American University Business Law Review

Volume 6 | Issue 1 Article 5

2017

The Price Of Free Mobile Apps Under The Video Privacy Protection Act

Suzanne L. Riopel
Washington College of Law

COMMENT

THE PRICE OF FREE MOBILE APPS UNDER THE VIDEO PRIVACY PROTECTION ACT

SUZANNE L. RIOPEL*

After the Washington City Paper published Judge Bork's rental history of 146 videos during the Supreme Court nomination hearings in 1988, Congress enacted the Video Privacy Protection Act ("VPPA"). The statute mostly adapted to changing video platforms, but the extent of its protections for smartphone users is questionable. This Comment will argue that the VPPA does not adequately safeguard consumers when app developers or providers allow users to download mobile apps for free. This Comment will discuss the statutory definitions of videotape service provider, consumer, and personally identifiable information ("PII"). It will explain how and why mobile apps collect personal data and what countermeasures the Federal Trade Commission ("FTC") has taken to regulate mobile businesses. The Comment will analyze the legislative history of the VPPA, the issues with the definitions of consumer and PII, and the societal response to privacy intrusions. This Comment will recommend that the FTC issue business guidance, promote consumer awareness, and bring enforcement actions against businesses that fail to protect consumers. This Comment will conclude that while the VPPA serves as the minimum standard to prevent unauthorized disclosures by mobile app providers and developers, new judicial standards and reliance on the FTC are better measures of regulating mobile commerce in this context.

---

* J.D. Candidate 2017, American University, Washington College of Law.

INTRODUCTION

The advent of the smartphone and its mobile applications ("apps") brought technology closer to the most private areas of one's life: users can manage their financial affairs, medical conditions, and dating prospects all in one place. Beyond convenience and efficiency, the smartphone created a new form of entertainment by allowing its users to watch videos clips, television episodes, and movies in the palms of their hands. Since 68% of Americans own smartphones, and 94.5% of all mobile apps downloaded are predicted to be free, consumer privacy concerns attached to these free apps are highly relevant.[1]

In *Riley v. California*,[2] Chief Justice John Roberts emphasized the privacy of a smartphone by describing it as "a digital record of nearly every aspect of [a person's] life from the mundane to the intimate."[3] Subsequently, the U.S. Supreme Court significantly increased the protection of mobile phones by requiring police to obtain a warrant before viewing information stored on an arrestee's cellphone.[4] The extent of permissible government intrusion into personal information is always a hotly contested issue, but businesses in the mobile community deserve more scrutiny because their actions are equally as intrusive and more evasive towards consumers' personal information.

One legislative protection is the Video Privacy Protection Act ("VPPA"), which prohibits a videotape service provider from knowingly disclosing personally identifiable information ("PII") of its consumers to

1. Monica Anderson, *Technology Device Ownership: 2015*, PEW (Oct. 29, 2015), http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015; Connie Guglielmo, *Mobile Apps Won't Lead to Riches for Most Developers*, FORBES (Jan. 13, 2014, 6:32 PM), http://www.forbes.com/sites/connieguglielmo/2014/01/13/mobile-apps-may-not-pave-the-way-to-developer-riches-sales-average-less-than-1250-a-day/#36b332b735d1 (Gartner, Inc. predicts that 94.5% of all mobile apps downloaded will be free apps).

2. 134 S. Ct. 2473 (2014).

3. *Id.* at 2490.

4. *Id.* at 2494–95.

third parties without consent.[5] Some courts view the VPPA as an antiquated law from the "videotape–era" whereas other courts broadly interpret the VPPA as including video platforms, such as online streaming websites and mobile apps.[6] As video technology becomes more advanced, the definitions of videotape service provider, consumer, and PII become more uncertain. In a society where privacy is rapidly eroding, the VPPA stands as one of the last remaining defenses in guarding our private viewing habits.[7]

This Comment argues that the VPPA does not adequately safeguard information linking a consumer's identity to his or her private viewing history when app developers allow users to download mobile apps for free. This Comment discusses the statutory definitions of videotape provider, consumer, and PII. Next, it explains how a mobile app collects data, such as a consumer's personal information and why businesses are encouraged to share that personal information with third parties regardless of whether the consumer consents. This Comment then analyzes the legislative history of the VPPA, the issues with defining consumer and PII, and the societal response to privacy intrusions.

This Comment recommends that the Federal Trade Commission ("FTC") publish business guidance, promote consumer awareness, and continue enforcement actions against businesses who fail to protect consumers. Since another amendment to the VPPA may be unnecessary and easily outdated by new technology, courts should maintain a broad interpretation of videotape service provider, follow the recent trend of rulings on the definition of consumer, and adopt a flexible standard in defining PII. Finally, this comment concludes that while the VPPA serves as the minimum standard to prevent unauthorized disclosures by app developers and providers, new judicial standards and regulatory guidelines are better ways to regulate mobile commerce.

II. HISTORY OF THE VPPA: 1988 ENACTMENT TO 2013 AMENDMENT

Prior to his controversial Supreme Court nomination, Judge Robert Bork stated, "[a]mericans only have the privacy rights afforded to them by direct

---

5. 18 U.S.C. § 2710 (2013).

6. *Compare* M.C.L.A. § 445.1712 (2016), *with* CONN. GEN. STAT. § 53–450 (1988) (effective Jul. 1, 2016) (comparing state–enacted versions of the VPPA that differ on whether the VPPA is expressly limited to videotapes).

7. *The Video Privacy Protection Act: Hearing Before the Subcomm. on Privacy, Technology and the Law of the Comm. on the Judiciary*, 112th Cong. 85–88 (Jan. 31, 2012) (Letter from Director Laura W. Murphy, ACLU to Chairman Al Franken and Ranking Member Tom Coburn) ("As it is currently drafted, the VPPA is in many ways a model statute. While it only covers a narrow class of records, it does so in an exemplary fashion.").

legislation."[8] Ironically, he would have to swallow his own words after a journalist simply asked a video store for Bork's rental history and published it in the *Washington City Paper*.[9] The article raised questions about privacy rights associated with an indivdual's private viewing habits, such as whether a person should be allowed to portray a man's character by the types of videos he privately watches.[10] In response, Congress enacted the Video Privacy Protection Act of 1988 to prevent videotape providers from disclosing a customer's viewing history to a third party without consent.[11] At the time, the statute generally applied to in–person transactions between VHS rental stores like *Blockbuster* and customer information primarily listed on hand–written records.

