. The issue presented by this Petition is thus the most important issue to reach this Court regarding the meaning of any part of the VPPA.

This Court should grant the petition and vacate the judgment of the Second Circuit.

STATEMENT OF THE CASE

A. Statutory Background

The VPPA was enacted in 1987 in response to a video-store clerk telling the Washington *City Paper* which videos then–Supreme Court nominee Judge Robert Bork’s family had rented. Pet. App. 31a. Under the VPPA, a “video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person” 18 U.S.C. § 2710(b)(1). The statute

defines “video tape service provider” as “any person, engaged in the business of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials.” *Id.* § 2710(a)(4). It defines “consumer” as “any renter, purchaser, or subscriber of goods or services from a video tape service provider.” *Id.* § 2710(a)(1). And “[t]he term ‘personally identifiable information’” is defined to “include[] information which identifies a person as having requested or obtained specific video materials from a video tape service provider.” *Id.* § 2710(a)(3). As amended, the law allows disclosure of personally identifiable information “to any person with the informed, written consent (including through an electronic means using the Internet) of the consumer” so long as the consent is “in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer”; “is given at the time the disclosure is sought or is given in advance for a set period of time”; and “the video tape service provider has provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw on a case-by- case basis” *Id.* (b)(2) (cleaned up).

Although “[t]he classic example [of a VPPA violation] will always be a video clerk leaking an individual customer’s video rental history,” *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 290 (3d Cir. 2016), there is no question that Congress specifically understood the Act to apply to disclosures of online viewing information: Congress amended the Act in 2013 to allow consent to be given online, keeping in place the rest of the statute. *Id.* at 287–88. And the Act explicitly includes all “audio visual materials,” not just physical tapes. 18 U.S.C. § 2710(a)(4).

Moreover, the VPPA was drafted with the expansion of technology in mind. Congress was concerned that in a

technological era in which consumer activities are “all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what . . . sort of television programs they watch,” which members likened to “Big Brother.” S. REP. No. 100-599, at 6, *as reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4352-6 (referencing GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949)). The Senate also cited Supreme Court opinions in which the Court “warned of the danger that new technologies would chip away at traditional privacy safeguards” and of “the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks.” *Id.* at 4–5 (citations omitted).

Congress passed the VPPA shortly after it enacted the Stored Communications Act, and it codified both statutes alongside the Wiretap Act of 1968. Collectively, Congress passed these laws to prevent “egregious violations of privacy” that occur because “[t]echnology now permits millions of important and confidential conversations to occur through a vast system of electronic networks,” which puts Americans “in the uncomfortable position of not knowing who might have access to our personal and business e-mails, our medical and financial records, or our cordless and cellular telephone conversations.” *Bartnicki v. Vopper*, 532 U.S. 514, 541 (2001) (Rehnquist, C.J., dissenting).

This Court has never interpreted the VPPA, and it has been cited by a Justice of this Court only once. *Carpenter v. United States*, 585 U.S. 296, 381 & n.4 (2018) (Alito, J., dissenting) (citing VPPA as an example of “federal statutes impos[ing] . . . restrictions on private entities’ use or dissemination of information in their own records without conferring a property right on third parties”).

B. Technological Background

This case is about a technology called the Meta Pixel that Meta Platforms, Inc., formerly known (and referred to here) as Facebook, uses to collect data about Americans' interactions with websites. Facebook offers the Meta Pixel for free to website operators. *See* Pet. App. 55a ¶ 43. When a website with a Pixel installed gets visited, the Pixel, operating in the background, sends a message to Facebook about the visitor's interaction with the website. *See id.* The website operator can configure the pixel to specifically send certain information about the interaction, including the URL of the site, the visitor's clicking of certain buttons, or the text the visitor types while using the site. *E.g.*, Pet. App. 58a ¶ 53; 55a ¶ 43.

Facebook's business model requires that it be able to track users' activity and link it to known facts about those users. To do this, Facebook uses pieces of software called "cookies." A cookie is a small block of data placed on a website-visitor's computer or web browser when the visitor browses a website. *E.g.*, Pet. App. 56a–57a ¶ 50. Any time people visit a Facebook website, cookies are sent to their browsers by which Facebook can subsequently identify them if they return to any Facebook website. Pet. App. 63a ¶ 65.

People who have Facebook accounts are sent a cookie that will immediately link them to their personal accounts and that will link those accounts with their activity on any website with a Pixel installed. *Id.* This particular cookie is called a "c_user" cookie, which corresponds to users' Facebook IDs, which are unique numbers identifying their Facebook profiles. Pet. App. 59a ¶ 55. Although the transmissions that websites send to Facebook when users interact with Pixels are written in computer code, Pet. App. 62a–63a ¶ 64 (example code), anyone who sees a

user’s c_user cookies—which is in the transmission, *id.*—can identify the user’s Facebook page by typing “www.facebook.com/[c-user cookie]” into a browser with the user’s c_user cookie number, Pet. App. 61a ¶ 62.

