CHAPTER THREE

THE VIDEO PRIVACY PROTECTION ACT AS A MODEL INTELLECTUAL PRIVACY STATUTE

Judge Robert Bork had offered his assessment of privacy's constitutional status in scholarly tomes and congressional testimony,[1] but in the fall of 1987, the only theory of privacy that mattered was Michael Dolan's. In *The Bork Tapes*, a self-consciously intrusive survey of Judge Bork's video rental history published in the *Washington City Paper*, reporter Michael Dolan offered the following insight: "The only way to figure out what someone is like is to examine what that someone likes — take a hard look at the tools of leisure he uses to chip away life's rough edges."[2] The article attempted to reconstruct the interior life of a U.S. Supreme Court nominee who would go on to criticize the constitutional right to privacy as "a loose canon in the law,"[3] confronting Judge Bork with his own vulnerability to privacy harms. The list of 146 videotapes Judge Bork had rented over the course of two years, leaked by a store clerk, revealed nothing particularly salacious. Judge Bork favored Alfred Hitchcock films, spy thrillers, and British costume dramas; someone in the Bork household had an affinity for John Hughes movies. The list's disclosure hardly intruded upon the sphere of intimate and domestic life protected from government intrusion by *Griswold v. Connecticut*[4] and its progeny.[5] Yet, against the backdrop of "[o]ne of the fiercest battles ever waged over a Supreme Court nominee,"[6] the publication of *The*

---

[1] *Nomination of Robert H. Bork to Be Associate Justice of the Supreme Court of the United States: Hearing Before the S. Comm. on the Judiciary*, 100th Cong. 115 (1987) (statement of Judge Robert H. Bork).

[2] Michael Dolan, *The Bork Tapes*, WASH. CITY PAPER (Sept. 25–Oct. 1, 1987), https://web.archive.org/web/20160313041803/http://theamericanporch.com/bork5.htm [https://perma.cc/37V2-T2ZD].

[3] ROBERT H. BORK, THE TEMPTING OF AMERICA 97 (1990).

[4] 381 U.S. 479 (1965).

[5] *See id.* at 484–86 (locating a right to privacy in the penumbras of the First, Third, Fourth, Fifth, and Ninth Amendments to the U.S. Constitution); *see also* Roe v. Wade, 410 U.S. 113, 151–53 (1973) (recognizing that the constitutional guarantee of privacy prevents the government from burdening an individual's activities related to marriage, procreation, contraception, family relationships, child rearing, and education unless the state can show a compelling countervailing interest).

[6] Linda Greenhouse, *Bork's Nomination Is Rejected, 58-42; Reagan "Saddened,"* N.Y. TIMES (Oct. 24, 1987), http://www.nytimes.com/1987/10/24/politics/24REAG.html [https://perma.cc/H2S8-4RKA].

Bork Tapes drew bipartisan ire and generated consensus[7] on the importance of intellectual privacy.[8]

The following year, Congress enacted the Video Privacy Protection Act[9] (VPPA), which restricted the disclosure of video records without the watcher's consent.[10] The Act followed a spate of privacy-protective statutes enacted in the 1970s and 1980s: the Privacy Act of 1974, the Privacy Protection Act of 1980, the Cable Communications Policy Act of 1984, and the Electronic Communications Privacy Act of 1986.[11] Policymakers had become increasingly concerned about "minimizing intrusiveness, maximizing fairness, and creating legitimate, enforceable expectations of confidentiality,"[12] especially after repeated judicial failures to secure personal privacy rights in spheres less intimate than reproduction.[13] Congress made its goals manifestly clear in supplementing constitutional privacy with statutory protection. First, the VPPA evinced a desire to embody purpose-specification,[14] use-limitation, and individual-participation principles already familiar from the first iteration of the Organisation for Economic Cooperation and Development (OECD) Privacy Guidelines, a set of internationally agreed-upon privacy principles developed in the 1980s.[15] Second, the Act recognized that a video watcher's privacy — like a reader's or a writer's privacy — implicates First Amendment values that Congress ought to safeguard.[16]

---

7 Michael deCourcy Hinds, *Personal but Not Confidential: A New Debate over Privacy*, N.Y. TIMES (Feb. 27, 1988), http://www.nytimes.com/1988/02/27/style/consumer-s-world-personal-but-not-confidential-a-new-debate-over-privacy.html [https://perma.cc/9UDE-7NCS].

8 Intellectual privacy is defined as "protection from surveillance or interference when we are engaged in the processes of generating ideas — thinking, reading, and speaking with confidants before our ideas are ready for public consumption." NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 5 (2015).

9 18 U.S.C. § 2710 (2012).

10 *Id.* § 2710(b).

11 S. REP. NO. 100-599, at 2–3 (1988) (noting that the VPPA "follows a long line of statutes passed by the Congress to extend privacy protection to records that contain information about individuals," *id.* at 2, and listing examples).

12 PRIVACY PROT. STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 396 (1977), https://www.ncjrs.gov/pdffiles1/Digitization/49602NCJRS.pdf [https://perma.cc/J3YG-8M5Z].

13 The Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3422 (2012), for example, was enacted in response to the Supreme Court's ruling in *United States v. Miller*, 425 U.S. 435 (1976), that individuals had no reasonable expectation of privacy in bank records because the records had been voluntarily disclosed to a third party, *id.* at 442–43. *See* S. REP. NO. 100-599, at 3.

14 *See* S. REP. NO. 100-599, at 8 ("The Act reflects the central principle . . . that information collected for one purpose may not be used for a different purpose without the individual's consent.").

15 *See* ORG. FOR ECON. CO-OPERATION & DEV., GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *reprinted in* OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 11, 14–16 (2002).

16 *See* S. REP. NO. 100-599, at 4–5.

The landscape of intellectual engagement has shifted significantly since 1988. A newspaper reporter who attempted to replicate Dolan's experiment today would have trouble finding a brick-and-mortar video rental store — and, once there, would scarcely find a satisfactory set of subscribers to snoop on. A Supreme Court nominee wanting to check out something more scandalous than *Pretty in Pink* would probably opt for an online transaction, availing himself or herself of an oft-overlooked privacy benefit of a digitized intellectual environment: privacy from the store clerk.[17] Our watching habits, like our reading habits, have moved online. The relevant players in video privacy are no longer Blockbuster and Hollywood Video, but rather Amazon, Netflix, and Hulu.[18]

Since 1988, doctrine has changed as well. *Lujan v. Defenders of Wildlife*[19] redefined the meaning of standing to sue, placing the emphasis on injury in fact.[20] In the lead-up to *Spokeo, Inc. v. Robins*,[21] information privacy scholars expressed their concern that the Supreme Court's ruling could undermine citizens' ability to seek relief under privacy-protective statutes like the VPPA.[22] In particular, *Spokeo* renewed interest in a persistent question: What kind of privacy harm constitutes an injury in fact?

In the United States' patchwork privacy regime, the VPPA is a unique gap-filler, extending protection — if only in part — to the expressive activities recognized as vital to the First Amendment but left underprotected by the Fourth.[23] This Chapter argues that technological and doctrinal changes have done less damage to the Video Privacy Protection Act than one might expect. The statute's weaknesses lie in its drafting errors and in the more pervasive difficulties courts have with evolving definitions, such as the definition of "personally identifiable information."[24] Despite these weaknesses, the VPPA and recent cases deploying the Act suggest that courts are not hesitant to recognize privacy harms as "injuries" when the harms implicate intellectual privacy. Because of its broad, technology-neutral language, the VPPA has managed to weather the past forty years. Though the statute's effectiveness,

---

[17] *See* BENJAMIN WITTES & EMMA KOHSE, BROOKINGS INST., THE PRIVACY PARADOX II: MEASURING THE PRIVACY BENEFITS OF PRIVACY THREATS 6 (2017), https://www.brookings.edu/wp-content/uploads/2017/01/privacy-paper.pdf [https://perma.cc/EZ76-84H4].

