FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

CHAD EICHENBERGER, *Plaintiff-Appellant*, v. ESPN, INC., a Delaware corporation, *Defendant-Appellee.*	No. 15-35449 D.C. No. 2:14-cv-00463-TSZ OPINION

Appeal from the United States District Court
for the Western District of Washington
Thomas S. Zilly, Senior District Judge, Presiding

Argued and Submitted October 3, 2017
Pasadena, California

Filed November 29, 2017

Before: Susan P. Graber, Mary H. Murguia,
and Morgan Christen, Circuit Judges.

Opinion by Judge Graber

SUMMARY*

Video Privacy Protection Act

The panel affirmed the district court's dismissal under Fed. R. Civ. 12(b)(6) of an action alleging that ESPN, Inc. disclosed the plaintiff's "personally identifiable information" in violation of the Video Privacy Protection Act of 1998 by giving a third party, Adobe Analytics, the plaintiff's Roku device serial number and by identifying videos he watched through the WatchESPN application.

The panel rejected ESPN's contention that the plaintiff lacked standing. The panel held that every disclosure of an individual's "personally identifiable information" and video-viewing history offends the interests that the statute protects, and that the plaintiff need not allege any further harm to have standing.

The panel held that "personally identifiable information" under the statute means only that information that would readily permit an ordinary person to identify a specific individual's video-watching behavior. Applying that definition here, the panel concluded that an ordinary person could not use the information that ESPN allegedly disclosed to identify an individual, because the allegedly-disclosed information cannot identify an individual unless it is combined with other data in Adobe's possession—data that ESPN never disclosed and apparently never even possessed.

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

The panel concluded that the plaintiff therefore failed to state a claim under Rule 12(b)(6).

COUNSEL

John A. Lawson (argued), Roger Perlstadt, and Ryan D. Andrews, Edelson PC, Chicago, Illinois, for Plaintiff-Appellant.

Daniel P. Collins (argued) and Glenn D. Pomerantz, Munger Tolles & Olson LLP, Los Angeles, California; Bryan H. Heckenlively, Jonathan H. Blavin, and Rosemarie T. Ring, Munger Tolles & Olson LLP, San Francisco, California; Ana-Maria Popp, Cairncross & Hempelmann P.C., Seattle, Washington; for Defendant-Appellee.

Marc Rotenerg and Alan Butler, Washington, D.C., as and for Amicus Curiae Electronic Privacy Information Center.

OPINION

GRABER, Circuit Judge:

Plaintiff Chad Eichenberger alleges that Defendant ESPN, Inc. violated the Video Privacy Protection Act of 1988 ("VPPA"), which bars a "video tape service provider" from knowingly disclosing "personally identifiable information concerning any consumer of such provider." 18 U.S.C. § 2710(b)(1). The district court dismissed the action under Federal Rule of Civil Procedure 12(b)(6) on the ground that the operative complaint fails to state a claim that the

information disclosed was "personally identifiable information" within the meaning of the VPPA. We affirm.

FACTUAL AND PROCEDURAL HISTORY

We accept as true all factual allegations in the operative complaint, and we construe them in the light most favorable to Plaintiff as the non-moving party. *Mollett v. Netflix, Inc.*, 795 F.3d 1062, 1065 (9th Cir. 2015).

Defendant produces sports-related news and entertainment programming. Though best known for its television channel, Defendant also offers access to video content through an application called the "WatchESPN Channel," which is available on the Roku digital streaming device. Roku allows users to view videos and other content on their televisions by means of Internet streaming.

Plaintiff downloaded the WatchESPN Channel on his Roku device and used it to watch sports-related news and events. He did not consent to Defendant's sharing his information with a third party. But every time Plaintiff watched a video, Defendant knowingly disclosed to a third party, Adobe Analytics: (1) Plaintiff's Roku device serial number and (2) the identity of the video that he watched.

Adobe uses the information obtained from Defendant to identify specific consumers by connecting that information "with existing data already in Adobe's profile of th[ose] individual[s]." Adobe obtains the additional information—such as "email addresses, account information, or Facebook profile information, including photos and usernames"—from sources other than Defendant. Adobe gives the resulting data back to Defendant in an aggregated

form; Defendant in turn provides advertisers with aggregated information about its users' demographics.

In this action, Plaintiff alleges that Adobe used the foregoing process to identify him as having watched specific videos. He argues that Defendant disclosed his "personally identifiable information" by giving Adobe his Roku device serial number and identifying the videos that he watched, because Defendant knew that Adobe could and would use that information to identify him. The district court dismissed the action on the ground that the information that Defendant disclosed did not constitute "personally identifiable information" within the meaning of the VPPA. Plaintiff timely appeals.