Website operators use the Meta Pixel because it allows them to collect data on their users and because it allows them to use Facebook to help them advertise to their customers. *E.g.*, Pet. App. 57a ¶ 51. So long as website operators get their users’ consent, there is nothing wrong with this—indeed, as defense-side amici in a petition pending before this Court note, “shar[ing] data with Meta so that Meta c[an] serve more targeted advertisements to Facebook users...is common online, particularly for content providers that provide a significant amount of their content for free.” Br. of Nat’l Football League at 2, *Nat’l Basketball Ass’n v. Salazar*, No. 24-994 (May 2, 2025); *see also* LOKKER, *Online Data Privacy Report: March 2024* at 3 (March 2024), <https://lokker.com/online-data-privacy-report-march-2024/> (noting that nearly half of retail websites share data with social-media platforms). The problems arise where websites apply their ordinary data-sharing and consent-requesting practices to data that Congress has deemed especially sensitive. *E.g.*, *Kurowski v. Rush Sys. for Health*, No. 22-CV-5380, 2023 WL 8544084, at *3 (N.D. Ill. Dec. 11, 2023) (denying motion to dismiss Wiretap Act claim where plaintiff alleged that defendant shared personal health information with Facebook).

C. This Case

Respondent Flipps Media, Incorporated, doing business (and referred to here) as “FITE,” operates a website on which subscribers can view pre-recorded combat-sports videos. Pet. App. 46a ¶ 2; Pet. App. 53a ¶ 34. Petitioner Detrina Solomon watched videos on FITE, Pet.

App. 74a–75a ¶¶ 105–07, and every time she watched a video, FITE used a `c_user` cookie on her browser to send the title of that video to Facebook alongside her Facebook ID, Pet. App. 74a–75a ¶ 107. Facebook used this information to identify Solomon as having watched specific videos on FITE, Pet. App. 59a–60a ¶¶ 54–55, which is the reason FITE sent this information to Facebook, *id.* But there is no question that an ordinary person reading the text that FITE sent to Facebook—which is a string of computer code, not English—would find that text difficult to understand. *E.g.*, 62a–63a ¶ 64. Although FITE got Solomon’s general consent to “automatically record information that your device sends” and “use this information for advertising and other marketing purposes,” Pet. App. 56a ¶ 46, FITE did not get Solomon’s consent “in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer” as required by 18 U.S.C. § 2710(b)(2), Pet. App. 48a ¶ 9, and never said that it would send video titles to any third party, *see generally id.*

Solomon sued FITE in the Eastern District of New York alleging violations of the VPPA. Pet. App. 45a–78a (complaint). The district court (Azrack, J.) dismissed Solomon’s complaint, holding that the messages FITE sent to Facebook were not “personally identifiable information” because an “ordinary person” could not use them to identify Solomon as having watched videos. Pet. App. 29a–42a.

Solomon timely noticed an appeal to the Second Circuit. The panel (Raggi, Chin, and Nardini, JJ.), recognized a clear circuit split on the dispositive issue of how to read the phrase “personally identifiable information.” It noted that “[t]wo approaches have emerged”: the “reasonable foreseeability standard” and

the “ordinary person standard.” Pet. App. 13a. The court, following *Eichenberger*, 876 F.3d at 985, and *In re Nickelodeon*, 827 F.3d at 278, and rejecting *Yershov*, 820 F.3d at 486, adopted the “ordinary person” standard for personally identifiable information. Pet. App. 19a–24a. Although the court “acknowledge[d] that the[] words [of the statute] could also be read to encompass computer code and digital identifiers decipherable only by a technologically sophisticated third party”—as the First Circuit had concluded—it held that “they are more naturally read as referring to information that would permit an ordinary person to learn another individual’s video-watching history.” Pet. App. 20a–21. Because Solomon had not alleged that FITE had transmitted to Facebook information with which an ordinary person could identify her, the court affirmed the dismissal of her complaint. Pet. App. 24a–26a.

Solomon sought rehearing en banc, which the Second Circuit denied without reasoning. Pet. App. 43a–44a. This petition follows.

D. Subsequent Developments

Since *Solomon* was decided, both its impact on pending VPPA cases and its clear split from other courts have been recognized by the lower courts. Just weeks after the decision, the Second Circuit acknowledged that “*Solomon* effectively shut the door for Pixel-based VPPA claims.” *Hughes v. Nat’l Football League*, No. 24-2656, 2025 WL 1720295, at *2 (2d Cir. June 20, 2025). For this reason, the respondent in *National Basketball Association v. Salazar*, No. 24-994, called *Solomon* “an asteroid [to the VPPA] that renders the statute’s protections virtually extinct.” Br. in Opp. at 14, No. 24-994 (June 30, 2025).

