MODERNIZING THE VIDEO PRIVACY PROTECTION ACT

*Marc Chase McAllister**

INTRODUCTION

Thomas Sanchez, a twenty-seven-year-old financial planner born and raised in New York City, has just enrolled in graduate school at Columbia University to become a filmmaker. Thomas distinctly remembers the 9/11 attacks and has decided to change careers to focus on creating films depicting the peaceful aspects of the Christian and Muslim faiths.

To develop his thesis, Thomas begins by watching mainstream films that depict the Muslim faith. Over a weekend, Thomas opens a Netflix account and views the following movies in his studio apartment on his Apple desktop computer: Malcolm X, The Kite Runner, American East, Lawrence of Arabia, and The Message. The next day, Netflix provides its advertising affiliate, Adobe Systems Incorporated, with the list of videos watched over the weekend by Netflix user #1853430 (the account number assigned to Thomas), along with that user's Internet Protocol ("IP") address and GPS coordinates at the time each video was viewed. After quickly linking the IP address and GPS coordinates to Thomas Sanchez, Adobe adds this information to its extensive digital dossier on Thomas, which includes his Facebook posts, Google searches, and Internet browsing history.[1] The following weekend, as Thomas is about to embark on a plane to visit his mother in Mexico for her sixtieth birthday celebration, he is removed from the terminal by Homeland Security officers,[2] who demand he turn over his smartphone and password for fear that he might be involved in future terrorist

---

* Marc McAllister is an Assistant Professor of Business Law at Texas State University. He has ten years of law school teaching experience and has completed three federal judicial clerkships. His articles have been published in respected journals such as the Washington and Lee Law Review (forthcoming), Seattle University Law Review, Penn State Law Review, Florida State University Law Review, Cincinnati Law Review, and Case Western Reserve Law Review.

[1] *See* Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 484-85 (1st Cir. 2016) (summarizing complaint's allegations that Gannett, the operator of the USA Today Mobile App, sends to Adobe information regarding video clips its users watched on the app, which Adobe then combines with other information to create user profiles which may include the user's name and address, age and income, household structure, and online navigation and transaction history).

[2] *See* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 92 (2015) (explaining that through programs like PRISM, the NSA legally compels companies like Microsoft, Google, Apple, and Yahoo to provide data on individuals of interest).

attacks due to his "interest" in the Muslim faith.[3] After a two hour search of his phone, Thomas is released. Having missed his plane, Thomas returns home to his apartment, angry and confused.

The Video Privacy Protection Act ("VPPA"),[4] enacted in 1988 after the *Washington City Paper* published Supreme Court nominee Robert Bork's video rental history,[5] was designed "[t]o preserve personal privacy with respect to the rental, purchase, or delivery of video tapes or similar audio visual materials,"[6] thereby protecting the right to privacy in one's movie and video selections.[7] When the VPPA was enacted, consumers obtained movies on VHS cassette tapes.[8] Today, on-demand television and internet streaming allow consumers to watch movies and videos on smart televisions, computers, and cell phones through services such as Netflix.[9] Although "video tapes" are largely a thing of the past, the multiple forms of "similar audio visual materials" that exist today, such as Thomas's Netflix downloads, are arguably subject to VPPA protection.[10] Yet, the VPPA often fails to protect modern forms of video-watching, due in part to the statute's poor

---

[3] *See* Cynthia McFadden et al., *American Citizens: U.S. Border Agents Can Search Your Cellphone*, NBC NEWS (March 13, 2017), https://www.nbcnews.com/news/us-news/traveling-while-brown-u-s-border-agents-can-search-your-cellphone-n732746 (reporting that naturalized citizens and people born and raised on American soil, mostly Muslim, are now routinely subjected to extensive, suspicionless searches of their smartphones at international airports, and that fewer than 5,000 phones were searched in 2015, whereas 25,000 phones were searched in 2016, and 5,000 were searched in February 2017 alone).

[4] Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (1988) (codified as amended at 18 U.S.C. § 2710 (2012)).

[5] *See* S. REP. NO. 100-599, at 5 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342-1; Mollett v. Netflix, Inc., 795 F.3d 1062, 1065 (9th Cir. 2015) (stating that the newspaper detailed 146 films that the Bork family had rented from an area video store). *See also* Andrea Peterson, *How Washington's Last Remaining Video Rental Store Changed the Course of Privacy Law*, WASHINGTON POST (Apr. 28, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/04/28/how-washingtons-last-remaining-video-rental-store-changed-the-course-of-privacy-law/ (reporting that, other than the sheer number of movies Bork and his family had rented over the two-year period, the reporter did not uncover anything too shocking, aside, perhaps, from Hitchcock and costume dramas).