STANDARD OF REVIEW

We review de novo the district court's decision to grant a motion to dismiss a claim under Rule 12(b)(6). *Mollett*, 795 F.3d at 1065. To survive a motion to dismiss, the claim must be plausible on its face. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). We must uphold a district court's decision to dismiss *either* if a cognizable legal theory is absent *or* if the facts alleged fail to suffice under a cognizable claim. *Mollett*, 795 F.3d at 1065.

DISCUSSION

A. *Standing*

Defendant first argues that Plaintiff lacks Article III standing because he has not alleged a concrete harm as required by *Spokeo, Inc. v. Robins* (*Spokeo I*), 136 S. Ct. 1540 (2016). We disagree.

To have Article III standing, a plaintiff must have suffered an injury in fact that is (1) concrete and particularized, (2) traceable to the defendant, and (3) redressable by judicial order. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992). For an injury to be concrete, it "must be '*de facto*'; that is, it must actually exist." *Spokeo I*, 136 S. Ct. at 1548. Nevertheless, an intangible harm may qualify as an injury in fact. *Id.* at 1549. In determining whether an intangible injury is sufficiently concrete, "both history and the judgment of Congress play important roles." *Id.*

In *Spokeo I*, the Supreme Court addressed whether a violation of procedural requirements imposed by the Fair Credit Reporting Act ("FCRA"), alone, could constitute an injury in fact sufficient to confer standing. *Id.* at 1549. There, the plaintiff (Robins) claimed that Spokeo had violated the FCRA by disseminating inaccurate information about him. *Id.* at 1546. Initially, we held that the alleged violation, by itself, sufficed to confer Article III standing. The Supreme Court vacated our decision and remanded, explaining that Article III "requires a concrete injury even in the context of a statutory violation" and that a "bare procedural violation, divorced from any concrete harm," is not enough. *Id.* at 1549. On remand, we held that even though Robins alleged procedural violations of the FCRA, he alleged a sufficient risk of harm (for example, the loss of employment opportunities) to obtain standing. *Robins v. Spokeo, Inc.* (*Spokeo II*), 867 F.3d 1108, 1118 (9th Cir. 2017).

Importantly, *Spokeo* concerned *procedural* violations of the FCRA that would not invariably injure a concrete interest. *Id.* at 1114 (describing the FCRA provisions at issue as "*procedural* requirements" (emphasis added)); *id.* at 1116

(examining the plaintiff's "*procedural* rights" (emphasis added)). Indeed, the central provision at issue in *Spokeo* was 15 U.S.C. § 1681e(b), which falls under the FCRA's "Compliance procedures" section and requires consumer reporting agencies to take "reasonable procedures to assure maximum possible accuracy" of the information they report. But a violation of that provision does not necessarily affect a plaintiff's concrete interests. *See Spokeo I*, 136 S. Ct. at 1550 (noting that "not all inaccuracies cause harm or present any material risk of harm" and giving, as an example, the dissemination of a consumer's incorrect zip code). As a consequence, the *Spokeo* plaintiff had to plead additional harm to obtain standing. *Id.*

By contrast, 18 U.S.C. § 2710(b)(1), the VPPA provision at issue here, codifies a context-specific extension of the *substantive* right to privacy: "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 . . . ." That provision does not describe a procedure that video service providers must follow. Rather, it protects generally a consumer's substantive privacy interest in his or her video-viewing history. *Mollett*, 795 F.3d at 1065 (citing S. Rep. No. 100-599, at 1 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342). Accordingly, *every* disclosure of an individual's "personally identifiable information" and video-viewing history offends the interests that the statute protects.

Congressional judgment leaves little doubt that 18 U.S.C. § 2710(b)(1) is a substantive provision that protects concrete interests. Congress enacted the VPPA "to extend privacy protection to records that contain information about individuals." S. Rep. No. 100-599, at 2. To that end, the

VPPA permits consumers to obtain damages for a violation of § 2710(b)(1) without showing consequential harm. 18 U.S.C. § 2710(c)(2).[1] The VPPA does not protect only against harms such as embarrassment and harassment—as Defendant argues. Rather, the statute also protects privacy interests more generally by ensuring that consumers retain control over their personal information. *See* S. Rep. No. 100-599, at 6–7 (explaining that the VPPA protects against intrusion in an age when consumers "provide to businesses . . . personal information without having any control over where that information goes").