But the VPPA is extinct only in the circuits that agree with the Second Circuit, and not all do. Recently, a federal district court in Wisconsin expressly disagreed with *Solomon* and denied a defendant’s motion to dismiss, reasoning that *Solomon* and the courts adopting an “ordinary person” test “identified little textual basis for the limitation they impose.” *Manza v. Pesi, Inc.*, No. 24-CV-690-JDP, 2025 WL 1445762, at *5 (W.D. Wis. May 20, 2025). Indeed, *both* parties in *Salazar* told this Court that *Solomon* involves an important circuit split. *Salazar* Br. in Opp. at 10 n.4 (“The Second Circuit acknowledged *Solomon* deepened an existing circuit split.”); *Salazar* Pet’r Reply at 2 (July 16, 2025) (“*Solomon* deepened a circuit split.”). This case-dispositive split will persist until this Court resolves it.

REASONS FOR GRANTING THE PETITION

This Court should grant this petition because the circuits are split on the meaning of “personally identifiable information”; that issue is case-dispositive in the many VPPA actions filed regarding online videos; three of the circuits have wrongly departed from the statutory definition of the relevant phrase; and this case presents an ideal vehicle to resolve this important question. This case thus meets this Court’s stated requirements for certiorari. *See* Supreme Court Rule 10(a).

I. The Circuits Are Split on The Meaning of “Personally Identifiable Information,” and That Issue Is Case-Dispositive

The circuit courts have read the VPPA’s definition of “personally identifiable information” in two ways. The “reasonable foreseeability standard,” adopted by the First Circuit, holds that information qualifies as “personally identifiable” if it is “reasonably and foreseeably likely to

reveal which . . . videos [someone] has obtained.” *Yershov*, 820 F.3d at 486; *see also Manza*, 2025 WL at 1445762 at *9 (recognizing circuit split, agreeing with *Yershov*, and holding that this standard is consistent with Seventh Circuit precedent). The “ordinary person” standard, adopted by the Second, Third, and Ninth Circuits, holds that information qualifies as “personally identifiable” only if it “readily permit[s] an ordinary person to identify a specific individual’s video-watching behavior.” *Eichenberger*, 876 F.3d at 985 (quoting *Nickelodeon*, 827 F.3d at 267); *Pet. App.* 20a.

In *Nickelodeon*, the Third Circuit considered whether the owner of a website offering children’s videos violated the VPPA by disclosing to Google information linking video titles to three pieces of information about Nickelodeon users: (a) “a user’s IP address,” which is “a number assigned to each device that is connected to the Internet that permits computer-specific online tracking,” 827 F.3d at 281 (quotation omitted); (b) “a user’s browser and operating system settings, which comprise a so-called ‘browser fingerprint,’” *id.* at 281–82; and (c) the computing device’s “unique device identifier,” *id.* at 282. The Third Circuit held that even though *Google* could use that information to “track the same computer across time,” that information was not “personally identifiable” because “[t]o an average person, an IP address or a digital code in a cookie file would likely be of little help in trying to identify an actual person.” *Id.* at 283.

In *Eichenberger*, the Ninth Circuit considered whether ESPN violated the VPPA when it “knowingly disclosed to . . . Adobe Analytics: (1) Plaintiff’s . . . device serial number and (2) the identity of the video that he watched.” 876 F.3d at 981. The Ninth Circuit explained that “[t]wo circuits have considered that question in

similar cases,” *id.* (citing *Nickelodeon*, 827 F.3d at 281, and *Yershov*, 820 F.3d at 484), “and each has articulated a different standard,” *id.* The court then “adopt[ed] the Third Circuit’s ‘ordinary person’ standard” and held that the information ESPN disclosed to Adobe was not “personally identifiable” because an ordinary person would not be able to use it to identify the viewer. *Id.* at 985.

By contrast, the First Circuit did not add any extra-textual requirement and thus reached the opposite result. In *Yershov*, it considered whether a website operator violated the VPPA by disclosing to Adobe, an internet-services company, “(1) the title of the video viewed, (2) the GPS coordinates of the device at the time the video was viewed, and (3) certain identifiers associated with the user’s device.” 820 F.3d at 484. The First Circuit answered in the affirmative. It used the metaphor of “a football referee announc[ing] a violation by ‘No. 12 on the offense,’” which is incomprehensible to the ordinary listener but “everyone with a game program knows the name of the player who was flagged.” *Id.* at 486. So too was the information sent to Adobe “personally identifiable” because when the website “makes such a disclosure to Adobe, it knows that Adobe has the ‘game program,’ so to speak.” *Id.* at 486.