[18] *See* Mike Spector & Peter Lattman, *Hollywood Video Closes Doors*, WALL ST. J. (May 3, 2010, 12:01 AM), http://www.wsj.com/articles/SB10001424052748704608104575220370429528864 [https://perma.cc/8D9M-FF2G].

[19] 504 U.S. 555 (1992).

[20] *Id.* at 560.

[21] 136 S. Ct. 1540 (2016).

[22] Brief of Amici Curiae Information Privacy Law Scholars in Support of Respondent at 10, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (No. 13-1339).

[23] *See* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 117–28 (2007).

[24] 18 U.S.C. § 2710(e) (2012).

like that of any other statute, depends on reasonable judicial interpretation, the VPPA's resilience despite technological and doctrinal changes indicates that the statute might prove an appropriate model for the next logical step in safeguarding the privacy of expressive activity: federal reader privacy legislation.

Section A discusses the VPPA's adaptation to both the technological developments of the past forty years and the Supreme Court's shifting standing doctrine. Section B addresses the lingering weaknesses in the statute's language. Finally, section C argues that the statute as originally drafted could serve as a model for a much-needed federal reader privacy statute. Section D concludes.

A. The VPPA's Surprising Resilience

The VPPA owes its resilience largely to the flexibility of its language. The VPPA prohibits videotape service providers from knowingly disclosing "personally identifiable information" to third parties unless the provider is compelled by a warrant, the provider obtains the consent of the record subject, the provider discloses only the names and addresses of consumers to engage in direct marketing to the consumer, or the provider makes the disclosure "incident to the ordinary course of business."[25] The Act defines "personally identifiable information" as "includ[ing] information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."[26] Congress cast a wide net with respect to standing, providing a cause of action to "[a]ny person aggrieved by any act of a person in violation of this section."[27] The civil remedies section was meant to "put[] teeth into the legislation,"[28] where the evil the statute intended to remedy was that film buffs would be broadly surveilled by private actors and that once in government hands, their cinematic preferences could be used against them.

1. Technological Resilience. — Before the VPPA's 2012 amendments, which allowed videotape service providers to obtain continuing rather than case-by-case consent from consumers to aggregate disclosure of their video records,[29] there was some uncertainty as to whether the VPPA applied to online streaming services. During congressional hearings, Senator Al Franken expressed concerns that the VPPA had become an obsolete, inoperable relic as the world moved from VHS tapes to

---

[25] *Id.* § 2710(b)(2).

[26] *Id.* § 2710(a)(3).

[27] *Id.* § 2710(c)(1).

[28] S. REP. NO. 100-599, at 8 (1988).

[29] *See* William McGeveran, *The Law of Friction*, 2013 U. CHI. LEGAL F. 15, 17–18 (critiquing the 2012 amendments as facilitating frictionless information sharing).

Netflix.[30] However, this concern was unfounded; courts had not struggled to extend the VPPA to the internet, thanks to the statute's technology-neutral language. Because the Act defined a videotape service provider as any person or entity in the business of rental, sale, or delivery of videotapes "or similar audio visual materials,"[31] this provision transitioned relatively smoothly into the twenty-first century.

The first class action lawsuit under the VPPA against an online service, *In re Hulu Privacy Litigation*,[32] was brought in July 2011.[33] Hulu moved to dismiss for lack of subject matter jurisdiction, arguing that it was not a "video tape service provider" under the Act, because it did not sell or rent physical objects like the brick-and-mortar businesses Congress would have recognized at the time of enactment.[34] Relying on dictionary definitions of "material," as well as the VPPA's legislative history, the district court concluded that Hulu was a "video tape service provider," because it was a purveyor of "similar audio visual materials" to prerecorded video cassette tapes.[35] The *Oxford English Dictionary*'s definition of "material" as "[t]ext or images in printed or electronic form . . . as *reading material, etc.*"[36] predated the 1988 Act, and the Senate Report's discussion of laser discs indicated "Congress's intent to cover new technologies for pre-recorded video content."[37] In light of "Congress's concern with protecting consumers' privacy in an evolving technological world," the district court held that the videotape service provider definition included online video streaming services.[38]

2. Doctrinal Resilience. — Doctrinal change also could have threatened the VPPA's efficacy. While the Act was drafted to grant standing up to the constitutional limit, conferring a cause of action on "[a]ny person aggrieved" under the Act,[39] Supreme Court cases decided in the years after the VPPA's enactment clarified that constitutional limit. According to the formulation set forth in *Lujan v. Defenders of Wildlife*, a congressional grant of standing passes constitutional muster only when

---

[30] *The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century*, *Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 3 (2012) ("Streaming is the future of video, but no judge has ever decided whether or not the *Video Privacy Protection Act* covers streaming video companies. I think it is clear that the law does cover new technologies like streaming because it does not just cover 'prerecorded video cassette tapes.' It also covers 'similar audio-visual materials.'").

[31] 18 U.S.C. § 2710(a)(4).

[32] No. C 11-03764, 2014 WL 1724344 (N.D. Cal. Apr. 28, 2014).

[33] *See* Class Action Complaint at 1, *In re Hulu*, No. C 11-03764, ECF No. 1.

[34] *In re* Hulu Privacy Litig., No. C 11-03764, 2012 WL 3282960, at *4 (N.D. Cal. Aug. 10, 2012).

[35] *Id.* at *6 (quoting S. REP. NO. 100-599, at 12 (1988)); *see also id.* at *5–6.

[36] *Id.* at *5 (quoting OXFORD ENGLISH DICTIONARY (3d ed. 2001), http://www.oed.com/view/Entry/114923 [https://perma.cc/9DWU-AHDZ]).

[37] *Id.* at *6.

[38] *Id.*

[39] 18 U.S.C. § 2710(c)(1) (2012).

the plaintiff has suffered a concrete, particularized, and actual or imminent injury in fact.[40]

(a) The VPPA Under the Lujan *Standard.* — Because of the nature of the harm Congress sought to prevent, the statute had little trouble meeting *Lujan*'s standard, even though the enacting Congress could not have foreseen the doctrinal shift. The VPPA evinces Congress's desire to prevent government intrusion upon the deliberative space in which citizens read, watch, think, and create. The Senate Report expressed Congress's solicitude for intellectual privacy, describing the protection of "an individual's choice of books and films [as] a . . . pillar of intellectual freedom under the [F]irst [A]mendment."[41] Surveying the case law — with particular emphasis on *Stanley v. Georgia*,[42] which recognized the First Amendment right to receive even obscene materials in the privacy of one's own home[43] — the enacting Congress linked the VPPA with core First Amendment rights.[44] Unregulated disclosure of records revealing "our loves, likes, and dislikes,"[45] the Senate Report argued, could inhibit the intellectual process, delegitimize dissent, and undermine the First Amendment value of avoiding the prescription of orthodoxy of thought.[46]

In *Amazon.com LLC v. Lay*,[47] Amazon sued the North Carolina Department of Revenue under the VPPA and the First Amendment, seeking injunctive relief to avoid complying with a request to disclose the names and addresses of its customers in addition to detailed descriptions of the products ordered by each customer.[48] The Department of Revenue had requested the records to determine whether Amazon had evaded sales taxes on online sales to North Carolina residents.[49] Because the Department of Revenue had already obtained product code numbers and "other . . . details" including "the order ID number, seller, ship-to city, county, postal code, the non-taxable amount of purchase, and the tax audit record identification" from Amazon, Amazon argued that complying with the request would give the Department of Revenue "all information necessary to know the expressive content of all purchases

---

40 Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

41 S. REP. NO. 100-599, at 4 (1988).

42 394 U.S. 557 (1969).