[6] S. REP. NO. 100-599, at 1 (1988). *See also* Video Privacy Protection Act, 18 U.S.C. § 2710(a)(4) (defining the term "video tape service provider" to "mean[] 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").

[7] *See* 134 CONG. REC. 10,259 (1988) (remarks of Senator Patrick Leahy).

[8] *See, e.g.*, Christina Bonnington, *A Surprisingly Number of Americans Still Regularly Use VCRs*, DAILY DOT (Sept. 5, 2017, 8:41 AM), https://www.dailydot.com/debug/us-vcr-usage/.

[9] *See* S. REP. NO. 112-258, at 2 (2012). Netflix is the world's largest subscription service for viewing movies, television programs, and other video content. *See* Mollett v. Netflix, Inc., 795 F.3d 1062, 1064 (9th Cir. 2015). The company launched in 1999 as an online DVD rental service that delivers DVDs through the mail and expanded in 2007 to allow subscribers to stream videos instantly online. *Id.*

[10] *See infra* notes 11-18 and accompanying text.

drafting,[11] its almost thirty-year old language,[12] and strict judicial interpretations of the statute.[13]

For example, although the VPPA protects against disclosure of a consumer's video-watching habits, a consumer may only sue a provider who discloses her "personally identifiable information,"[14] such as her name or address. Recently, however, courts have held that the term "personally identifiable information" does *not* encompass most "static digital identifiers"—like a user's IP address (a number that is assigned each device that is connected to the Internet),[15] or a device's unique device identifier (a sixty-four bit number that corresponds to a particular device)[16]—even though such identifiers allow many third-party data recipients, such as Adobe, to easily identify a particular person as having viewed a certain video.[17] And, this is true even though the VPPA's sponsors quite obviously sought to extend the statute to modern video formats and included language in the statute to accomplish that goal.[18]

The United States has no single, comprehensive law regulating privacy or personal data and instead relies on a patchwork of federal and state laws and regulations, as well as common law principles.[19] Federal laws generally govern specific industries or particular types of data.[20] Unlike the VPPA, many privacy statutes protect the types of identifying information made possible by new technology.[21] For example, the Children's Online Privacy

---

11 *E.g.*, Sterk v. Redbox Automated Retail, LLC, 672 F.3d 535, 538 (7th Cir. 2012) ("The statute is not well drafted."). *See also* Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 486 (1st Cir. 2016) (recognizing that "[t]he statutory term 'personally identifiable information' is awkward and unclear"); *In re* Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 284 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 624 (2017) (stating that "the proper meaning of the phrase 'personally identifiable information' is not straightforward").

12 The VPPA was revised in 2013, but at that time Congress failed to update the definition of "personally identifiable information" in the statute. *E.g.*, *In re Nickelodeon*, 827 F.3d at 287-88.

13 *See* discussion *infra* Part III.

14 *See* Video Privacy Protection Act, 18 U.S.C. § 2710(b)-(c) (2012). *See also Sterk*, 672 F.3d at 538 (discussing the scope of the statute's private right of action).

15 *See In re Nickelodeon*, 827 F.3d at 281.

16 *See id.* at 282 n.124.

17 *See id.* at 281-90.

18 *See infra* notes 100-09 and accompanying text.

19 *See* Mauricio Paez & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Businesses*, 43 N. KY. L. REV. 29, 40 (2016).

20 *See* Dirkes v. Borough of Runnemede, 936 F. Supp. 235, 238 (D.N.J. 1996) (listing various federal privacy statutes that collectively "reflect the Congressional desire to keep an individual's right to privacy apace with advances in technology").