Most recently, in this case, the Second Circuit held that FITE did not violate the VPPA when it sent to Facebook Solomon’s unique Facebook ID matched with computer code that Facebook could read as the title of the videos Solomon watched but that an ordinary person could not understand. Pet. App. 19a. The Second Circuit adopted the Third and Ninth Circuits’ tests, holding that the specific transmission in *Solomon* was insufficient because “the Complaint [does not] plausibly allege that an ordinary person could identify Solomon through her [Facebook

identification number].” Pet. App. 25a. But then the Second Circuit took the test a step further, holding that computer code can *never* be “personally identifiable” because “[i]t is implausible that an ordinary person would [read it] and [understand] it” Pet. App. 25a (“The exemplar depicts some twenty-nine lines of computer code, and . . . [t]he words of the title . . . are interspersed with many characters, numbers, and letters. It is implausible that an ordinary person would look at the phrase ‘title% 22% 3A% 22-% E2% 96% B7% 20The% 20Roast% 20of% - 20Ric% 20Flair’ . . . and understand it to be a video title.”).

The circuits are, thus, intractably split on the meaning of “personally identifiable information.” They acknowledge this: the Ninth and Second Circuits explicitly “decline[d] to adopt *Yershov*’s reasonable foreseeability standard.” Pet. App. 23a (citing *Yershov*, 820 F.3d at 486; *In re Nickelodeon*, 827 F.3d at 290; *Eichenberger*, 876 F.3d at 985). And indeed, there is no question that *Solomon* is fully inconsistent with *Yershov* because *Solomon* held that computer code of *any* kind cannot *ever* be “personally identifiable,” which would necessarily mean that *Yershov*’s result is wrong. Pet. App. 24a–26a.

The interpretive question here is case dispositive. If the Second Circuit is correct, then the online sharing of video viewing information via computer code will never give rise to a cause of action. The Second Circuit made this explicit in another case decided soon after *Solomon* when it said that “*Solomon* effectively shut the door for Pixel-based VPPA claims.” 2025 WL 1720295, at *2. Yet “Pixel-based VPPA claims” remain viable in the First Circuit and in circuits that have not yet weighed in on the issue but where district courts disagree with *Solomon*. See *Manza*, No. 24-CV-690-JDP, 2025 WL 1445762, at *5 (disagreeing

with *Solomon* and permitting a Pixel-based VPPA claim to proceed). Only this Court can resolve this split and determine whether VPPA claims alleging online information sharing may proceed.

II. The Second Circuit’s Rule Is Incorrect and Divorced from the Statutory Text

This Court’s interpretation of a statute always begins, and in this case ends, with the text. *See Bostock v. Clayton County*, 590 U.S. 644, 653 (2020) (“Only the written word is the law.”). Here, Congress’s text reads, in relevant part:

A videotape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person.

* * *

[T]he term “personally identifiable information” includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.

18 U.S.C. § 2710(b)(1), (a)(3).

The Second Circuit’s “ordinary person” standard departs from the plain meaning of the phrase “personally identifiable information.” And, even if there were any ambiguity in the plain meaning of the phrase, the standard does not make practical sense.

1. All courts to have considered the meaning of “personally identifiable information” begin with the shared premise that “[personally identifiable information] includes more than just information that, on its face, shows that a particular individual obtained a particular video.” *Manza*, 2025 WL 1445762 at *4; Pet. App. 19a; *Eichenberger*, 876 F.3d at 984; *Yershov*, 820 F.3d at 486; *Lee v. Springer Nature Am., Inc.*, 769 F. Supp. 3d 234, 254–55 (S.D.N.Y. 2025)). That makes sense: many people have the same name, and so “[a] combination of characteristics, such as an address and a physical description, may be as or more descriptive of an individual than a name.” *Lee*, 769 F. Supp. 3d at 255.

From that premise, the Second Circuit acknowledges that “the plain language of the VPPA [is] broad enough to ‘encompass computer code and digital identifiers,’” *Manza*, 2025 WL 1445762 at *5 (quoting *Solomon*, 136 F.4th at 52), and of course it is: “One could not skirt liability under the VPPA, for example, by disclosing a unique identifier and a correlated look-up table.” *In re Hulu Priv. Litig.*, No. C 11–03764 LB, 2014 WL 1724344, at *11 (N.D. Cal. Apr. 28, 2014). In any ordinary interpretation of the word “identify,” referees “identify” who committed a foul when they “announce[] a violation by ‘No. 12 on the offense’ [because] everyone with a game program knows the name of the player who was flagged.” *Yershov*, 820 F.3d at 486.