The purpose of the Act is to prevent videotape service providers from knowingly disclosing their consumers' PII to third parties without consent subject to certain exceptions.[12] Subsequently, videotape service providers could only disclose PII to the consumer, a person who has informed and written consent from the consumer, a person incident to the ordinary course of business, a law enforcement agency pursuant to a warrant, or a person directed by court order. In addition, videotape service providers could also disclose a consumer's name and address if the consumer had an opportunity to refuse the disclosure.[13] Furthermore, court orders in a civil proceeding must show a "compelling need" for the information and consumers must have reasonable notice of the court proceeding with the opportunity to contest the civil claim.[14] An aggrieved consumer may bring a civil action for actual damages up to $2,500 against businesses for unauthorized disclosures within two years from the violation or the date of discovery.[15]

Since 1988, the terms "videotape service provider," "consumer," and "personally identifiable information" within the VPPA have become increasingly vague due to evolving technology. After litigation ensued over the release of customer viewing histories by online streaming providers to social media websites, specifically *Netflix* to *Facebook*,[16]

---

8. MICHAEL DOLAN, *The Bork Tapes Saga*, *in* THE AMERICAN PORCH: AN INFORMAL HISTORY OF AN INFORMAL PLACE (2002).

9. *Id.*

10. *Id.* ("While I stewed in a sudden outbreak of conscience — what if Robert Bork only rented homosexual porn?").

11. Video Privacy Protection Act, Pub. L. No. 100–618, 102 Stat. 3195 (1988).

12. S. REP. NO. 10–599, at 5 (1988).

13. 18 U.S.C. § 2710(b)(2) (2013).

14. *Id.* § 2710(b)(2)(F).

15. *Id.* § 2710(c).

16. No. 5:11–00379, 2012 WL 2598819 (N.D. Cal. July 5, 2012).

business–backed lobbying firms prompted Congress to amend the VPPA in early 2013.[17] This amendment allowed consumers to meet the statutory requirement of giving "informed and written consent" via electronic means that would be valid for a period up to two years or until withdrawn.[18] Allegedly this would simplify the process for businesses without lowering privacy expectations.[19] Although Congress intended the amendment to reflect the realities of the twenty–first century, Congress did not alter the definition of videotape service provider, consumer, or PII, which has left courts to determine the boundaries of those terms.[20]

A. Statutory Definitions

"Videotape service provider" is defined as "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials."[21] Most courts have broadly construed the meaning of "videotape service provider" to include online streaming providers (Netflix, Hulu, and YouTube), DVD and video game kiosks (Redbox), and a variety of mobile apps (USA Today and Cartoon Network).[22]

The online–streaming company, Hulu, contested this broad interpretation by arguing that the VPPA only applies to businesses that rented or sold prerecorded physical video cassettes or other similar audio visual material, and therefore, modern video platforms are excluded from the VPPA.[23] The court, however, rejected this argument because "similar audio visual material" is defined as "text or images in printed or electronic form," and the digital content that Hulu provides falls within that definition.[24]

---

17. *See* OFFICE OF THE CLERK, H.R., http://disclosures.house.gov/ld/ldsearch.aspx (search client name as "Netflix," amount reported as "1," and year as "2013").

18. 18 U.S.C. § 2710(b)(2)(B).

19. Video Privacy Protection Act, Pub. L. No. 112–258, 126 Stat. 2414 (2013).

20. 18 U.S.C. § 2710(a)(4); *see also* Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1253 (11th Cir. 2015) (citing 158 Cong. Rec. H6849–01 (Dec. 18, 2012)).

21. "Similar audiovisual materials" could include short video clips that are popular online and on mobile apps, but no case has decided the issue. A compilation of short video clips, such as Vine videos, could equally be indicative of an individual's private interests, which likely would not be protected based on *Ellis*.

22. *See, e.g.*, Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482 (1st Cir. 2016); Sterk v. Redbox Automated Retail, LLC, 770 F.3d 618 (7th Cir. 2014); *In re* Hulu Privacy Litig., 86 F. Supp. 3d 1090 (N.D. Cal. 2015).

23. Kathryn E. McCabe, *Just You and Me and Netflix Makes Three: Implications for Allowing "Frictionless Sharing" of Personally Identifiable Information under the Video Privacy Protection Act*, 20 J. INTELL. PROP. L. 413, 431 (2013).

24. *See In re* Hulu Privacy Litig., No. C 11–03764 LB, 2012 WL 3282960, at *5–6 (explaining that the plain reading of statutory language on videotapes and similar audiovisual material and the Senate Report focuses on video content regardless of the media format or business model involved).

Furthermore, the Senate Report also states that the scope of the VPPA reaches beyond businesses that primarily offer video content.[25] For example, a department store that sells videotapes would be required to extend privacy protections to transactions involving videos.[26]

Although VPPA claims are generally made against videotape service providers, some courts have allowed lawsuits against a person or an entity that has received personal information from a videotape service provider.[27] For example, in *Amazon v. Lay*,[28] the court allowed a VPPA claim by Amazon against the Department of Revenue for coercing the company to list all names, addresses, and video sales of its North Carolina residents.[29] However, in *Daniel v. Cantrell*,[30] the Sixth Circuit dismissed a VPPA claim made by a criminal defendant against the district attorney's office that requested and received a list of pornographic videos watched by the defendant without a warrant or the defendant's consent.[31]

The VPPA defines "consumer" as "any renter, purchaser, or subscriber of goods or services from a videotape provider," but lately, the definition of the word "subscriber" has been disputed in the context of electronic and mobile commerce when content is available for free.[32] Since the VPPA does not define "subscriber," the court in *Austin–Spearman v. AMC*[33] used the plain meaning of the word and concluded that a person who visits a website to watch videos, without more, is not a subscriber.[34] The court held that a subscriber must have a "deliberate and durable affiliation with the provider, whether or not for payment," which is "generally undertaken in advance and by affirmative action [by the] subscriber" to "supply the provider with sufficient personal information to establish the [on–going]

---

25. *See* S. REP. NO. 100–599, at 13 (1988) (providing example of a golf shop that rents or sells videos).

26. *Id.*

27. *See* Amazon v. Lay, 758 F. Supp. 2d 1154, 1167 (W.D. Wash. 2010) (holding that North Carolina's Department of Revenue violated the VPPA when it required Amazon to disclose personal information about its customers). *But see infra* footnote 28 and accompanying text.

28. 758 F. Supp. 2d 1154 (W.D. Wash. 2010).

29. *Id.* at 1171–72.

30. 375 F.3d 377 (6th Cir. 2004).

31. *See id.* at 381–84 (finding that the video store defendants were the only proper parties, even though they were complying with the district attorney's office's request).