43 *Id.* at 565.

44 *See* S. REP. NO. 100-599, at 4.

45 *Id.* at 7 (quoting 134 CONG. REC. 5400, 5401 (1988) (statement of Sen. Simon)).

46 *See* W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 642 (1943) ("If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion or force citizens to confess by word or act their faith therein.").

47 758 F. Supp. 2d 1154 (W.D. Wash. 2010).

48 *Id.* at 1158–60.

49 *Id.*

from Amazon by individual North Carolina residents."[50] The district court agreed that combining the two data sets would violate the VPPA and concluded that standing presented no obstacle under the VPPA or the First Amendment, seeing the two as inextricably linked.[51]

First, given relaxed standing requirements in the First Amendment arena, the court reasoned, there was no reason to wait for the privacy violation to lead to some tangible harm, such as economic damage, to grant standing.[52] Because "[i]n the context of First Amendment speech, a threat of enforcement may be inherent in the challenged statute," the claim was ripe for review.[53] Furthermore, the court found imminent harm associated with the potential VPPA violation of the chilling effect that disclosure would have on speech: "the fear of disclosure of their reading, watching, and listening habits poses an imminent threat of harm and chill to the exercise of First Amendment rights."[54]

In *Sterk v. Redbox Automated Retail, LLC*,[55] the Seventh Circuit found that a class of consumers whose video rental information had been disclosed to one of Redbox's third-party vendors had standing to sue. First, the court acknowledged Congress's role in "creating legal rights, the invasion of which creates standing, even though no injury would exist without the statute."[56] Second, the court anticipated the holding of *Spokeo* — that bare procedural violations fell short of the constitutional standing requirements articulated in *Lujan*. The Seventh Circuit was explicit that the VPPA protects core privacy rights: "'technical' violations of the statute (*i.e.*, impermissible disclosures of one's sensitive, personal information) are *precisely what Congress sought to illegalize by enacting the VPPA*."[57] Accordingly, the plaintiffs easily cleared the constitutional standing requirements.[58]

In *Austin-Spearman v. AMC Network Entertainment LLC*,[59] the U.S. District Court for the Southern District of New York found that plaintiffs suing under the VPPA had standing. Writing that by enacting the VPPA Congress had created a legal right, the invasion of which constituted injury in fact, the court concluded that "wrongful disclosure even

---

50 *Id.* at 1159.

51 *Id.* at 1170–72.

52 *Id.* at 1162; *see also* Cal. Pro-Life Council, Inc. v. Getman, 328 F.3d 1088, 1094 (9th Cir. 2003) (noting that "in the First Amendment protected speech context, the Supreme Court has dispensed with rigid standing requirements to address the chilling effect on speech").

53 *Amazon*, 758 F. Supp. 2d at 1162 (quoting Wolfson v. Brammer, 616 F.3d 1045, 1059 (9th Cir. 2010)).

54 *Id.* at 1163.

55 770 F.3d 618 (7th Cir. 2014).

56 *Id.* at 623 (quoting Kyles v. J.K. Guardian Sec. Servs., Inc., 222 F.3d 289, 294 (7th Cir. 2000)).

57 *Id.* (emphasis added).

58 *Id.*

59 98 F. Supp. 3d 662 (S.D.N.Y. 2015).

without additional injury [afforded] a right to relief."[60] Underscoring the similar standing rationales offered by the Seventh, Ninth, and Eleventh Circuits, the *Austin-Spearman* court noted that "every court to have addressed this question has reached the same conclusion, affirming that the VPPA establishes a privacy right sufficient to confer standing through its deprivation."[61]

(b) Spokeo Inc. v. Robins. — *Spokeo v. Robins* generated a wealth of scholarly debate long before being decided by the Supreme Court — and with good reason. The case was expected to resolve the uncertainty surrounding the so-called "no injury" class action.[62] *Spokeo* presented an opportunity to clarify what types of consumer protection and privacy injuries satisfied the injury-in-fact requirement.

Spokeo is a website that aggregates information on "individuals, including contact data, marital status, age, occupation, economic health, and wealth level."[63] Thomas Robins's Spokeo entry indicated that he was a wealthy advanced-degree holder who was married with children.[64] Robins was none of those things. In fact, Robins was actively seeking employment.[65] Robins sued Spokeo in the Central District of California, alleging that Spokeo had violated the Fair Credit Reporting Act (FCRA) by disseminating consumer reports that fell below the "maximum possible accuracy" standard.[66] The district court held that, even though Robins claimed the inaccurate reports had hampered his job search, Robins had not yet suffered an injury in fact and thus did not have standing.[67] The Ninth Circuit reversed.[68] Spokeo appealed and the Supreme Court granted certiorari on the issue of standing.[69]

Fifteen information privacy scholars filed an amicus brief in the case, expressing several concerns. First, the scholars argued that a broad con-

---

60 *Id.* at 662.

61 *Id.* at 666.

62 *See* Samuel Issacharoff et al., *Panel 1: The Current State of the Consumer Class Action*, 11 N.Y.U. J.L. & BUS. 647, 656–57 (2015); Paul Scrudato et al., *No Injury? No Problem*, 2015–2016 SUP. CT. PREVIEW 125, 125 (2015); Daniel Townsend, *Who Should Define Injuries for Article III Standing?*, 68 STAN. L. REV. ONLINE 76, 76–77 (2015).

63 Robins v. Spokeo, Inc., 742 F.3d 409, 410 (9th Cir. 2014), *vacated and remanded*, 136 S. Ct. 1540 (2016).

64 Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1546 (2016).

65 *Robins*, 742 F.3d at 411.

66 *Id.* at 412 (quoting 15 U.S.C. § 1681e(b) (2012)); Robins v. Spokeo, Inc., No. CV10-05306, 2011 WL 597867, at *1 (C.D. Cal. Jan. 27, 2011).

67 *Robins*, 2011 WL 597867, at *1 (finding that Robins had alleged only that Spokeo's inaccuracies might affect his ability to obtain credit and employment and concluding that "[a]llegations of possible future injury do not satisfy the [standing] requirements" (alterations in original) (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990))).

68 *Robins*, 742 F.3d at 414.

69 Spokeo, Inc. v. Robins, 135 S. Ct. 1892, 1892 (2015) (mem.).

ception of standing was necessary "[t]o reinforce the statutory obligations of reasonableness and transparency."[70] Second, the scholars argued that the FCRA's statutory design envisioned "enlist[ing] consumers themselves in the process of correcting inaccurate information."[71] Third, the scholars explained the concrete harms that Robins and similarly situated consumers could suffer due to inaccurate information on Spokeo: reduced employment prospects as employers screen out applicants whose applications do not match other available records or applicants who seem overqualified.[72] Fourth, the scholars argued that "[a] broad ruling in this case would disrupt established privacy law well beyond the boundaries of the FCRA."[73] The scholars went further, alleging that "[a] broad ruling in this case could foreclose the private suits Congress envisioned as VPPA remedies."[74] The scholars' amicus brief reflected a consensus view that *Spokeo* could be potentially disastrous for privacy-protective statutes, vitiating privacy protections by narrowing the scope of privacy harms.[75]

In *Spokeo v. Robins*, the Supreme Court reaffirmed that "a bare procedural violation, divorced from any concrete harm, [could not] satisfy the injury-in-fact requirement of Article III."[76] The Court first noted that the Ninth Circuit erred in conflating *Lujan*'s particularity and concreteness prongs when determining whether Robins had suffered an injury in fact.[77] *Spokeo* was largely a restatement of settled law. The Court reiterated that "[t]o establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'"[78] Rather than narrow the scope of privacy harms to require economic damage, the Court stated that "intangible injuries can nevertheless be concrete," citing free speech and free exercise rights as examples of intangible interests that nevertheless generate standing to sue.[79] The Court suggested that because Congress is "well positioned to identify intangible harms," courts ought to consider legislative judgments when assessing whether a plaintiff has standing under a statutory provision, as long as that provision protects a concrete interest.[80] To

---

70 Brief of Amici Curiae Information Privacy Law Scholars in Support of Respondent, *supra* note 22, at 10.

71 *Id.* at 4.