But even though the Second Circuit acknowledged that “personally identifiable information” could be read to include the information shared by FITE, it concluded that the statute is “more naturally read as referring to information that would permit an ordinary person to learn another individual’s video-watching history.” Pet. App. 21a.

Although the court “[did not] explain[] why” it reached its counter-textual conclusion, *Manza*, 2025 WL 1445762, at *5, it appears to have done so by confusing whether a piece of information is “identifiable” of a specific person’s relationship to a specific video with whether that piece of information has to be decoded or translated before it can be understood. But those are different concepts, and exempting encoded information from counting as “personally identifiable” is atextual and leads to absurd results.

For example, imagine that a video clerk reveals that a recent customer was an Oscar winner for Best Actress. That single piece of information is insufficient to “identify” the customer: there have been 80 such winners, so the recipient of the information cannot tell who it is. But if the same video clerk intends to identify two-time Best Actress winner Meryl Streep as the customer in question, then encoding the message by saying “it was the person named at <<https://www.imdb.com/name/nm0000658/>>” would identify Ms. Streep just as uniquely as saying her name or “the Oscar winner who won Best Actress for *Sophie’s Choice*.” Of course, no ordinary person could look at the website URL above and instantly say “that must be Meryl Streep.” But putting the URL into any web browser leads to Ms. Streep’s IMDB page. And although not all “ordinary” Americans know that Streep won the Oscar for her role in *Sophie’s Choice*, any person could use that information to consult a reliable source and identify Ms. Streep.

The Second Circuit’s opinion creates an unwarranted and atextual distinction among these types of information, all of which are personally identifying. It concluded, without any defensible explanation, that “identifiable” means facially comprehensible to a hypothetical ordinary

person who, by mere assumption, has no ability to translate, decode, or consult any other source. It then reasoned that FITE’s disclosure to Facebook was not “personally identifiable” because “[i]t is implausible that an ordinary person would look at the phrase ‘title% 22% 3A% 22-% E2% 96% B7% 20The% 20Roast% 20of% 20Ric% 20Flair’ . . . and understand it to be a video title” and because “[t]he Complaint is devoid of any details about *how* an ordinary person would use a [Facebook c_user number] to identify Solomon.” Pet App. 24a–25a (emphasis in original). Accordingly, as a district court critical of *Solomon* recognized, “[u]nder [the “ordinary person” test], a video tape service provider is free to disclose a customer’s video purchases . . . so long as the provider uses a ‘code’ that an ‘ordinary person’ could not decipher.” *Manza*, 2025 WL 1445762 *8.

That result ignores statutory text, and makes little sense too. The phrase “personally identifiable information” means what it says. It means (1) “information,” which is “a signal or character (as in a communication system or computer) representing data,” *Information*, MERRIAM-WEBSTER, <https://www.merriam-webster.com/dictionary/information> (2) that is capable (as indicated by “identifiable”) of (3) “identify[ing]” a “person.” A message reading “some D.C. Circuit judge rented *The Man Who Knew Too Much* in 1986” is not “personally identifiable information” with respect to Judge Robert Bork because to *any* recipient the message links thirteen people to that film. See Pub. L. 98–353 (H.R. 5174), 98 Stat. 333 (July 10, 1984) (establishing thirteenth D.C. Circuit judgeship); see also Dolan, *supra* (explaining that Judge Bork rented, among many other films, Alfred Hitchcock’s 1956 thriller *The Man Who Knew Too Much*). By contrast, the encrypted message

reading “*Vsfivx Fsvo, Xli Qer Als Oria Xss Qygl; use Caesar’s cipher, shift four*” immediately links Robert Bork to *The Man Who Knew Too Much*, even though it must go through a simple decoding process to be comprehensible. *E.g.*, CRYPTII, <https://cryptii.com/pipes/caesar-cipher> (enter “Robert Bork, The Man Who Knew Too Much” and select “shift 4, a→e) (last accessed Aug. 20, 2025). That encrypted message uniquely “identifies” Judge Bork, though of course an “ordinary person” must take the additional step of employing Caesar’s cipher to understand that information.

What’s more, the Second Circuit’s “ordinary person” standard ignores the meaning of the word “disclose.” The law forbids “disclos[ing], to any person, personally identifiable information.” 18 U.S.C. § 2710(b)(1). Any VPPA violation must therefore involve at least two people: the sender, a “videotape service provider” who “knowingly discloses” “information,” and “any [other] person” the information is sent “to.” *Id.* The word “disclose” necessarily requires a recipient who can understand a piece of information. *See United States v. John Doe, Inc. I*, 481 U.S. 102, 109 (1987) (“For there to be a disclosure, grand jury matters must be disclosed to *someone*.” (quoting *United States v. Archer-Daniels-Midland Co.*, 785 F.2d 206, 212 (8th Cir. 1986) (emphasis in *Archer-Daniels-Midland*)); *Disclose*, BLACK’S LAW DICTIONARY, (“To make (something) *known* . . .” (emphasis added)). The “disclos[ure]” of “personally identifiable information” “to any person” thus necessarily depends on there being a *person* who *understands* that information; one cannot “disclose” information to a potato.