32. 18 U.S.C. § 2710(a)(1) (2013); Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1255 (11th Cir. 2015) ("The VPPA does not define the term 'subscriber,' and we, as a circuit, have yet to address what that term means. The few districts courts that have weighed in on the issue appear to be divided.").

33. 98 F. Supp. 3d 662, 669 (S.D.N.Y. 2015).

34. *Id.* at 669.

relationship."[35] In *Ellis v. Cartoon Network*,[36] the Eleventh Circuit considered nearly identical factors of subscribership as the court in *Austin-Spearman* in holding that a person who downloads a free mobile app, without more, is not a subscriber.[37] *Ellis* analogized downloading a free app to marking a website as a favorite within your Internet browser because "a user is free to delete the app without consequences whenever he likes and never access the content again."[38] In *Yershov v. Gannett Satellite Info. Network, Inc.*,[39] the USA Today app user did not pay, register, make any commitment, receive emails, or receive access to restricted content.[40] However, since the app automatically sent the defendant's Android ID, GPS location, and the title of the watched video, the First Circuit reasoned that the user provided sufficient personal information to fall within the definition of subscriber, even though arguably he did not provide the information; the app simply took it from him.[41]

Furthermore, PII includes "information which identifies a person as having requested or obtained specific video materials or services from a videotape service provider."[42] A uniform definition of PII does not exist[43] and the VPPA does not define the boundaries of PII.[44] Some courts have construed PII as information that identifies a specific person and links that specific person to his or her viewing history.[45] Generally, courts do not dispute that a person is identifiable by name and address, social security

35. *Id.* at 668–69.

36. 803 F.3d 1251, 1255 (11th Cir. 2015).

37. *See Ellis*, 803 F.3d at 1257 (affirming the dismissal of a VPPA claim because the mobile app user did not register, pay, provide personal information, or access exclusive content).

38. *Id.*

39. 104 F. Supp. 3d 135 (D. Mass. 2015), *rev'd on other grounds*, 820 F.3d 482 (1st Cir. 2016).

40. *Id.* at 137–138.

41. *Id.* at 489.

42. 18 U.S.C. § 2710(a)(3) (2013).

43. *See* Paul Schwartz & Daniel Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1828–32 (2011) (comparing VPPA, Gramm–Leach–Bliley Act, and Children's Online Privacy Protection Act).

44. 18 U.S.C. § 2710.

45. *See* Robinson v. Disney Online, No. 14–CVn4146, 2015 WL 6161284, at *3 (S.D.N.Y. Oct. 20, 2015) (referring to the Eleventh Circuit and U.S. District Courts in Georgia, New Jersey, and Washington). *But see* Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 145 (D. Mass. 2015) ("[T]he conclusion that PII is information which must, without more, itself link an actual person to actual video materials is flawed.") (internal quotations omitted), *rev'd on other grounds*, 820 F.3d 482 (1st Cir. 2016).

number, and date of birth.[46] Most litigation is about whether a specific person is identifiable from an Internet–specific or a device–specific identity, and whether a sufficient nexus exists between that identity and a video that the user watched.[47] Thus far, courts have held that usernames, IP addresses, and streaming media device players' identification number, without more, does not identify individual persons to their viewing history.[48] Some courts have held that PII is information that by its nature identifies an individual or video and not a numeric or alphanumeric code.[49] Although many numeric and alphanumeric codes can be traced to an individual (e.g. a social security number), courts are looking for a more tangible, immediate link.[50]

For example, Hulu wrote its own code for its watch pages to allow a browser to properly display videos on the video player.[51] Each watch page includes a Facebook "Like" button, and when a Hulu user visits a watch page, the code sends a request to Facebook to load the button.[52] If a user logged into Facebook within the past month, his Facebook ID and the title of the video he was watching would be sent directly to Facebook in the form of a "c_user" cookie and URL.[53] Although the combination of this information is PII, the district court held that no VPPA violation occurred because Hulu sent the user's identity and video material separately (albeit simultaneously) to a social media website.[54] Since Facebook did not receive the two pieces of information in the same transmission, which would have implied a connection between the user's identity and video material, the court held Hulu could not be liable under the VPPA unless it knew that Facebook was reverse engineering PII.[55]

---

46. *See* 18 U.S.C. § 2710(b)(2)(D) (consumer's name and address, if the videotape service provider did not provide notice and an opportunity for the consumer to refuse disclosure); *Yershov*, 820 F.3d at 486 (social security number); *see generally In re* Pharmatrak, Inc., 329 F.3d 9, 18 (1st Cir. 2003) (date of birth).

47. *See, e.g.*, Robinson v. Disney Online, 152 F. Supp. 3d 176, 179–80 (S.D.N.Y. 2015); *In re* Hulu Privacy Litig., 86 F. Supp. 3d 1090, 1095–97 (N.D. Cal. 2015).

48. *See Robinson*, 152 F. Supp. 3d at 184 (online streaming media device's serial number); *In re* Nickelodeon Consumer Privacy Litig., No. 15–1441, 2016 WL 3513782, at *20 (3d Cir. Jun. 27, 2016) (an IP address).

49. *See Robinson*, 152 F. Supp. 3d at 184 (holding that an anonymized device serial number, unlike a name or address, does not itself identify a particular person).

50. *See Nickelodeon*, 2016 WL 3513782, at *15–20.

51. *Hulu*, 86 F. Supp. 3d at 1092.

52. *Id.* at 1093.

53. *Id.* at 1093–94.

54. *Id.* at 1096.

55. *Id.* at 1097.

B. Explaining the Technology: How Do Mobile Apps Reveal Personal Information to Third Parties?

Some background on the mechanics of smartphones, mobile apps, and the Internet is necessary to understand the gravity of the potential privacy harms posed by such technology. Smartphones are sold with some pre–installed mobile apps, and the rest are available in app stores owned by mobile operating systems, such as: Apple iOS, Google Android, and Windows Phone OS.[56] When a user pays for a mobile app, the purchase cost is divided between the app provider and the app developer.[57] Since developers may want to provide apps as inexpensively as possible to increase the volume of purchasers, they often choose a "freemium" business model.[58] In a "freemium" business model, when a user downloads a mobile app for free, app developers earn money from upgrade costs, in–app purchases, sponsorship, and advertisements.[59] Advertisers often offer to pay and supply app developers with a software code that properly displays the ad, but the code also collects data from the user's phone and transmits it back to the advertiser.[60]

A common misconception among consumers is that they remain anonymous by not registering or expressly disclosing personal information within a mobile app. Each mobile phone is assigned a unique mobile identification number ("MIN"), which its owner cannot change or opt out of being tracked.[61] A smartphone can identify its real time geographic location by cell–site data (identifying radio cell towers nearest to the device), GPS (receiving radio signals from satellite systems in geosynchronous orbit), and wireless geolocation (comparing access points used to connect to the internet against a database of known routers).[62] The only way to disable all geolocation technologies is by turning off the

---

56. *See* FTC, UNDERSTANDING MOBILE APPS, http://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps#privacy (last visited Feb. 4, 2016).