72 *Id.* at 17–25.

73 *Id.* at 27.

74 *Id.* at 28.

75 *See, e.g.*, Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 365–66 (2015).

76 Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016).

77 *Id.* at 1548.

78 *Id.* (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)).

79 *Id.* at 1549.

80 *Id.*

determine whether an intangible harm is concrete, the Supreme Court instructed the judiciary to relate alleged intangible harms to harms traditionally regarded as providing the basis for a lawsuit in English and American common law.[81] The majority opinion made no statement on whether Robins's hampered job search or the mere inaccuracy of the information contained in Spokeo's searchable database would confer standing,[82] instead remanding the case to the Ninth Circuit.[83]

(c) Status Quo Post-Spokeo. — Contrary to the dire prognostications of the information privacy scholars and even some post-decision commentators,[84] *Spokeo* did little to change the way courts treat privacy harms under the VPPA. Post-*Spokeo* cases confirm this. In *In re Nickelodeon Consumer Privacy Litigation*,[85] the Third Circuit extensively analyzed *Spokeo* and found that "[t]he Supreme Court's recent decision . . . does not alter our prior analysis."[86] In so concluding, the court relied on the congressional judgment that certain types of information ought to remain private, regardless of whether disclosure presents a material risk of harm.[87] The court then noted before proceeding to the merits that the privacy the VPPA protects is a traditional basis for a lawsuit.[88] Despite its fanfare, *Spokeo* proved not to be particularly revolutionary — and the intellectual privacy harms that the VPPA seeks to prevent and to remedy are not so hard to grasp.

As a caveat, there is one provision of the VPPA where standing doctrine as articulated in *Spokeo* poses a genuine problem: the data retention provision. Courts have held that the Act's data retention provision does not create a private right of action.[89] While these opinions have depended on typical statutory interpretation arguments,[90] not a restrictive theory of injury in fact, *Spokeo* suggests that even a well-drafted

---

[81] *See id.*

[82] *Id.* at 1550 & n.8.

[83] *Id.* at 1550.

[84] *See, e.g.*, *The Supreme Court, 2016 Term — Leading Cases*, 130 HARV. L. REV. 437, 446 (2016) ("While *Spokeo* seemed only to reiterate well-established tenets of standing, its consequences may be far-reaching. *Spokeo* jeopardizes the breadth of many laws whose enforcement is likewise premised on suits by classes of persons whom the proscribed conduct has a tendency to injure, regardless of proof of consequential harms.").

[85] 827 F.3d 262 (3d Cir. 2016).

[86] *Id.* at 273. *But see infra* pp. 1775–77 (arguing that *Spokeo* ought to have changed the Third Circuit's analysis with respect to the VPPA data retention provision).

[87] *In re Nickelodeon*, 827 F.3d at 273–74.

[88] *Id.*

[89] *See, e.g.*, Rodriguez v. Sony Comput. Entm't Am., LLC, 801 F.3d 1045, 1052 (9th Cir. 2015) (agreeing with the Sixth and Seventh Circuits that Congress declined to provide a private right of action to challenge unlawful retention of data beyond the statutory time limit).

[90] *See infra* section B, pp. 1777–82; *see also, e.g.*, Sterk v. Redbox Automated Retail, LLC, 672 F.3d 535, 538 (7th Cir. 2012) ("If (c) appeared after all the prohibitions, which is to say after (d) and (e) as well as (b), the natural inference would be that any violator of any of the prohibitions could be sued for damages. But instead (c) appears after just the first prohibition, the one in subsection

VPPA might not authorize data retention suits.[91] Like the consumer notification provision of the FCRA analyzed in *Spokeo*, the data retention provision is likely to be deemed a procedural requirement that cannot, without a more detailed showing of harm, support standing for suit.[92] Furthermore, Justice Thomas's concurrence distinguished between suits alleging the violation of private rights and suits alleging the violation of public rights.[93] For suits alleging violations of private rights, a plaintiff need only allege that his legal rights were invaded to have standing to sue — but if a plaintiff sues to enforce "general compliance with regulatory law,"[94] a showing of concrete and particularized harm stemming from the violation is necessary.[95] The data retention provision of the VPPA is unconnected to an individual's (private) intellectual privacy rights, and as such would likely be considered "a series of regulatory duties . . . owe[d] to the public collectively."[96] A plaintiff could perhaps allege concrete and particularized harm by pointing to the enacting Congress's purpose in including the retention provision: "to reduce the chances that an individual's privacy will be invaded, by requiring the destruction of information in an expeditious fashion."[97] But courts thus far have not appeared amenable to this argument.[98] Furthermore, even if a court accepted that the violation of the retention provision increased the plaintiff's risk of a privacy violation, the plaintiff would struggle to

(b), prohibiting disclosure. This placement could be an accident, but . . . the more plausible interpretation is that it is limited to enforcing the prohibition of disclosure.").

91 For an application of *Spokeo* to a data retention provision similar to the VPPA, see *Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 912 (7th Cir. 2017) (finding no standing to challenge violations of the data retention provision under the Cable Communications Policy Act); and *Braitberg v. Charter Commc'ns, Inc.*, 836 F.3d 925, 930 (8th Cir. 2016) (same).

92 *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016) ("A violation of one of the FCRA's procedural requirements may result in no harm. For example, even if a consumer reporting agency fails to provide the required notice to a user of the agency's consumer information, that information regardless may be entirely accurate. In addition, not all inaccuracies cause harm or present any material risk of harm.").

93 *See id.* at 1551 (Thomas, J., concurring).

94 *Id.* (quoting Ann Woolhandler & Caleb Nelson, *Does History Defeat Standing Doctrine?*, 102 MICH. L. REV. 689, 693 (2004)).

95 *Id.* at 1551–52.

96 *Id.* at 1553.

97 *See* S. REP. NO. 100-599, at 15 (1988).

98 *See* Sterk v. Redbox Automated Retail, LLC, 672 F.3d 535, 538 (7th Cir. 2012) ("How could there be injury, unless the information, not having been destroyed, were disclosed?"). For an argument that an imminence requirement is nonsensical given the threat posed by data miners, hackers, and large, easy-to-deidentify online data sets, see Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1750 (2010) ("If we fail to regulate reidentification that has not yet ripened into harm, then adversaries can nudge each of us ever closer to the brink of connection to our personal database of ruin.").

claim that retention beyond the statutory limits produces an *imminent* risk of harm — and thus would lack standing.[99]

B. The VPPA's Statutory Interpretation Vulnerabilities

As it turns out, the primary obstacle to seeking redress for privacy harms under the VPPA is not standing's injury-in-fact requirement. Rather, privacy problems present themselves as ordinary statutory interpretation problems. More so than by standing doctrine or the evolving nature of technology, plaintiffs are barred by: (1) the definition of the word "subscriber," (2) the definition of "personally identifiable information," and (3) statutory ambiguity as to whether only "videotape service providers" can be defendants in VPPA lawsuits. To make the VPPA actionable in the twenty-first century requires more reasonable interpretations and, perhaps, more thoughtful drafting. Courts may not currently interpret the Act to keep pace with technological change, but since most obstacles to doing so are not inherent in the statute, there is no reason courts could not embrace more reasonable interpretations of the statute's broad language. The standing overhaul some commentators expected of *Spokeo v. Robins* would have done little to give the VPPA sharper "teeth," but revisiting these statutory interpretation questions might. Data retention provision aside, when plaintiffs stumble in their quests for relief under the VPPA, they trip over the meaning of words, not the meaning of privacy.