A further mistake in adopting the “ordinary person” standard thus lies in the conclusion that “18 U.S.C. § 2710(b) . . . views disclosure from the perspective of the

disclosing party...[and], [a]s a result, ‘personally identifiable information’ must have the same meaning without regard to its recipient’s capabilities.” *Eichenberger*, 876 F.3d at 985; *see also* Pet. App. 21a (“It does not make sense that a video tape service provider’s liability would turn on circumstances outside of its control and the level of sophistication of the third party.” (citing *Eichenberger*, 876 F.3d at 985)). But “disclosure” happens only if someone receives a piece of information, *John Doe, Inc. I*, 481 U.S. at 109, an inquiry that necessarily depends on “the level of sophistication” of the recipient, *contra, e.g., Eichenberger*, 876 F.3d at 985.

The “ordinary person” standard is wrong, then, because it misreads “identifiable” to mean something like “comprehensible to most people without translation or decoding,” when that is not a requirement in the text. That standard also writes out the plain meaning of the word “disclose” by requiring “personally identifiable information” to be defined without any reference to who is receiving the information.

2. The above is sufficient to show the Second Circuit’s rule is wrong, for “[w]hen the express terms of a statute give us one answer and extratextual considerations suggest another, it’s no contest.” *Bostock*, 590 U.S. at 652. But all reasonable extratextual considerations suggest that the Second Circuit’s rule is wrong besides.

Congress passed the VPPA with the very specific context of Judge Bork’s experience explicitly in mind. “Applying th[e] logic [of the Second Circuit’s rule] to the Judge Bork case would mean that the video store would be free to disclose Judge Bork’s rental history so long as the store matched that history with an ID number provided by the reporter instead of with the judge’s name,” or if the reporter “use[d] a ‘code’ that an ‘ordinary person’ could

not decipher.” *Manza*, 2025 WL 1445762, at *8. That view “makes no sense.” *Id.*

The purpose of the VPPA is to prevent video tape service providers from disclosing information that allows third parties to identify a customer’s video purchases. That purpose is not served by allowing video tape service providers and third parties to knowingly evade the statute by disclosing a customer’s identity with a number unknown to the “ordinary person” but known by the recipient.

Id. Indeed the rule “would suggest that even Social Security numbers are not [personally identifiable information] because an ‘ordinary person’ might not be able to use the number to identify an individual without significant effort.” *Id.* (citing *In re Vizio, Inc., Consumer Privacy Litigation*, 238 F. Supp. 3d 1204, 1224–25 (C.D. Cal. 2017)). The statute’s only conceivable purpose is undermined—indeed fully eliminated—by the Second Circuit’s rule: Under the Second Circuit’s rule, a video tape service provider may reveal *anything it wants* to *anyone it wants* so long as it uses a simple code. *Id.* That cannot be right.

Some courts have reasoned, and some VPPA defendants have complained, that the “ordinary person” standard is somehow necessary because Congress could not have imagined, and was thus not concerned with, internet video viewing. *E.g.*, *Eichenberger*, 876 F.3d at 985; Br. of National Football League in *Salazar*, *supra*, at 2–3 (“[T]he VPPA [is] . . . a statute designed to protect the patrons of brick-and-mortar video stores from public disclosure of their video rental histories.”). Besides wrongly inserting extratextual considerations, this is

incorrect for at least two other reasons. First, there is no relevant difference between a physical video store sharing someone’s video-viewing history with a media company and an online video provider sharing someone’s video-viewing history with a social-media company. Sure, Judge Bork was a prominent public figure and Solomon is not. But the Second Circuit’s rule permits video providers to share the viewing history of celebrities, elected officials, and the entire federal judiciary with the owners of Facebook, X (née Twitter), and Snapchat; and it is easy to imagine those people publishing that information on their platforms for their own political and business purposes. Second, Congress was indeed *explicitly* concerned with the aggregation of large amounts of video-viewing information “lodged together in computers.” S. REP. 599, 2, 1988 U.S.C.C.A.N. 4342-1, 4342-1 at 5–6. That is what is at issue here.