57. *See generally* Tristan Louis, *How Much Do Average Apps Make?*, FORBES (Aug. 10, 2013, 5:30 PM), http://www.forbes.com/sites/tristanlouis/2013/08/10/how-much-do-average-apps-make (referring to Apple and Google paying $5 billion and $900 million, respectively, to app developers in 2012).

58. *See* FTC, *supra* note 56.

59. *Id.*

60. *See generally* Wei Meng ET AL., *The Price of Free: Privacy Leakage in Personalized Mobile In–App Ads*, GA. INST. TECH., 1, 3 (2016) (explaining that advertisers partner with app developers to provide in–app advertising, which collect user information like demographics and geolocation, in exchange for payment).

61. Nancy King, *Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices*, 60 FED. COMM. L. J. 229, 243 (2008).

62. *In re* Smartphone Data Application, 977 F. Supp. 2d 129, 137 (E.D.N.Y. 2013).

smartphone.[63] Yet, Pew Research Center reported that 83% of adult smartphone users rarely, if ever, turn off their phones.[64] In 2010, nearly all of the top fifty iPhone and Android apps including apps that contained video content transmitted a person's MIN and location to third parties.[65] By 2013, the FTC found that nearly 60% of apps collected geolocation, contacts, call logs, unique identifiers, and other personal information stored on a mobile phone, and those apps later transmitted that information to third parties.[66] The market for the mass collection of personal data, known as the "big data industry," thrives on selling consumer data to businesses who want to efficiently target their sale efforts to realize a better return on their marking investment.[67] In the words of former Path CEO David Morin, uploading phone contacts from users' phones to company servers is referred to as "an industry's best practice."[68]

C. Federal Trade Commission Efforts to Regulate Mobile Businesses

The Federal Trade Commission ("FTC") is the primary federal administrative agency that regulates business practices involving the use, disclosure, or access to personal data on mobile phones.[69] While the VPPA provides a remedial measure, the FTC has the authority to investigate and

---

63. *Id.* at 138.

64. Lee Rainie & Kathryn Zickuhr, *Americans' Views on Mobile Etiquette: Always on Connectivity*, PEW (Aug. 25, 2015), http://www.pewinternet.org/2015/08/26/chapter-1-always-on-connectivity ("Most smartphone owners say they rarely (47%) or never (36%) turn their phones off").

65. *See What They Know — Mobile*, WALL ST. J. (Dec. 18, 2010, 12:01 AM), http://blogs.wsj.com/wtk-mobile (reporting the results of a study by technology consultant David Campbell).

66. *FTC Report Faults Mobile App Makers on Privacy*, FRANKFURT KURNIT KLEIN & SELZ, PC (Jan. 7, 2013), http://fkks.com/news/ftc-report-faults-mobile-app-makers-on-privacy.

67. *See generally* ADAM TANNER, WHAT STAYS IN VEGAS: THE WORLD OF PERSONAL DATA — LIFEBLOOD OF BIG BUSINESS — AND THE END OF PRIVACY AS WE KNOW IT (2014).

68. Nick Bilton, *Disruptions: So Many Apologies, So Much Data Mining*, N.Y. TIMES (Feb. 12, 2012, 11:00 AM), http://bits.blogs.nytimes.com/2012/02/12/disruptions-so-many-apologies-so-much-data-mining.

69. *See* King, *supra* note 61, at 247. Note the D.C. Circuit June 2016 decision may allow for the Federal Communications Commission ("FCC") to regulate consumer privacy concerns. *See* U.S. Telecom Ass'n v. FCC, No. 15–1063, 2016 WL 3251234 at *699, *716 (D.C.C. 2016) (reclassifying internet service providers (ISPs) as offering telecommunications services and classifying mobile broadband service as a "commercial mobile service" subjected to common carrier regulations); 15 U.S.C. § 45(a)(2) (2006) (prohibiting the FTC from regulating common carriers). However, U.S. Telecomm has filed a petition for an *en banc* hearing of the case and may appeal to the the United States Supreme Court to reverse the D.C. Circuit's ruling, which will allow the FTC to have continued jurisdiction over mobile app consumer privacy concerns.

prosecute businesses for unfair or deceptive business practices.[70] Unfair or deceptive business practices are "likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[71]

In the past few years, the FTC has pursued app providers and developers for violating consumer protections: Apple and Google each paid out $32.5 million and $22.5 million in settlements.[72] The FTC also seeks to prevent consumer protection violations through business guidance, consumer awareness, and policy recommendations.[73] For businesses, the FTC reports establish a privacy framework by recommending that companies have a privacy policy, collect information only necessary for the operation of the mobile app, and/or seek affirmative consent before collecting and sharing information.[74] For consumers, the FTC provides general strategies for protecting personal data by hosting public workshops aimed at raising privacy awareness by discussing mobile device tracking and big data.[75]

III. PAYING PRIVACY FOR FREE APPS

Privacy is governed by federal and state laws, enforced by federal agencies, and self-regulated by the industry. This Section will analyze the legislative history of the VPPA, issues the statutory definitions of consumer and PII, and the societal response to privacy intrusions.

A. Legislative History of the VPPA

The legislative history of the VPPA demonstrates strong concerns about preserving the confidentiality of an individual's private viewing history regardless of the business model or media format involved. The VPPA followed a string of federal statutes intended to protect privacy interests: Fair Credit Reporting Act of 1970, Privacy Act of 1974, Electronic Funds Transfer of 1980, Cable Communications Policy Act of 1984, and

---

70. 15 U.S.C. § 45(a) (2006).

71. *Id.* § 45(n).

72. *See* FTC Enforcement, https://www.ftc.gov/enforcement/cases-proceedings (search "Apple Inc.," click the only available case, and view "Decision and Order" then search "Google Inc.," choose the federal case, and view the district court order).

73. *See Privacy & Data Security Update*, FTC, https://www.ftc.gov/reports/privacy-data-security-update-2015 (last visited Feb. 4, 2016).