Despite Congress's care in drafting provisions that would withstand technological change, the Video Privacy Protection Act is, in some sections, sloppily drafted. Though it is susceptible to the ordinary canons of statutory interpretation, courts are sometimes forced to conclude that the drafters were simply careless. For one thing, the civil remedies provision is sandwiched between the nondisclosure and data retention provisions, creating ambiguity as to whether remedies are available only for unauthorized disclosure, or for unlawful retention as well.[100] For another, in 18 U.S.C. § 2710(b)(1), the statute states that "[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 for the relief provided in subsection (d)."[101] But subsection (d) is not a remedies provision; it sets forth the

---

[99] When a sufficiently particularized increased risk exists, that risk must be imminent. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 416 (2013) (rejecting a theory of standing premised on a risk of communications being unlawfully intercepted by a surveillance program, because the risk was not "certainly impending"); *see also* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016) (requiring a substantial probability of future identity theft to grant standing in data breach litigation); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015) (same).

[100] *See* Rodriguez v. Sony Comput. Entm't Am., LLC, 801 F.3d 1045, 1050 (9th Cir. 2015); Daniel v. Cantrell, 375 F.3d 377, 384 (6th Cir. 2004).

[101] 18 U.S.C. § 2710(b)(1) (2012).

definition of personal information.[102] These drafting faults have not impeded the enforcement of the VPPA altogether, but they have allowed judicial discretion to narrow the protections the statute offers.

1. Subscriber Definition. — Any aggrieved "renter, purchaser, or subscriber of goods or services from a video tape service provider" may sue under the VPPA.[103] The VPPA's definition of a "subscriber" has given rise to disagreement among courts. In *Ellis v. Cartoon Network, Inc.*,[104] the Eleventh Circuit held that "a person who downloads and uses a free mobile application on his smartphone to view freely available content, without more, is not a 'subscriber' . . . under the VPPA."[105] The court in *Ellis* reasoned that subscriber status requires "some type of commitment, relationship, or association (financial or otherwise) between a person and an entity,"[106] and that such commitment might be established by "payment, registration, commitment, delivery, [expressed association,] and/or access to restricted content."[107] Notably, payment for a separate service that allows broader access to free material on another platform does not create a subscriber relationship.[108] In contrast, the First Circuit in *Yershov v. Gannett Satellite Information Network, Inc.*[109] looked to the plain meaning of "subscriber" and found that installing a mobile app was sufficient to create a subscriber relationship when the installation required the user to exchange personal information for access to services.[110]

The textualist critique of *Yershov* is matched by the purposivist critique of *Ellis*, but this Chapter hopes to underscore that this provision's vagueness begets further vagueness. If a financial commitment is not required to be a subscriber, because such a requirement would obliterate the statutory distinction between renters or purchasers and subscribers, what kind of commitment suffices? The *Ellis* court stated that by downloading the Cartoon Network app, Ellis "did not provide any personal information to Cartoon Network, . . . did not sign up for any periodic services or transmissions, and did not make any commitment . . . that would allow him to have access to exclusive or restricted content."[111]

---

102 *Id.* § 2710(d).

103 *Id.* § 2710(a)(1).

104 803 F.3d 1251 (11th Cir. 2015).

105 *Id.* at 1252.

106 *Id.* at 1256.

107 *Id.* (alteration in original) (quoting Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 147 (D. Mass. 2015), *rev'd*, 820 F.3d 482 (1st Cir. 2016)).

108 Perry v. Cable News Network, Inc., 854 F.3d 1336, 1342 (11th Cir. 2017) (confirming that a cable subscriber who uses an associated free online app is not a subscriber to the app, even when the user has paid for the cable subscription, because any exclusive content the user accesses is by virtue of his payment for the cable subscription, not the app).

109 820 F.3d 482 (1st Cir. 2016).

110 *Id.* at 489.

111 *Ellis*, 803 F.3d at 1257.

When seemingly limited-purpose mobile apps collect information on users' geolocation data, browser history, calendar events, photo library, contacts, and device information as a matter of course,[112] is it plausible that Ellis did not provide Cartoon Network with any personal information? Why is an agreement to adhere to an app's terms of service or to allow sweeping access to one's cell phone an insufficient commitment? Would the court have been inclined to call Ellis a subscriber if Cartoon Network had pushed content to the app, or if Ellis had enabled push notifications for the arrival of new content? On the other hand, if Yershov became a subscriber simply by providing the USA Today App with personally identifying information (PII), the nonconsensual disclosure of which necessarily generates a VPPA claim, does the "subscriber" limitation do any work at all? The VPPA has generally adapted well to the shift toward online video consumption. But as media companies waver between "free with advertising" and "freemium" models,[113] Congress should clarify what subscription without payment might mean if the VPPA is to remain vital.

2. Permissible Defendants. — The VPPA is unclear on whether defendants other than video service providers may be held liable. Some courts have held that because "there is no limitation in" 18 U.S.C. § 2710(c)(1) itself, plaintiffs can sue not only disclosers of personally identifiable information, but also receivers of that information.[114] A majority of circuit courts that have weighed in on the issue, however, have found that only videotape service providers who disclose personally identifiable information can be held liable.[115] While this statutory ambiguity underscores the general problems with the statute's drafting, the provision has not aged particularly badly. Increasingly, the pertinent privacy threats are posed by online video service providers that maintain records rather than receive them, because such entities can contribute to and compile "digital dossiers" — that is, "[d]etailed records of an

---

112 Kenneth Olmstead, *Mobile Apps Collect Information About Users, with Wide Range of Permissions*, PEW RES. CTR.: FACT TANK (Apr. 29, 2014), http://www.pewresearch.org/fact-tank/2014/04/29/mobile-apps-collect-information-about-users-with-wide-range-of-permissions/ [https://perma.cc/644E-PEZC].

113 *See* Vineet Kumar, *Making "Freemium" Work*, HARV. BUS. REV., May 2014, at 27, 27–29.

114 Amazon.com LLC v. Lay, 758 F. Supp. 2d 1154, 1167 (W.D. Wash. 2010); *see also* Dirkes v. Borough of Runnemede, 936 F. Supp. 235, 240 (D.N.J. 1996).

115 *See In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 281 (3d Cir. 2016); Daniel v. Cantrell, 375 F.3d 377, 383 (6th Cir. 2004) ("[I]f *any* person could be liable under the Act, there would be no need for the Act to define a [videotape service provider] in the first place.").

individual's reading materials, purchases, diseases, and website activity," which can form the basis of "a profile of an individual's . . . psychology, beliefs, politics, interests, and lifestyle."[116]

3. "Personally Identifying Information." — Perhaps the most alarming aspect of *Spokeo* is Justice Alito's flippant treatment of the importance of a zip code.[117] A zip code is not typically considered PII, the mere disclosure of which could cause or risk harm,[118] but "the combination of a ZIP code, birth date, and gender will be sufficient to identify 87% of individuals in the United States."[119] Given rapid technological developments, perhaps the concept of PII is expanding more quickly than the Supreme Court — and legislators — can keep up.[120] Indeed, the term has been criticized as increasingly meaningless.[121]

VPPA cases highlight courts' difficulty interpreting the term "personally identifiable information." In *In re Hulu Privacy Litigation*,[122] for example, the U.S. District Court for the Northern District of California acknowledged the flexibility in the VPPA's treatment of PII. The statute provides examples of information — names, addresses — that could constitute personal information, but wisely does not limit the PII definition. As the court put it, "[t]he statute does not require an actual name and requires only something akin to it."[123] The court found that the harm from disclosure of PII is present *whether or not* a third party actually identifies the user, but the court eventually decided that the disclosure of "a unique identifier" to a third party, without more data, does not violate the VPPA.[124] Because there was no evidence that a third party correlated the unique identifier with any other information to identify specific people as having requested or obtained video materials

---

116 DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 5 (2004).

117 *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016) ("It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm.").