Practically speaking, the “ordinary person” standard is nearly impossible to apply and regardless does not prevent against any supposed unfairness that video tape service providers may worry about. The Second Circuit was “concerned about the potential breadth of the VPPA and unfairness to video tape service providers . . . [because] liability under the VPPA should not turn on ‘circumstances outside a videotape service provider’s control,’” and it reasoned that “an ‘ordinary person’ standard ‘better informs’ video tape service providers about their obligations under the act.” *Manza*, at *7 (citing *Pet. App. 21a*); *Eichenberger*, 876 F.3d at 985). But there is no reason to believe that the “level of sophistication” of the person to whom disclosure is made is “outside of [the service provider’s] control.” *Id.* A videotape service provider who sends encrypted information to someone the provider incorrectly believes to be incapable of reading it

has not *knowingly* disclosed information; but a provider who sends encrypted information that an ordinary person could not read to someone the provider knows can read it has knowingly disclosed information. The person to whom someone knowingly sends a message is, therefore, very much within the sender’s “control.”

Meanwhile, it is fatally unclear what an “ordinary person” knows and does not. Does an “ordinary person” know, for example, who the Circuit Justice of the Second Circuit is, such that the phrase “the Circuit Justice of the Second Circuit rented *The Man Who Knew Too Much*” would identify the Honorable Sonia Sotomayor, Associate Justice of this Court? *See* SUPREME COURT OF THE UNITED STATES, CIRCUIT ASSIGNMENTS (Sept. 28, 2022). Would an “ordinary person” know how to look that information up, or would that person think that “circuit justice” is a reference to electronic, not judicial, circuits? Would a message in Tibetan be comprehensible to an “ordinary person” in the United States? Probably not—but what about to someone in Queens, New York, home to the largest Tibetan-speaking population in the United States? *See, e.g.,* CENTRAL TIBETAN ADMINISTRATION, BASELINE STUDY OF THE TIBETAN DIASPORA COMMUNITY OUTSIDE SOUTH ASIA 45 (2020). On the Second Circuit’s logic, a videotape service provider’s liability may depend on how common or uncommon certain referential knowledge is, which may be well beyond the service provider’s ability to predict. *Contra* Pet. App. 21a. That makes little sense.

Finally, there is no merit to the critique that holding online video providers liable for knowingly disclosing their customers’ video records to third parties would “force content providers” to abandon “the free apps and services that [targeted] advertising makes possible,” as a recent

defense-side amicus brief put it. Br. of National Football League in *Salazar, supra* at 2 (quoting D. Daniel Sokol & Feng Zhu, Essay, *Harming Competition and Consumers Under the Guise of Protecting Privacy: An Analysis of Apple's iOS 14 Policy Updates*, 107 Cornell L. Rev. Online 94, 100 (2022)) (alteration in Br. of National Football League). Anyone who wants to use tracking pixels to target customers with advertisements may do so by simply seeking their specific consent. 18 U.S.C. § 2710(b)(2). Indeed providers often explain their tracking practices in privacy policies at the bottom of their sites, *e.g.* Pet. App. 55–56a ¶ 45; the VPPA requires only that they treat video records, which Congress deemed to be especially sensitive, with slightly more care.

III. This Case Is an Ideal Vehicle to Resolve an Important Question

Further, this Court should grant this petition because the resolution of the question presented is case-dispositive in almost every VPPA case involving online video viewing, and the procedural posture and record are ideal for clean resolution.

The Second Circuit has already recognized that “*Solomon* effectively shut the door for Pixel-based VPPA claims” in the Second Circuit. *Hughes*, 2025 WL 1720295, at *2. But nationally, VPPA cases are common and increasing, with one source estimating that “[i]n 2024, . . . 250 VPPA class actions were filed against companies—nearly double the number of similar suits filed in 2023.” Anjali C. Das, WILSON ELSER, *Courts Continue to Grapple with VPPA Class Actions* (June 16, 2025), <https://perma.cc/D5R3-2Q7A>. Without this Court’s intervention, these hundreds of cases will have different outcomes depending only on where they are filed. Moreover, because much more video watching currently

happens online and not via brick-and-mortar video rental stores,¹ claims under the VPPA for unauthorized sharing of video viewing information will be essentially foreclosed for the foreseeable future under the Second Circuit’s rule.

This case cleanly presents the issue. There is no dispute that Solomon plausibly pleaded that she had a Facebook account and that there was “information transmitted by FITE to Facebook via the Pixel[],” Pet. App. 24a, which included “some twenty-nine lines of computer code” in which one could see “the . . . words of the [video] title[s]” that Solomon watched “interspersed with many characters, numbers, and letters” alongside her “Facebook ID,” *id.* The only question is whether, accepting those allegations as true, that information is “personally identifiable” under the VPPA. The Second Circuit held that it was not, and that was the sole legal basis for the Second Circuit’s affirming the dismissal on the merits; it explicitly declined to address any other questions given that holding. Pet. App. 26a & n.15. The question is purely legal and cleanly presented on this minimal record. Accordingly, if this Court disagrees with the Second Circuit—as it should—then the case would be remanded for further proceedings, with Solomon having plausibly alleged the transmission of personally identifiable information.