Historical practice confirms that understanding. Violations of the right to privacy have long been actionable at common law. *See Braitberg v. Charter Commc'ns, Inc.*, 836 F.3d 925, 930 (8th Cir. 2016) (stating that "there is a common law tradition of lawsuits for invasion of privacy"). Indeed, the Supreme Court has noted that "both the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person." *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989). Tellingly, privacy torts do not always require additional consequences to be actionable. *See, e.g.*, Restatement (Second) of Torts § 652B cmt. b. (Am. Law Inst. 1977) (recognizing the tort of

[1] In Defendant's view, the word "aggrieved" suggests that the statute requires a showing of additional harm and that, without such a showing, a consumer does not have standing. We disagree. The Supreme Court has explained that the term "aggrieved" demonstrates an "intent to cast the standing net broadly." *Fed. Election Comm'n v. Akins*, 524 U.S. 11, 19 (1998) (addressing the term in the context of prudential standing). Regardless, congressional history clearly shows that Congress thought that every unauthorized disclosure "aggrieves" a consumer. *Mollett*, 795 F.3d at 1065.

intrusion upon seclusion, for which the "intrusion itself" makes the defendant liable). The VPPA functions in the same way.

Thus, although the FCRA outlines *procedural* obligations that *sometimes* protect individual interests, the VPPA identifies a *substantive* right to privacy that suffers *any time* a video service provider discloses otherwise private information. As a result, every 18 U.S.C. § 2710(b)(1) violation "present[s] the precise harm and infringe[s] the same privacy interests Congress sought to protect" by enacting the VPPA. *Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1043 (9th Cir. 2017) (so holding with respect to the Telephone Consumer Protection Act of 1991). Accordingly, *Spokeo I* and *Spokeo II* are distinguishable from this VPPA claim, and Plaintiff need not allege any further harm to have standing. *Id.*[2] We therefore join the two other circuits that, after *Spokeo I*, have found Article III standing in similar cases arising under the VPPA. *Perry v. Cable News Network, Inc.*, 854 F.3d 1336, 1341 (11th Cir. 2017); *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 274 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 624 (2017).

[2] The VPPA's history shows why an allegation of additional harm is unnecessary. Congress enacted the VPPA after a newspaper published Supreme Court nominee Robert Bork's video rental history. Notably, Judge Bork's rental history was decidedly commonplace, and the article did not hurt his nomination. Case Comment, *Statutory Interpretation—The Video Privacy Protection Act—Eleventh Circuit Limits the Scope of "Subscriber" for VPPA Protections.—Ellis v. Cartoon Network, Inc., 803 F.3d 1251 (11th Cir. 2015)*, 129 Harv. L. Rev. 2011, 2018–19 (2016). Were we to accept Defendant's argument regarding standing, the VPPA would not provide legal recourse to those in the precise situation that prompted the statute's enactment in the first place.

B. "*Personally Identifiable Information*"

The district court dismissed Plaintiff's claim on the ground that the allegedly disclosed information did not constitute "personally identifiable information" within the meaning of the VPPA. The VPPA defines "personally identifiable information" to "include[] 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(a)(3). We agree with the district court's conclusion.

As an initial matter, "personally identifiable information" must include more information than that which, by itself, identifies an individual as having watched certain videos. Instead, "personally identifiable information" covers some information that *can be used* to identify an individual.

Two reasons support that conclusion, and both flow directly from the VPPA's text. First, § 2710(a)(3) uses the open-ended word "includes," which suggests that the proffered definition describes only one example of "personally identifiable information." Read in context, the word "includes" seems particularly deliberate here. *Compare* 18 U.S.C. § 2710(a)(3) (using the word "includes") *with* 18 U.S.C. § 2710(a)(1), (a)(2) & (a)(4) (using the word "means" to define other statutory terms). Second, Congress used the word "identifi*able*." 18 U.S.C. § 2710(a)(3) (emphasis added). And the suffix "able" means "capable of." *Webster's Third New Int'l Dictionary* 4, 1123 (unabr. ed. 1981). It follows, then, that the term "personally identifiable information" covers some information that is "capable of" identifying a person, as well as information that, standing alone, identifies a person.

The question remains, though: Under the VPPA, what information did Congress intend to cover as "capable of" identifying an individual? Two circuits have considered that question in similar cases, and each has articulated a different standard. *Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482, 486 (1st Cir. 2016); *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 284 (3d Cir. 2016).

In *Yershov*, the First Circuit held that the term "personally identifiable information" encompasses "information *reasonably and foreseeably likely* to reveal which . . . videos [a person] has obtained." 820 F.3d at 486 (emphasis added). The court concluded that an iPhone user's GPS coordinates and device identifier fell within that definition. *Id.* In a similar case, though, the Third Circuit held that a unique IP address did not qualify as "personally identifiable information," because the term includes only information that "readily permit[s] *an ordinary person* to identify a [particular individual as having watched certain videos]." *In re Nickelodeon*, 827 F.3d at 290 (emphasis added). We adopt the Third Circuit's "ordinary person" standard.