118 *See* Ohm, *supra* note 98, at 1734 (describing the PII provisions of privacy-protective statutes as affording heightened protections to certain types of information "because of their unusual tendency to cause harm").

119 Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1842 (2011) (citing Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* 1 (Carnegie Mellon Univ., Sch. of Comput. Sci., Data Privacy Lab, Working Paper No. 3, 2000)).

120 *See* Ohm, *supra* note 98, at 1742 (noting that, despite consensus that movie ratings and search queries can lead to the identification of individual users in practice, no regulation treats this data as PII).

121 *See, e.g.*, *id.* at 1732 ("At the very least, legislators must abandon the idea that we protect privacy when we do nothing more than identify and remove PII. The idea that we can single out fields of information that are more linkable to identity than others has lost its scientific basis and must be abandoned.").

122 No. C11-03764, 2014 WL 1724344 (N.D. Cal. Apr. 28, 2014).

123 *Id.* at *14.

124 *Id.* at *12.

or services, the court determined that no "personally identifiable information" had been compromised.[125]

Two approaches to the PII problem predominate. The First Circuit interprets PII as any "information reasonably and foreseeably likely to reveal," directly or indirectly, an individual consumer's identity.[126] In contrast, the Third and Ninth Circuits have defined PII as "information that would readily permit an ordinary person to identify a specific individual's video-watching behavior,"[127] partly because this approach gives better notice to video service providers than a standard that depends on the sophistication of the third party to which the service provider provides information.[128] The statutory language and structure reasonably encompass the First Circuit's less rigid interpretation of PII.[129] The Third Circuit arrived at a narrower interpretation, which the Ninth Circuit later adopted,[130] despite recognizing that an interpretation of "identifiable" as simply "capable of identifying" is within the plain meaning of the statute.[131] Only after consulting the legislative history did the Third Circuit settle upon its "ordinary person" test.[132] But under this purposivist approach, the "ordinary person" test cannot be right for two reasons. First, the Senate Report states that the PII provision "uses the word 'includes' to establish a minimum, but not exclusive, definition of personally identifiable information."[133] Second, the "ordinary person" test excludes information routinely treated as PII, but which an ordinary person could not use, from the statutory PII category. An ordinary person could not, without more, deduce identity from a Social Security Number — but a Social Security Number is routinely treated as identifying.[134] It is possible the Third and Ninth Circuits adopted the "ordinary person" test because the dissemination of a unique identifier generated by a corporation to track its users, rather than by a government to track its citizens, seems harmless[135] — but that is a standing question, not a definitional one.

---

125 *Id.* at *12–13.

126 Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 486 (1st Cir. 2016) (finding that a device's GPS location data was PII).

127 *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 290 (3d Cir. 2016).

128 Eichenberger v. ESPN, Inc., 876 F.3d 979, 985 (9th Cir. 2017); *In re Nickelodeon*, 827 F.3d at 289–90.

129 *See In re* Vizio, Inc., Consumer Privacy Litig., 238 F. Supp. 3d 1204, 1224 (C.D. Cal. 2017) (acknowledging that "statutory structure confirms that Congress intended [the term] to encompass more than a person's name and physical address").

130 *Eichenberger*, 876 F.3d at 985.

131 *In re Nickelodeon*, 827 F.3d at 285; *see also id.* at 285–86.

132 *Id.* at 284–85, 290.

133 S. REP. NO. 100-599, at 12 (1988).

134 Ariel Pardee, Yershov v. Gannett*: Rethinking the VPPA in the 21st Century*, 69 ME. L. REV. 251, 258 (2017).

135 *See id.*

Some courts have agreed with the essential point that an ordinary person cannot link even names and addresses (which the VPPA explicitly categorizes as PII) to individual consumers without referencing other data, but have balked at the "reasonable foreseeability" test's perceived overbreadth.[136] But liability isn't unlimited under this test. The test's limiting principle is exactly what it says on the tin: video service providers would be liable only for disclosure that could reasonably and foreseeably lead to identification, and "there is certainly a point at which the linkage of information to identity becomes too uncertain, or too dependent on too much yet-to-be-done, or unforeseeable detective work."[137] To the extent evidence suggests that we are not approaching the point at which all information is reasonably likely to lead to personal identification,[138] courts can incorporate that judgment call into the reasonable foreseeability test; it is no less daunting a task than a judicial determination of the technological savvy of the average citizen. By treating "foreseeable" as if it means "conceivable," the Third and Ninth Circuits misconstrue the First Circuit's test and miss an opportunity to remain faithful to both Congress's language and purpose.

There is no particular reason that courts could not come to recognize, as scholars have, that information beyond names and addresses could be PII. Particularly in light of people-search services like Spokeo itself, "data availability heightens the ability to turn non-PII into PII."[139] Again, this fault is one of cramped statutory interpretation — the statute does not prohibit the disclosure of identities, but rather the disclosure of identifiable information. What is needed here is not redrafting, but instead a more current judicial understanding of what is identifiable and a recognition that the VPPA was not drafted for video service providers' convenience, but for patrons' privacy.[140] One could envision a plaintiff alleging that the disclosure of non-PII created an imminent risk of being identified. In this scenario, a court willing to accept the already-available metrics for assessing the risk of identification that different types of information pose[141] could find a violation of the VPPA even when disclosing unique identifiers — and *Spokeo* would pose no bar.

---

136 *See, e.g.*, Robinson v. Disney Online, 152 F. Supp. 3d 176, 181 (S.D.N.Y. 2015) ("If nearly any piece of information can . . . be combined with other information so as to identify a person, then the scope of PII would be limitless.").

137 Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 486 (1st Cir. 2016).

138 Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1, 30–33 (2011) (arguing that Professor Paul Ohm's fears concerning the risk of reidentification are overblown).

139 Schwartz & Solove, *supra* note 119, at 1842.

140 *See* Wendy Beylik, Case Comment, *Enjoying Your "Free" App? The First Circuit's Approach to an Outdated Law in* Yershov v. Gannett Satellite Information Network, Inc., 58 B.C. L. REV. ELECTRONIC SUPP. 60, 74–75 (2017).

141 *See* Schwartz & Solove, *supra* note 119, at 1879.

C. Reader Privacy Legislation

The Video Privacy Protection Act addresses harms caused when individual records of consumption of expressive material are disclosed without authorization; its legislative history and its unchanged viability after *Spokeo* both rest on the Act's First Amendment bent. But there is no VPPA equivalent for books. The rise of ebooks and electronic reading platforms has led to a state of private surveillance over reading habits similar to private surveillance over video watching.[142] In some cases, the private actors are the same — yet a consumer could conceivably sue Amazon for disclosing that he watched *Fifty Shades of Grey* but not that he read it.

Federal reader privacy legislation is sorely needed for three reasons. First, most states have enacted statutes preventing the disclosure of individual library records,[143] but these laws create a "patchwork," providing inconsistent protection nationally.[144] For example, some state statutes prevent public libraries, subject to open-records laws, from disclosing a patron's borrowing records to private citizens — the paradigmatic nosy reporter — but impose no requirements on government access to such records.[145] Other states, however, require a warrant before library records may be disclosed to law enforcement.[146]

Second, unlike the VPPA, which protects both purchases and rentals, library records laws do not extend to book purchases and rentals from for-profit entities.[147] This regime creates an artificial distinction between borrowing and purchasing, when there is no obvious difference in the intellectual privacy significance of the two acts. Most state laws also distinguish between borrowing a physical book and borrowing an ebook from a library; in the latter case, the terms of the ebook license dictated by the electronic delivery service would govern whether reader information could be disclosed to third parties.[148]

---

142 *See* Meredith Mays Espino, Comment, *Sometimes I Feel Like Somebody's Watching Me . . . Read? A Comment on the Need for Heightened Privacy Rights for the Consumers of eBooks*, 30 J. MARSHALL J. INFO. TECH. & PRIVACY L. 281, 282 (2013).