74. Christopher G. Cwalina ET AL., *Mobile App Privacy: The Hidden Risks*, HOLLAND & KNIGHT (2013) (referring to FTC, *Protecting Consumer Privacy in an Area of Rapid Change* (2012) and FTC, *Marketing Your Mobile App: Get it Right From the Start* (2013)).

75. *See* Matthew Hettrich, *Data Privacy Regulation in the Age of Smartphones*, 31 TOURO L. REV. 981, 985–86 (2015).

Electronic Communication Privacy Act of 1986.[76] These statutes embodied a central principle that information obtained for one purpose should not be used for an unintended purpose without consent.[77] The American Civil Liberties Union ("ACLU"), the Video Software Dealers Association ("VSDA"),[78] and the Direct Marketing Association ("DMA") briefed Congress on the importance of the privacy legislation in the advent of computers, "which we are forced to turn over an enormous quantity and variety of personal information in exchange for doing business."[79] Rather than focus on a specific video format or medium, the opening statement of S. 2361 expressed that the First and Fourth Amendments protect the "freedom to obtain information from whatever source and whatever medium" from unauthorized and unconsented intrusions.[80] When private and public actors reveal or share a consumer's identifiable information with content–based transactions, they affect a consumer's freedom of choice by increasing the risk that his interests will negatively reflect on his identity or character.[81] If a consumer perceives that the benefit of a transaction is outweighed by the risk that the transaction will become publicly known, then the resulting effect may be that "individuals are chilled in their pursuit of ideas and their willingness to experiment with ideas outside of the mainstream."[82]

B. Issues with Defining Consumer and PII

Another amendment to the VPPA is not a permanent solution because applying the statutory definitions of subscriber and PII are inherently problematic in the context of technology. If Congress amended the VPPA or courts broadened "subscriber" to include unregistered mobile app users, then the word "consumer" may have little difference from the word "any

---

76. *See Video and Library Privacy Protection Act of 1988: HEARING ON H.R. 4947 and S. 2361 Before the H. Comm. on the Judiciary*, 100th Cong. 20–21 (1988) [hereinafter *VPPA of 1988*] ("Beginning in 1970 with the passage of the [FCRA] and ending with last Congress with the [ECPA], the Congress has shown its concern with the expanding computerization of our society and the protection of each and every individual's 'right to be let alone.'").

77. *See generally* S. REP. NO. 10–599, at 2–3 (1988) (describing the purposes behind the privacy statutes enacted from 1970–1988).

78. In 2006, VSDA merged with Interactive Entertainment Merchants Association to form the Entertainment Merchants Association. *See* EMA History, http://www.entmerch.org/about-ema/ema-history.html (last visited Aug. 23, 2016).

79. *VPPA of 1988*, *supra* note 76, at 54.

80. *Id.* at 22.

81. *Id.* at 41 ("Even today, there are people in every community who believe that a person's interest in a subject must reflect not merely his intellectual interests, but his character and attitudes.")

82. S. REP. NO. 10–599, at 7 (1988) (statement by American Civil Liberties Union).

person" within the statute,[83] and legislative bodies may be hesitant to amend its definition.[84] To trigger VPPA protection, a mobile app user must fall within the definition of "consumer" as "any renter, purchaser, or subscriber of goods or services from a videotape provider."[85] Under this definition, a user, who uses a free mobile app to view video content, is neither a renter nor a purchaser; he is only protected if he falls within the meaning of a subscriber.[86]

A subscription–based mobile app is a business model that offers more than the basic version, which is usually free and ad–supported, and sells a premium version that allows full access to content at a monthly or annual fee.[87] Under this business model, free mobile app users would either have to upgrade to a premium version or register to be a subscriber under the VPPA.[88] *Austin–Spearman*, *Ellis*, and *Yershov* considered payment, registration, access to restricted content, commitment, expressed association, and delivery as factors of subscription.[89] However, the last four factors are misleading because they require payment or registration. A user is almost always required to pay before accessing restricted content.[90] A user's commitment or expressed association to a mobile app or the company that owns the app is evidenced by a financial commitment or

---

83. Austin–Spearman v. AMC Network Entm't LLC, 98 F. Supp. 3d 662, 670 (S.D.N.Y. 2015).

84. *See generally* Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1256–57 (11th Cir. 2015) ("Congress could have employed broader terms in defining 'consumer' when it enacted the VPPA (e.g., 'user' or 'viewer') or when it later amended the Act (e.g., 'a visitor of a web site or mobile app'), but it did not.").

85. 18 U.S.C. § 2710(a)(1) (2013).

86. *See supra* notes 30–36 and accompanying text.

87. *See* Mark Hoelzel, *Subscriptions are Enjoying a New Prominence as a Revenue Engine for Digital Content and Apps*, BUS. INSIDER (Jul. 7, 2015, 2:35 PM), http://www.businessinsider.com/subscriptions-for-app-and-website-revenue-2015-3 ("Many digital media companies have embraced monthly and annual subscriptions. The business model allows digital media companies to provide a premium experience that offers more than the basic, often ad–supported service level."); *see also* Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 148 (D. Mass. 2015) (discussing paid, free, and subscription apps), *rev'd on other grounds*, 820 F.3d 482 (1st Cir. 2016).

88. *See Austin–Spearman*, 98 F. Supp. 3d at 669 ("'Subscription' entails an exchange between subscriber and provider whereby the subscriber imparts money and/or personal information . . . .").

89. *See Yershov*, 104 F. Supp. 3d at 147; *Ellis*, 803 F.3d at 1256; *Austin–Spearman*, 98 F. Supp. 3d at 669.

90. After reading a limited number of free articles, NY Times and WSJ require that the user pay a subscription before accessing more articles. *See Subscribe Now*, N.Y. TIMES (last visited Sept. 14, 2016), http://www.nytimes.com; *Subscribe Now*, WALL ST. J (last visited Sept. 14, 2016), https://buy.wsj.com/wsjpstlabor16/?inttrackingCode=aaqnz4za&icid=WSJ_ON_PHP_ACQ_NA.

registration.[91] Delivery under the subscription–based business model is "an individual making periodic payments . . . for delivery of magazines, newspapers, or other content," or a person who adds his personal information to a company's mailing list to receive or contribute to its contents.[92]

The basic version of free mobile apps do not always prompt users for registration, and without registration, the circuits are split about whether a relationship can exist between the user and the mobile app or the company that owns it.[93] Even if a free mobile app requires signing up or logging in, users often have the option to login using their Facebook or Google accounts.[94] In the context of the VPPA, courts have not yet considered whether signing in with a Facebook or Google account is considered the equivalent of registration. Whether courts adopt such a viewpoint will depend upon the user having a "deliberate and durable affiliation" with the mobile app. If signing in with a Facebook or Google account allows the mobile app to access enough personal information to identify a specific person (i.e. name, date of birth, location, e–mail address, and contacts), then the user is likely a subscriber.[95] An added complexity is when a user chooses not to login but has recently logged into Facebook, and the software code transmits his Facebook ID and the title of the watched video without his knowledge.[96] In this situation, a user may be interpreted as having no "deliberate and durable affiliation" with the mobile app because the user, himself, did not log in.[97] When a mobile app allows unregistered

---

91. *See Ellis*, 803 F.3d at 1257 ("[P]laintiff did not make any [financial] commitment or establish any relationship that would allow him to have access to exclusive or restricted content.").