The "ordinary person" test better informs video service providers of their obligations under the VPPA. The VPPA protects consumer privacy by directing video service providers not to do certain things with consumer information. To that end, 18 U.S.C. § 2710(b)(1) focuses on what information a video service provider "knowingly discloses." In other words, the statute views disclosure from the perspective of the disclosing party. It looks to what information a video service provider discloses, not to what the recipient of that information decides to do with it. As a result, "personally identifiable information" must have the same meaning without regard to its recipient's capabilities.

Holding otherwise would make "[t]he lawfulness of [a] disclosure . . . depend on circumstances outside of [a video service provider's] control." *Mollett*, 795 F.3d at 1066. The Third Circuit's "ordinary person" test, by contrast, provides video service providers with enough guidance to comply with the VPPA's requirements.

The interpretation that we adopt fits most neatly with the regime that the VPPA's enacting Congress likely had in mind. In 1988, the Internet had not yet transformed the way that individuals and companies use consumer data—at least not to the extent that it has today. Then, the VPPA's instructions were clear. The manager of a video rental store in Los Angeles understood that if he or she disclosed the name and address of a customer—along with a list of the videos that the customer had viewed—the recipient of that information could identify the customer. By contrast, it was clear that, if the disclosure were that "a local high school teacher" had rented a particular movie, the manager would not have violated the statute. That was so even if one recipient of the information happened to be a resourceful private investigator who could, with great effort, figure out which of the hundreds of teachers had rented the video. Plaintiff's Roku device serial number is like the information in the latter scenario. It creates a sizable "pool" of possible viewers—here, Roku users—just as the information in the latter example does—there, high school teachers.

It is true that today's technology may allow Adobe to identify an individual from the large pool by using other information—as Plaintiff alleges. But the advent of the Internet did not change the disclosing-party focus of the statute. And we are not persuaded that the 1988 Congress intended for the VPPA to cover circumstances so different

from the ones that motivated its passage. Therefore, drawing on the Third Circuit's reasoning, we hold that "personally identifiable information" means only that information that would "readily permit an ordinary person to identify a specific individual's video-watching behavior." *In re Nickelodeon*, 827 F.3d at 267.

Applying that definition here, the operative complaint is deficient. Plaintiff alleges that Defendant disclosed to Adobe: (1) his Roku device serial number and (2) the names of the videos that he watched. As Plaintiff concedes, that information *cannot* identify an individual unless it is combined with other data in Adobe's possession—data that ESPN never disclosed and apparently never even possessed. Indeed, according to Plaintiff, Adobe can identify individuals only because it uses a complex "Visitor Stitching technique" to link an individual's Roku device number with other identifying information derived from "an enormous amount of information" collected "from a variety of sources." We conclude that an ordinary person could not use the information that Defendant allegedly disclosed to identify an individual. Plaintiff has therefore failed to state a claim under Rule 12(b)(6).

Our decision today, though it adopts a different test, does not necessarily conflict with *Yershov*. The First Circuit's *holding* in that case was quite narrow. The court held

> only that the transaction described in the complaint—whereby Yershov used the mobile device application that Gannett provided to him, which gave Gannett the GPS location of Yershov's mobile device at the time he viewed a video, his device identifier, and the

> titles of the videos he viewed in return for access to Gannett's video content—plausibly plead[ed] a case that the VPPA's prohibition on disclosure applies.

Yershov, 820 F.3d at 489. The First Circuit relied, in part, on the nature of GPS location data, which the court noted "would enable *most people* to identify [an individual's home and work addresses]." *Id.* at 486 (emphasis added). And the court expressly noted that, at some point, "the linkage of information to identity becomes too uncertain" to trigger liability under the VPPA. *Id.* That is precisely the situation here.

Nor does our holding make the statute powerless. Names and addresses, of course, still qualify. *See* 18 U.S.C. § 2710(b)(2)(D) (permitting video service providers to "disclose personally identifiable information . . . if [among other conditions] the disclosure is *solely of the names and addresses of consumers*" (emphasis added)). It is not difficult to imagine other examples that may also count—for example, an individual's name and telephone number or an individual's name and birthday or, as in *Yershov*, the GPS coordinates of a particular device. And modern technology may indeed alter—or may already have altered—what qualifies under the statute. A Facebook link or an email address may very well readily enable an "ordinary person" to identify an individual. We need not and do not opine on the merits of those theories. The allegations before us, though, are simply too attenuated to qualify under the standard that we adopt today.[3]

[3] In view of our holding, we need not reach any other issue. We therefore do not decide, for example, whether Plaintiff has adequately alleged his status as a "consumer" under the VPPA.

CONCLUSION

Plaintiff has Article III standing to bring his claim because 18 U.S.C. § 2710(b)(1) is a substantive provision protecting consumers' concrete interest in their privacy. We affirm the judgment of dismissal because the information described in Plaintiff's complaint does not constitute "personally identifiable information" under the VPPA.

AFFIRMED.