143 Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace*, 28 CONN. L. REV. 981, 1031 & n.213 (1996) (identifying library patron privacy laws in forty-two states); *see also* Bruce S. Johnson, *"A More Cooperative Clerk": The Confidentiality of Library Records*, 81 LAW LIBR. J. 769 app. (1989) (collecting library records confidentiality laws for all states except Hawaii, Idaho, Kentucky, Mississippi, New Hampshire, Ohio, Texas, Utah, and West Virginia).

144 BJ Ard, *Confidentiality and the Problem of Third Parties: Protecting Reader Privacy in the Age of Intermediaries*, 16 YALE J.L. & TECH. 1, 25 (2013).

145 *Id.*

146 *Id.* at 25–26.

147 *Id.* at 28–29.

148 *Id.* at 38, 40–41.

Third, and most importantly, the notion of reader privacy implicates First Amendment values that the First Amendment cannot protect. The Supreme Court has observed that "[t]he authors of the First Amendment . . . chose to encourage a freedom . . . [that] embraces the right to distribute literature, and necessarily protects the right to receive it."[149] The Court has also recognized the chilling effect that surveillance can have on protected First Amendment activity,[150] including surveillance activity that undermines the ability to speak anonymously.[151] But in the absence of statutory protection, the First Amendment is not enough to prevent the chilling effect of surveillance on the consumption of expressive materials. The First Amendment governs state action, but citizens are increasingly surveilled not by state actors, but by private corporations that render the need for direct government surveillance of such activity redundant.[152] Private actors can serve as government data collection agents, skirting the state action requirement despite replicating the fear driving *Stanley v. Georgia* — that the government might use an individual's reading habits against him in a criminal proceeding.[153] The Supreme Court has directed lower courts to use "the most scrupulous exactitude" to determine whether a warrant for the seizure of expressive material is sufficiently particularized.[154] But this heightened Fourth Amendment scrutiny vanishes when the government seeks such material from a third party rather than conducting a search or seizure directly.[155] In addition to the state action problem, attempts to derive a reader privacy right from the First Amendment right to receive information have largely languished in the realm of theory[156] — and besides, such attempts would fall into the category of "chilling-effects" claims fraught with standing issues[157] that the VPPA has overcome. If readers are to expect privacy from private actors as they read ebooks or paperbacks, whether they live in California or Kentucky, Congress will have to enact federal reader privacy legislation.

---

149 Martin v. City of Struthers, 319 U.S. 141, 143 (1943) (citation omitted).

150 *See* Solove, *supra* note 23, at 142–43.

151 *E.g.*, McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995); Talley v. California, 362 U.S. 60, 64 (1960).

152 *See* John Palfrey, *The Public and the Private at the United States Border with Cyberspace*, 78 MISS. L.J. 241, 243 (2008).

153 *See* Stanley v. Georgia, 394 U.S. 557, 565 (1969); Solove, *supra* note 23, at 146–47.

154 Stanford v. Texas, 379 U.S. 476, 485 (1965).

155 Solove, *supra* note 23, at 114.

156 *See, e.g.*, Marc Jonathan Blitz, *Constitutional Safeguards for Silent Experiments in Living: Libraries, the Right to Read, and a First Amendment Theory for an Unaccompanied Right to Receive Information*, 74 UMKC L. REV. 799, 808–18 (2006).

157 Matthew Lynch, *Closing the Orwellian Loophole: The Present Constitutionality of Big Brother and the Potential for a First Amendment Cure*, 5 FIRST AMEND. L. REV. 234, 267 (2007).

A review of the scholarship reveals several commonly proposed features of a federal reader privacy statute.[158] First, the statute should prohibit the nonconsensual disclosure of reader-identifying information in association with particular transactions, except when disclosed to law enforcement after a showing of probable cause.[159] Second, a reader privacy statute should bar tracking and disclosure of reader activity beyond what is necessary to render the reading service usable, as well as limit the retention of reader records for longer than is necessary to complete the transaction or to protect a business's financial interest in the transaction.[160] Third, a reader privacy statute should disfavor aggregate consent to surveillance and disclosure of reader activity, but rather should encourage opt-in disclosure on a transaction-by-transaction basis.[161] Fourth, a reader privacy statute should reliably create a private right of action and make statutory damages available.[162] Plaintiffs who have sued under privacy-protective statutes, alleging harm from data collection, have often been unable to state a cognizable injury.[163] An effective reader privacy statute must avoid this pitfall.

Finally, at a higher level of generality, federal privacy legislation should try to avoid the shortcomings that have plagued other privacy-protective statutes. For example, Professor Orin Kerr has criticized the Electronic Communications Privacy Act as premised on assumptions that "[c]hanging technology and evolving constitutional law have dramatically shifted."[164] Broad drafting that permits expansive statutory interpretation lends itself toward endurance in the face of technological change.[165] Some argue that Congress is better positioned than courts to

---

158 An additional article by Professor Clark Asay addresses informational privacy generally, not intellectual privacy harms specifically. Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321 (2013). However, Asay specifically considers the serious harm to privacy interests in an age when data brokers can craft comprehensive profiles of "[w]here [an individual] likes to eat, where he was throughout the day, his favorite hobbies, [and] the types of books he reads, among other intimate details." *Id.* at 337 (footnote omitted).

159 Cohen, *supra* note 143, at 1037; *see also* Asay, *supra* note 158, at 342; Jennifer Elmore, Note, *Effective Reader Privacy for Electronic Books: A Proposal*, 34 HASTINGS COMM. & ENT. L.J. 127, 140 (2011) (arguing that the ECPA should be amended to prevent reader information from being "disclosed without a search warrant or court order").

160 Cohen, *supra* note 143, at 1037–38; Elmore, *supra* note 159, at 140.

161 Cohen, *supra* note 143, at 1038.

162 Asay, *supra* note 158, at 351.

163 *See, e.g.*, Brookman, *supra* note 75, at 365 (citing, among other cases, *In re* Google, Inc. Privacy Policy Litig., No. C-12-01382, 2013 WL 6248499, at *13 (N.D. Cal. Dec. 3, 2013)).

164 Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 378 (2014).

165 *See* Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 533–34 (2013) ("[M]any of [Congress's] most successful statutes have endured largely because of vague terms that can be adapted by judicial officials to apply to changed circumstances, suggesting that courts have their own adeptness in keeping up with the times.").

determine how best to deal with privacy threats posed by advancing technology.[166] This may be true, but Congress inconsistently amends privacy statutes in response to technological change — the Family Educational Rights and Privacy Act[167] (FERPA) and the Consumer Credit Protection Act[168] (CCPA) have been updated, while the Electronic Communications Privacy Act of 1986[169] (ECPA) remains largely unchanged.[170] In light of this variable pattern, reader privacy legislation should not be drafted with the expectation that Congress will find the political will to amend it after every paradigm-shifting product launch. Rather, it ought to be drafted to evolve with the times and to withstand potential doctrinal obstacles.