21 COPPA is just one privacy statute that has modernized privacy laws to account for new technologies. The Gramm-Leach Financial Modernization Act, 15 U.S.C. § 6809(4) (2012), which prohibits financial institutions from disclosing "nonpublic personal information" to a nonaffiliated third party, has a similar focus. *See also* 16 C.F.R. § 313.3(o)(2)(F) (2012) (defining "personally identifiable financial information" to include, in part, any information collected through an Internet "cookie"); 34 C.F.R. § 99.3 (2010) (broadly defining the term "personally identifiable information" in the Family

Protection Act ("COPPA")[22] prohibits certain disclosures of a child's "personal information" online,[23] and by statute defines "personal information" to include, among other traditional identifiers, a child's name, physical address, and e-mail address.[24] Through FTC regulations, COPPA's definition of "personal information" also encompasses more modern identifiers, such as "a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier."[25] By giving the FTC power to expand the category of personally identifying information under COPPA, Congress enabled that particular statute to keep pace with evolving technology.[26] The VPPA, however, has not been similarly updated, and is ripe for revision.[27]

This Article explores the four major interpretative issues that have plagued the VPPA in the last few years and attempts to resolve circuit splits on two of those issues with proposed revisions to the statute. First, this Article proposes that the outdated VPPA definition of "personally identifiable information" be replaced with a more modern definition (e.g., similar to the COPPA definition) that encompasses digital identifiers such as IP addresses and unique device identifiers, thereby resolving a circuit split on this issue and ensuring the VPPA protects today's common video formats. Second, this Article proposes that the types of "consumers" the VPPA protects should include those who download and use smartphone apps to view movies and videos, again resolving a circuit split on the issue. Finally, recognizing that not all disclosures of personally identifiable information are equally invasive of privacy, this Article proposes amending the VPPA to increase the penalty for disclosures of personally identifiable information that, like the Robert Bork disclosure, are reasonably likely to be made public.

Part I of this Article examines the data collection practices of modern businesses. Part II summarizes the VPPA's provisions and legislative history. Part III examines recent judicial interpretations of the VPPA on the four most important issues of interpretation concerning the statute. Finally, Part IV sets forth proposed revisions to the statute.

Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2012), to include "indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name," as well as "[o]ther information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty").

22 15 U.S.C. §§ 6501-6506.

23 *Id.* § 6502.

24 *Id.* § 6501(8).

25 16 C.F.R. § 312.2 (2018) (defining "personal information").

26 *See In re* Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 287 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 624 (2017).

27 *Id.* at 287-88.

I. DATA COLLECTION BY BUSINESSES

Every day, Americans provide personal information to businesses with very little understanding or control over how that information is used.[28] Activities that produce information include using a cell phone, shopping for a home or car, making a retail purchase, browsing the Internet, using social media, responding to a survey, entering a sweepstakes, and subscribing to a magazine.[29] According to privacy expert and Harvard Law School Fellow Bruce Schneier, "The overwhelming bulk of [modern data collection] is corporate, and it occurs because we ostensibly agree to it."[30]

Although consumers engage in various online and offline activities that reveal personal information, most corporate data collection today occurs through the Internet, which routinely captures what we read, watch, listen to, and think about (through, for example, our Google searches).[31] Much of that data is actually metadata, the information trail of transactions and communications.[32] With a text message, for example, the content of the text message is data, whereas the addresses of the accounts involved and the date and time the message was sent and received are all metadata.[33] Accordingly, much metadata is simply a by-product of modern computing and communication—"the exhaust of the information age."[34]

Companies often obtain consumer data in exchange for free services.[35] Google, for example, offers free e-mail, web search, and various other services in exchange for its users' data.[36] Once collected, data becomes so valuable that businesses sell it to data brokers,[37] including the types of

---

28 S. REP. NO. 100-599, at 6-7 (1988).

29 *See* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY iv-v (2014), available at https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [hereinafter FTC DATA BROKER REPORT] (reporting information and findings developed through the FTC's issuance of Orders to File Special Reports to nine data brokers pursuant to Section 6(b) of the Federal Trade Commission Act, 15 U.S.C. § 46(b), which sought information about the data brokers' practices starting January 1, 2010, related to the collection and use of consumer data). *See also id.* at 8-9 (describing the business practices of the nine data brokers subject to the FTC's study).

30 SCHNEIER, *supra* note 2, at 55. Schneier uses the term "surveillance," which "is a politically and emotionally loaded term," to capture the notion of "'systematic observation'" inherent in modern-day electronic surveillance. *Id.* at 4.

31 *See id.* at 4, 55.

32 *See id.* at 20.

33 *See id.*

34 *Id.*

35 *See id.* at 57-59. *See also id.* at 62 ("We use systems that spy on us in exchange for services. It's just the way the Internet works these days. If something is free, you're not the customer; you're the product.").