92. *See Yershov*, 104 F. Supp. 3d at 147.

93. *Compare id.* (explaining that once downloaded, the free USA Today app did not prompt the user to sign up or log in, but the First Circuit held that the user was a subscriber because he established a relationship or commitment to the USA Today when the app took his Android ID, GPS location, and the title of the watched video) *with Ellis*, 803 F.3d 1251 (stating that the free Cartoon Network app did not require the user to sign up or log in, and even though the app transmitted the user's Android ID and the title of the watched video, the Eleventh Circuit held that the user was not a subscriber because he had no ongoing relationship with Cartoon Network).

94. *See Austin–Spearman*, 98 F. Supp. 3d at 664 ("[S]ites can include a 'Facebook Login,' which lets visitors log into a website using their Facebook credentials.").

95. *See id.* at 669 ("[A] subscriber's deliberate and durable affiliation with the provider . . . require[s] some sort of ongoing relationship between provider and subscriber, one generally undertaken in advance and by affirmative action on the part of the subscriber, so as to supply the provider with sufficient personal information to establish the relationship and exchange.").

96. *Id.* at 664.

97. *See id.* at 670 (rejecting the defendant's proposition that when a website can access information about a user, who previously logged into Facebook albeit not

users to view free content and does not provide notice to a user that by not registering he waives VPPA protection, these websites and mobile apps can share PII to third parties without violating the VPPA.[98]

Courts apply the same analysis of "subscriber" for consumers who access content between their computer, tablet, phone, and other devices, which is problematic.[99] Many companies use cross–device tracking that involves two techniques: (1) "deterministic" linking based on information a user provides to a device, such as an email account, and (2) "probabilistic" linking based on inferences from information that the user has no control over, such as shared IP addresses between two devices that are consistently used together in the same location.[100] For example in *Ellis*, a user watched a video, and the app sent the user's Android ID and the title of the video, without consent, to a third party analytics company, who had the ability to track the user across devices.[101]

The current definition of PII is identical to its previous version, which is unhelpful in resolving disputes over Internet–specific and device–specific identities.[102] As a standard, the definition remains open and flexible to new technological developments.[103] For example, VCR and VHS tapes became affordable in the 1980s, but DVDs became the dominant medium by the late 1990s.[104] Now, online streaming is gaining traction against DVDs and cable television with Netflix alone reporting 43.2 million subscribers.[105] Since video platforms tend to phase out with new technology, the legislature could amend the definitions in the VPPA, but such amendments

---

through the website itself, he or she is a subscriber). *But see Yershov*, 104 F. Supp. 3d at 147.

98. *See id.* at 671 (dismissing VPPA claim).

99. *See* Eichenberger v. ESPN, Inc., No. C14–463 TSZ, 2015 WL 7252985, at *1, *2 (W.D. Wash. May 7, 2015).

100. *See* FTC Cross–Device Tracking Workshop (Nov. 16, 2015), https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking (click "video," "Part 1," and "transcript").

101. *See* Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1254 (11th Cir. 2015) ("Bango[, an analytics company,] uses Android IDs 'to identify and track specific users across multiple electronic devices, applications, and services.'").

102. *Compare* 18 U.S.C. § 2710 (2013), *with* Video Privacy Protection Act, Pub. L. No. 100–618, 102 Stat. 3195.

103. Schwartz & Solove, *supra* note 43, at 1829.

104. *See* Johnnie L. Roberts, *The VCR Boom: Prices Drop as their Popularity Grows*, WALL ST. J. (Sept. 22, 1985).

105. *See* Christopher Palmeri, *U.S. DVD Sales Continue to Slide as Digital Viewing Soars*, BNA (Jan. 6, 2015, 11:46 AM), http://www.bloomberg.com/news/articles/2015-01-06/u-s-dvd-sales-continue-to-slide-as-digital-viewing-soars; Scott Moritz & Gerry Smith, *Pay–TV Losing 300,000 Users is Good News Amid Cord–Cutting*, BNA (Oct. 19, 2015, 11:39 AM), http://www.bloomberg.com/news/articles/2015-10-19/pay-tv-losing-300-000-customers-is-good-news-in-cord-cutting-era.

would serve for a limited amount of time.[106] If PII is defined too narrowly, it will fail to protect privacy interests because new technology will render the statute irrelevant and obsolete.[107] Conversely, a broad definition of PII could encompass too much information, which may blur the distinction between PII and non–PII.[108]

The problem with an open–ended definition is that it fails to differentiate PII from non–PII. The definition simply states that PII "includes information which identifies a person as having requested or obtained specific video materials or services."[109] In the context of smartphones, a mobile identification number in isolation does not reveal its user's viewing history unless pieced together with other information.[110] When a business sends a user's MIN to an analytics company, however, that company can automatically link the MIN to a specific person and across multiple devices.[111] *In re Hulu Privacy Litigation*[112] held that a business is liable if it disclosed both the user's MIN and a correlated reference table to the analytics company — but is not liable if the business only disclosed the MIN and the analytics company had a reference table of their own.[113]

One method of distinguishing between PII and non–PII is comparing the consumer's identity to traditional notions of personal information, such as comparing MIN as more private than a residential address but not akin to a name.[114] However, when courts are "on the fence" about categorizing a term as PII because they do not think it is readily apparent that the information can identify a specific person, courts will often classify the term as non–PII.[115] The Tenth Circuit reasoned that when a statute

---

106. *See generally* Schwartz & Solove, *supra* note 43, at 1827.

107. *See id.*

108. *See id.*

109. 18 U.S.C. § 2710(a)(3) (2013).

110. *See* Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 142 (D. Mass. 2015).

111. *See id.* at 146 (discussing that third parties may have access to databases that link Android IDs to specific persons); Ellis v. Cartoon Network, 803 F.3d 1251, 1254 (11th Cir. 2015) (referring to the district court's analysis).