The VPPA's flexibility over time and technology, in addition to its consistent ability to afford plaintiffs standing, suggest that with some tweaks and more careful drafting, the statute could serve as a model for broader protection of records of expressive consumption. First, outside the law enforcement context, the Act bars providers of expressive material from nonconsensually disclosing information identifying the material's consumer.[171] The Act also requires government actors seeking such records or related identifying information to obtain a warrant[172] and provides a clear statutory exclusionary rule[173] not commonly found in the United States' slate of sector-specific privacy statutes.[174] Second, the Act permits the nonconsensual disclosure to parties other than law enforcement only when such disclosure is made to collect a debt, fulfill an order, process a request, or transfer ownership.[175] In addition, the Act's retention provision, though it provides a generous one-year grace period,

---

166 *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 859 (2004). Kerr, however, limited his preference of congressional enactment over interpretation-driven evolution to the criminal context, acknowledging that judges can tailor decisions to technologies Congress could not have foreseen and that judges are not as susceptible to interest group capture. *Id.* For a reader privacy law potentially applicable to both civil and criminal contexts, a law establishing a bright-line procedural rule for law enforcement but otherwise offering broad protection against disclosure could thread the needle.

167 20 U.S.C. § 1232g (2012).

168 Pub. L. No. 90-321, 82 Stat. 146 (1968) (codified as amended in scattered sections of 15 and 18 U.S.C.).

169 Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

170 *Cf.* Murphy, *supra* note 165, at 533 (observing that "although Congress has demonstrated some willingness to amend and enact laws that reflect contemporaneous concerns, it has also demonstrated a stubborn resistance or woeful incapacity to rectify obviously flawed and outdated provisions" and that "important statutory distinctions in the ECPA have notoriously been rendered obsolete with the passage of time").

171 *See* 18 U.S.C. § 2710(b)(1) (2012).

172 *Id.* § 2710(b)(2)(C).

173 *Id.* § 2710(d).

174 Murphy, *supra* note 165, at 506.

175 *Id.* § 2710(a)(2), (b)(2)(E).

embodies the desired purpose-limitation principle.[176] Third, the VPPA's original iteration required case-by-case consent to disclosure of video watching history and related identifying information.[177] Fourth, as discussed in section A.2, the VPPA has managed to avoid the standing obstacles that have limited the practical effectiveness of other privacy statutes. Moreover, in a civil action, the Act provides for statutory damages, as well as punitive damages and reasonable attorney's fees for prevailing plaintiffs.[178] Finally, the VPPA's broad language means that technological change has not narrowed its scope or rendered its protections obsolete, unlike other privacy statutes that retain arbitrary distinctions based on outdated understandings of the tools citizens would use to communicate and receive ideas.[179]

The VPPA's enacting Congress recognized the close link between the First Amendment and reader privacy as well as video privacy, with one Senator noting: "It is nobody's business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy watch on television or read or think about when they are home."[180] In fact, the enacting Congress considered extending protection to books, "recognizing that there is a close tie between what one views and what one reads," but the Senate Judiciary Subcommittee on Technology and the Law "was unable to resolve questions regarding the application of such a provision for law enforcement."[181] Federal reader privacy legislation modeled on the Video Privacy Protect Act, then, is an opportunity to correct the Act's original sin.

---

176 *See id.* § 2710(e).

177 *See* McGeveran, *supra* note 29, at 17 & n.12 (criticizing the departure from the Act's original language, which required "the informed, written consent of the consumer [to be] given at the time the disclosure is sought," *id.* at 17 n.12 (quoting 18 U.S.C. § 2710(b)(2))).

178 § 2710(c)(2).

179 Murphy, *supra* note 165, at 533 ("To the extent that statutes do maintain flexibility, such flexibility results as often from careful (or fortuitous) drafting that allows for expansive judicial interpretations as from subsequent amendment. For instance, because the VPPA covers not just 'prerecorded video cassette tapes' but also 'similar audio visual materials,' courts could readily interpret the statute to include DVDs and other materials." (quoting Dirkes v. Borough of Runnemede, 936 F. Supp. 235, 239 n.5 (D.N.J. 1996))).

180 S. REP. NO. 100-599, at 5 (1988) (quoting *Nomination of Robert H. Bork to Be Associate Justice of the Supreme Court of the United States: Hearing Before the S. Comm on the Judiciary*, 100th Cong. 2820 (1987)).

181 *Id.* at 8.

D. Conclusion

In his *Taxonomy of Privacy*, Professor Daniel Solove echoes Professor William Ian Miller by suggesting that privacy is essential to the "production of civilized society"[182] — and more importantly, that human beings need privacy in order to become themselves.[183] It is that notion of privacy — privacy as creating a space for self-discovery and self-production through the consumption of expressive materials — that the VPPA protects. If the window to Judge Robert Bork's soul and the answer to Michael Dolan's question — "But does anyone really know Robert Bork? I mean, really?"[184] — could be found in the judge's rental history or Netflix queue, it is no wonder that *Spokeo*'s holding failed to gut the VPPA.

The fear that *Spokeo* would fundamentally alter the landscape of standing in a way that harmed plaintiffs alleging privacy harms was unfounded, at least in the arena of intellectual privacy. A deeper analysis of why courts have found standing when plaintiffs have sued under the VPPA should reassure privacy scholars, because it reaffirms — as *Spokeo* did explicitly — that intangible harms, including privacy harms, are no less cognizable for being intangible. Concepts of intellectual privacy beyond tort privacy, which has been criticized for its limitations, will remain cognizable after *Spokeo*, since statutory privacy protections remain related, if not identical, "to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[185] Despite some scholarly attempts to lump the VPPA in with consumer protection statutes, the VPPA is not a consumer protection statute at all — it is deeply bound up in the First Amendment and its various self-expression justifications.[186] Against this backdrop, the seemingly amorphous harm, a disclosure without a material threat of identity theft, other economic damage, or even deep psychological distress, is easy to understand. Courts have been grappling with the idea

---

182 Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 537 (2006) (quoting WILLIAM IAN MILLER, THE ANATOMY OF DISGUST 178 (1997)).

183 *Id.*

184 Dolan, *supra* note 2.

185 Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016). Other courts have expanded on the close connection between privacy statutes and their common law antecedents. For example, one court noted that a state video privacy statute modeled on the VPPA presented no special standing obstacles because "the right guaranteed . . . is similar in kind to other privacy rights that were gradually recognized by American courts over the course of the last century, following the publication of Samuel Warren and Louis Brandeis's landmark article *The Right to Privacy*." Perlin v. Time Inc., No. 16-10635, 2017 WL 605291, at *13 (E.D. Mich. Feb. 15, 2017) (citing Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)). Moreover, "precursors to American privacy law can be found in nineteenth century English law," including English cases protecting an individual's expressive materials, such as the etchings in his or her possession. *Id.*

186 *See* Cohen v. California, 403 U.S. 15, 24–25 (1971) (discussing the self-expression rationale for the First Amendment).

that burdens on the First Amendment right chill socially valuable behavior for decades.[187] Though the VPPA does not address itself primarily to state actors, but rather recognizes that private actors could easily become a tool in the government surveillance of the production of ideas, the harm VPPA guards against is so fundamental and so *ordinary* in courts of law, that *Spokeo* has not made a major change.

As the post-*Spokeo* VPPA cases show, the VPPA contains many flaws — but failure to grant standing is the least of them. The VPPA could use redrafting, not to bring the Act into the twenty-first century, but to bring courts clarity. The weaknesses in the VPPA are mostly a matter of statutory interpretation, particularly a cramped judicial notion of what information is personally identifiable. The Act also suffers from a narrow "subscriber" definition and a lack of clarity on who can be held liable under the Act. Ideally, these flaws would be addressed by congressional revision, but in the absence of legislative action, plausible statutory arguments can be made for broader interpretations of these provisions. If targeted redrafting came to pass, the VPPA could prove a broadly useful model to safeguard the reader records left underprotected by the current regime. Of course, as with any statute, whether redress is available under this statute once plaintiffs are through the courtroom door will remain largely a matter of interpretation.

187 *See* Toni M. Massaro, *Chilling Rights*, 88 U. COLO. L. REV. 33, 45–56 (2017).