IV. This Court Should Grant This Case And Hold *Salazar*

Finally, as mentioned above, the petition in *National Basketball Ass’n v. Salazar*, No. 24-994, also involves the VPPA. But this case should take precedence, because the

¹ As of the date of this petition, only one Blockbuster Video store remains. See BLOCKBUSTER, *About Us*, <https://bendblockbuster.com/> (last accessed Aug. 20, 2025).

issue from this petition is dispositive in any case involving video viewing online, which is essentially every VPPA case in the modern era. The primary statutory issue in *Salazar*, by contrast, applies only in a subset of VPPA cases. Accordingly, Petitioner respectfully recommends that this Court consider the two petitions together, grant this petition, and hold *Salazar* pending disposition of this case.

The *Salazar* petition presents two questions: the pleading standard for alleging injury under Article III, and the meaning of “subscriber” to a “video tape service provider,” which is at issue in certain VPPA cases and not others. *See* Pet. for Cert. at i, *National Basketball Ass’n v. Salazar*, No. 24-994 (Mar. 14, 2025). On the standing issue, there is no circuit split—every court to have considered the issue has held that the unauthorized disclosure of the protected information at issue gives rise to Article III standing. *See* Supp. Br. of Resp. at 1 in *National Basketball Ass’n v. Salazar*, No. 24-994 (Aug. 13, 2025).

Meanwhile, the *Salazar* petition acknowledges that the split on the question of who counts as a “subscriber” to a video tape service provider under the VPPA applies in only a subset of cases. In particular, the *Salazar* Petitioner argues that the Court should grant cert. in that case because the appellate courts “have split over whether the VPPA covers consumers, like Salazar, who rent, purchase, or subscribe to a video tape service provider’s non-audiovisual goods and services.” *Salazar* Pet’r Reply 3. But that, by definition, is only a subset of VPPA plaintiffs; in some cases, it is clear that a plaintiff is a subscriber to a provider’s audiovisual goods and services. Here, for instance, there is no dispute that the plaintiff was a subscriber to the audiovisual product that the defendant offered. Pet. App. 9a (noting that “Solomon was a

Facebook user and subscriber of FITE’s TrillerVerzPass digital video streaming service”). The *Salazar* split thus has no impact on this case and many others like this one. By contrast, the definition of “personally identifiable information” applies in *Salazar*, *Solomon*, and any other VPPA case involving online video viewing—which is basically every case under the statute.

For this reason, the Respondent in *Salazar* told this Court that “[u]nless the Second Circuit reconsiders *Solomon* . . . , it is difficult to see how [the] claim [in *Salazar*] can survive.” *Salazar* Br. in Opp. 15. And the Petitioner in *Salazar* also acknowledged that, given *Solomon*, there is a “possibility that *Salazar* might eventually lose on another ground.” *Salazar* Pet’r Reply 8. The *Salazar* Petitioner nonetheless argued that this Court should not hold that petition pending *Solomon* because “[n]either the district court nor the Second Circuit has decided whether *Salazar* can win despite *Solomon*,” *id.*, but that is not accurate: as the Second Circuit has since said in *Hughes*, *Solomon* “shut the door for Pixel-based VPPA claims.” *Hughes*, 2025 WL 1720295, at *2. That would mean *Salazar* has no claim. The issue presented by this petition is thus case-dispositive in all online VPPA cases. It should be heard first by this Court.

Accordingly, in terms of efficiently managing the two cases, it makes sense for this Court to grant this petition first to determine if Pixel-based VPPA claims are viable at all. If the claims are viable (and they should be), this Court can then determine if either of the issues in *Salazar* require this Court’s additional attention. But if the door is closed to Pixel-based VPPA cases because there is no disclosure of “personally identifiable information,” then this Court would have no need to address the merits of either of the questions presented by *Salazar* and would

likely be able dispose of it summarily, either by denying certiorari or granting, vacating, and remanding.

CONCLUSION

The petition for certiorari should be granted.

Respectfully submitted,

NICOMEDES S. HERRERA
HERRERA KENNEDY LLP
5072 Annunciation Circle
Suite 207
Ave Maria, FL 34142
(510) 422-4700

CHRISTOPHER J. CORMIER
BURNS CHAREST LLP
4725 Wisconsin Ave. NW,
Suite 200
Washington, DC 20016
(202) 577-3977

JASON HARROW
Counsel of Record
CHARLES GERSTEIN
GERSTEIN HARROW LLP
400 7th Street NW,
Suite 304
Washington, DC 20004
jason@gerstein-harrow.com
(323) 744-5293

Counsel for Petitioner

AUGUST 2025