112. 86 F. Supp. 3d 1090 (N.D. Cal. 2015).

113. *Id.* at 1097 (requiring proof that the recipient knew that the company used a code, the recipient is capable of decoding the contents, and the company and the recipient had some mutual understanding that there has been a disclosure).

114. *See Yershov*, 104 F. Supp. 3d at 141, 482 ("It requires no great leap of logic to conclude that the unique identifier of a person's smartphone or similar device — its "address," so to speak — is also PII. A person's smartphone 'address' is an identifying piece of information, just like a residential address.").

115. *See In re* Nickelodeon Consumer Privacy Litig., No. 15–1441, 2016 WL 3513782, at *21 (3d Cir. 2016) ("[I]n our view, personally identifiable information under the [VPPA] means the kind of information that would readily permit an ordinary person to identify a specific individual's video–watching behavior.").

involving PII does not provide an exhaustive definition of the term, the disclosure of a device's unique identification number and user's pay–per–view history is not PII.[116] Instead, the court found that, rather than identify an individual, the disclosure by itself provided "nothing but a series of numbers."[117] As a result, courts may defer to the legislature or make a conservative decision.

Another method of classifying PII is if a person or entity aggregates enough non–PII, what was originally non–PII can become personally identifying.[118] For example, in *Northwestern Memorial Hospital v. Ashcroft*,[119] the court quashed a subpoena for the patient records of women who had undergone partial abortions because it violated privacy rights.[120] Although the hospital redacted the patients' names, Judge Posner expressed concern that "skillful Googlers" would be able to discern a patient's identity by piecing together public information, redacted medical records, and sexual history.[121]

By construing a narrow reading of the word "consumer" with an open–ended definition of PII, the privacy loopholes that remain between the statutory definition and the case law leave free mobile app users open to exploitation. Free mobile app users may be unprotected under the VPPA unless the app requires registration or expressly discloses the types of information it collects and shares prior to use.

C. Societal Response to Privacy Intrusions

Privacy concerns attached to smartphones remain a significant public concern, and both the President and Congress have made efforts to address those concerns. In 2015, President Barack Obama recognized that "consumers feel like they no longer have control over their personal information" and announced a proposal for several new cyber security initiatives including the Consumer Privacy Bill of Rights.[122] In the past

116. *See* Eichenberger v. ESPN, Inc., No. C14–463, 2015 WL 7252985, at *3 (Wash. May 7, 2015) (citing Pruitt v. Comcast Cable Holdings, LLC, 100 F. App'x 713 (10th Cir. 2004)).

117. *Id.* at *3.

118. *See* Schwartz & Solove, *supra* note 43, at 1841–43.

119. 362 F.3d 923 (7th Cir. 2004).

120. *See generally id.*

121. *Id.* at 929 ("Some of these women will be afraid that when their redacted records are made a part of the trial record . . . skillful 'Googlers,' sifting the information contained in the medical records concerning each patient's medical and sex history, will put two and two together . . . [and] expose them to threats, humiliation, and obloquy.").

122. *See* Hettrich, *supra* note 75, at 1008.

few years, Congress has amended the Children's Online Privacy Protection Act ("COPPA")[123] and enacted the Health Information Technology for Economic and Clinical Health ("HITECH") to protect information transmitted over mobile apps.[124]

In a study by UC–Berkeley, 78% of respondents reported that mobile phone data was as private as, or more private than, computer data.[125] Since Edward Snowden revealed NSA's mass surveillance programs in 2013, 25% percent of Americans have reported changing their behavior on technological platforms including mobile phones,[126] but more than 50% of Americans consider it difficult to find tools and strategies to remain private on the Internet or mobile phones.[127] When businesses advocate that consumers should self–regulate their privacy, it results in the average consumer failing to take advantage of technological measures to protect their information.[128] Most companies provide constructive notice at best, and consumers are usually required to "take it or leave it."[129]

Although the Millennial Generation may have broader expectations about what is public information, adults between eighteen and twenty–four are more likely than any other age group to report that data stored on mobile phones is more private than on personal computers.[130] The majority of young adults disapprove of the government collecting data for national security,[131] and 60% of mobile app users have chosen not to install apps that require the user to divulge more personal information than necessary to operate the app.[132]

---

123. *See* COPPA, 16 C.F.R. § 312 (2013) (amending the Rule to apply to commercial websites and online services including mobile apps directed to children under thirteen that collect, use, or disclose personal information from children).

124. *See* HITECH, 42 U.S.C. § 17938 (2009) (increasing penalties for HIPAA violations).

125. Jennifer M. Urban ET AL., *Mobile Phones and Privacy*, BERKELEY CENTER OF L. & TECH. 12 (2012).

126. Mary Madden & Lee Raine, *Americans' Privacy Strategies Post–Snowden,* PEW (Mar. 16, 2015) http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden.

127. Madden & Raine, *supra* note 126.

128. *See* Clark D. Asay, *Consumer Information Privacy and the Problems of Third–Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 334 (2013).

129. *See* Asay, *supra* note 128.

130. *See* Urban, *supra* note 125, at 23.

131. *See* Drew Desilver, *Young Americans and Privacy: It's Complicated*, PEW (Jun. 30, 2013), http://www.pewresearch.org/fact-tank/2013/06/20/young-americans-and-privacy-its-complicated.

132. Monica Anderson, *8 Conversations Shaping Technology*, PEW (Mar. 10, 2016), http://www.pewresearch.org/fact-tank/2016/03/10/8-conversations-shaping-technology.

Consumer awareness and education through unconventional means is a promising solution. For example, the political satirist John Oliver on *Last Week Tonight* has gained recognition for speaking in layman's terms and using humor when educating Americans about complex topics.[133] When the Federal Communications Commission ("FCC") sought public comment on net neutrality rules, John Oliver encouraged his one million viewers to comment on the FCC website.[134] After the episode's release, the FCC received 45,000 comments and 30,000 emails, whereas previous proposals received roughly 2,000 comments.[135] The FCC stated, "[w]e've been experiencing technical difficulties with our comment system due to heavy traffic. We're working to resolve these issues quickly."[136] The FCC ultimately voted in favor of net neutrality.

If privacy violations result in minimal or isolated privacy harms, consumers may consider them offset by the benefit of the free flow of information, which include the advantages of free content, expedited services, and relevant advertising.[137] For example, Josh Mohrer, an Uber executive, used the service's "God mode" to track the movements of journalist Johana Bhuiyan without her permission and emailed her a copy of all of her Uber rides; however, the isolated event did not affect the demand for Uber.[138] In the VPPA context, when content contains sensitive information, the greater the demand is for ensuring that persons or entities privy to or entrusted with that information, such as videotape service providers, do not share that information.[139] For example, if a person watched a documentary on a male–to–female transition, as opposed to a popular film, he may have a higher interest in protecting his viewing

133. *See* Paeste v. Guam, 798 F.3d 1228, 1231 (9th Cir. 2015) (citing to John Oliver's episode on U.S. territories in its opinion); Terrance F. Ross, *How John Oliver Beats Apathy*, ATLANTIC (Aug. 14, 2014), http://www.theatlantic.com/entertainment/archive/2014/08/how-john-oliver-is-procuring-latent-activism/376036.

134. *Last Week Tonight with John Oliver: Net Neutrality*, YOUTUBE (June 1, 2014), https://www.youtube.com/watch?v=fpbOEoRrHyU.

135. Elise Hu, *John Oliver Helps Rally 45,000 Net Neutrality Comments to FCC*, NPR (June 3, 2014, 11:56 AM), http://www.npr.org/sections/alltechconsidered/2014/06/03/318458496/john-oliver-helps-rally-45-000-net-neutrality-comments-to-fcc.

136. Ben Brody, *How John Oliver Transformed the Net Neutrality Debate Once and For All*, BNA POLITICS (Feb. 26, 2015, 10:00 AM), http://www.bloomberg.com/politics/articles/2015-02-26/how-john-oliver-transformed-the-net-neutrality-debate-once-and-for-all.

137. *See generally* Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877 (2000).

138. *See* Katherine Gnadinger, *The Apps Act: Regulation of Mobile Application Privacy*, 17 SMU SCI. & TECH. L. REV. 415, 426 (2014).

139. *See* Jay Stanley, *A Supply and Demand Curve for Privacy*, ACLU (Dec. 15, 2014, 11:15 AM), https://www.aclu.org/blog/freefuture/ supply-demand-curve-privacy.

history from potentially conservative employers.[140] If the price of free apps is allowing a business to collect and share specific identifiers attributable to consumers' viewing history, privacy concerns may influence consumers, depending on the content, to shift to encrypted apps that do not collect information on its users.[141] When business practices become highly intrusive and publicly known or widespread, consumers begin to consider the legitimacy of that business, rather than just price, in choosing between competitors.

IV. FTC, CONSUMER AWARENESS, AND PII FACTORS TEST

The FTC should promulgate a rule stating that a mobile app cannot access a phone's content unless the app requires registration or an express privacy disclosure prior to use and requests consent to access its content.[142] For app developers who choose to use a privacy disclosure, the FTC should work with the mobile app community to standardize the plain language of these disclosures to explain what information is collected, when the information is collected, and why it is collected.[143] Another possibility is for the FTC to consider initiatives that relay information to consumers in an understandable way, such as through television shows that address social and legal issues.[144]

Regulations should require companies that collect PII to present the consumer with notice of the intended third party recipients of such PII and the third parties' proposed uses. While policymakers cannot force a consumer to pay attention to a privacy notice, they can make it more likely for the consumer to do so by requiring notices to be accessible and in a format that attracts more interests from the consumer.[145]

Since amendments to the VPPA are unnecessary or easily outdated by new technology, courts should maintain a broad construction of "videotape service provider," follow the trend of recent rulings on who is a "consumer," and adopt a flexible standard to determine PII.[146] In addition,

---

140. John Vandiver, *Report Finds Army Discriminated Against Transgender Civilian Employee*, STARS & STRIPES (Oct. 21, 2014), http://www.stripes.com/news/report-finds-army-discriminated-against-transgender-civilian-employee-1.310017.

141. Stanley, *supra* note 139. For example, Telegram is an encrypted messaging app that allows users to send, among other things, videos, but these messages have a self-destruct timer.

142. H.R. 4048, 113th Cong. (2014).

143. *See* Asay, *supra* note at 128, at 34.

144. *See* Hettrich, *supra* note 75, at 985–86 (explaining how the FTC promotes public education but no mention of innovative methods).

145. *See generally* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Privacy Harms*, 55 B.C. L. REV. 93 (2014).

146. *See* Schwartz & Solove, *supra* note 43, at 1841.

courts should consider using a factors test to determine whether, given the context, information is PII.

If the plaintiff and the defendant meet the definitions of a "videotape service provider" and a "consumer," respectively, courts should review three factors: (1) the nexus between the alleged personal identifiable information to traditional notions of PII, (2) the consequences of disclosing the alleged personal identifiable information in a modern context, and (3) the proximity between the transfers of information related the consumer's identity and the video's title or description.

First, courts should consider the nexus between the alleged PII and traditional notions of PII. For example, if a complainant claimed that a video provider collected and disclosed a video title and the location of his or her home by accessing location–tracking enabled on her mobile phone, a court may consider the location akin to an address that is traditionally considered PII.[147] Since the location is not attached to other unique information similar to a name or credit card number, a court may also consider the location not private information given that a residential address is publically disclosed.

Second, courts should weigh the consequences of the type of information disclosed. If the information is readily understandable (e.g. a video title or explicit URL) or requires little effort by third parties to piece the information together, courts would be more inclined to consider it PII.[148] Another consideration is whether the type of information is one that society has an interest in keeping private, such as a young woman viewing videos about the physical and emotional effects of having an abortion.[149]

Third, the courts should consider whether the individual's information and the video title or description is transmitted separately or together, and if separately, the length of time between the transmissions. In *Hulu*, the court began this analysis by holding that simultaneously transmitting a user's URL and "c_user" cookie as separate pieces of information to a third party, such as Facebook, did not constitute PII.[150] However, the court did not discuss how much information Facebook could expect to receive at the same time it received information from Hulu.[151] If no other information was received from Hulu at the same time, then Hulu transmitting the two pieces of information separately is no different than transmitting the information together.

---

147. *See* Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 140 (D. Mass. 2015).

148. *See In re* Hulu Privacy Litig., 86 F. Supp. 3d 1090, 1092 (N.D. Cal. 2015).

149. *See generally* Schwartz & Solove, *supra* note 43.

150. *See Hulu Privacy Litig.*, 86 F. Supp. 3d at 1097.

151. *See generally id.* at 1090.

CONCLUSION

The VPPA serves as an important but minimum standard when preventing app providers and developers from collecting and sharing a user's personal information. Although a videotape service provider is prohibited from knowingly disclosing a consumer's PII without consent, recent court decisions favor traditional notions of PII. The VPPA as amended in 2013 does not add any protection for consumers using the Internet or other mobile devices.