36 SCHNEIER, *supra* note 2, at 58.

37 *See* FTC DATA BROKER REPORT, *supra* note 29, at 1. *See also id.* at 3 (describing "data brokers" as "companies whose primary business is collecting personal information about consumers from a variety

companies who are the recipients of data in recent VPPA cases,[38] who in turn resell it to other companies.[39]

Data brokers use data aggregated from various sources[40]—including data gathered from a user's multiple devices,[41] and even from other data brokers[42]—to build detailed profiles on individual consumers and create potential customer lists, such as persons with a "diabetic focus," "potential inheritors," "expectant parents," and "discount shoppers."[43] These efforts are

---

of sources and aggregating, analyzing, and sharing that information, or information derived from it, for purposes such as marketing products, verifying an individual's identity, or detecting fraud").

38 *See, e.g.*, Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 484 (1st Cir. 2016) (involving smartphone app video-viewing data transmitted by defendant, producer of the USA Today newspaper, to Adobe Systems Incorporated, "an unrelated third party that offers data analytics and online marketing services to its clients by collecting information about consumers and their online behavior"); Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1254 (11th Cir. 2015) (involving smartphone app video-viewing data transmitted by the Cartoon Network to Bango, a data analytics company); Locklear v. Dow Jones & Co., 101 F. Supp. 3d 1312, 1314 (N.D. Ga. 2015) (involving Roku video-streaming data disclosed to mDdialog, an analytics and advertising company that creates user identities and individualized profiles).

39 SCHNEIER, *supra* note 2, at 3, 55.

40 *See* FTC DATA BROKER REPORT, *supra* note 29, at iv, 11 (finding that data brokers collect data from many sources, including bankruptcy information, voting registration, consumer purchase data, web browsing activities, warranty registrations, and other details of consumers' everyday interactions, which they then compile to form a detailed composite of a consumer's life; also noting that "[d]ata brokers do not obtain this data directly from consumers, and consumers are thus largely unaware that data brokers are collecting and using this information").

41 *See* FED. TRADE COMM'N, CROSS-DEVICE TRACKING, ii-2 (2017) (reporting that "third-party companies are tracking consumers with increasing accuracy, correlating user behavior across multiple platforms;" and noting that with cross-device tracking, "[c]ompanies can gather information about consumers across their connected devices, including smartphones, tablets, personal computers, smart televisions, and even smartwatches and other wearables," which they then combine with information about consumers' offline activities).

42 *See* FTC DATA BROKER REPORT, *supra* note 29, at 11-14 (explaining that data brokers primarily obtain information from government sources; other publicly available sources, including social media, blogs, and the Internet; and commercial sources); *id.* at 14 (noting that most data brokers buy or sell information to each other, such that "it may be virtually impossible for a consumer to determine the originator of a particular data element").

43 *See id.* at iv-v, 3; SCHNEIER, *supra* note 2, at 62.

designed to facilitate targeted advertising,[44] but can become quite intrusive on privacy.[45]

Internet surveillance is traditionally accomplished via "cookies," or "persistent identifiers."[46] Cookies were originally designed to remember a website user from visit to visit or click to click.[47] To accomplish this goal, each cookie contains a unique number that allows the site to identify a specific user, which in turn allows the site to find the user's account, keep a shopping cart associated with the user, and remember the user the next time he or she visits the site.[48] Although cookies are inherently anonymous, companies can often correlate them with other information that identifies a particular individual, such as when a consumer uses her credit card to make a purchase online.[49]

After companies realized they could place their cookies on pages belonging to other sites, the "third-party cookie" was born, leading to the tracking of web users across many different sites.[50] The result is a "shockingly extensive, robust, and profitable surveillance architecture"

---

44 SCHNEIER, *supra* note 2, at 61-62. *See* Sense Networks, LINKEDIN, https://www.linkedin.com/company/sense-networks-inc (last visited November 16, 2017) (Sense Networks describes itself as "appl[ying] big science to mobile location data for predictive analytics in advertising," noting that "[t]he company's technology platform receives streaming location data from mobile phones in real-time, processes the data in the context of billions of historical data points, and analyzes it to better understand human activity." Using this approach, the company has "built over 150 million mobile user profiles for use in mobile advertising."). *See also* Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 484-85 (1st Cir. 2016) (summarizing complaint's allegations that defendant Gannett, the operator of the USA Today Mobile App, sends to Adobe information regarding its customers' use of the app and that Adobe takes this and other information gleaned from a variety of sources to create individual user profiles, all of which allow Adobe's clients, such as Gannett, to "accurately target advertisements to its users").

45 *See* SCHNEIER, *supra* note 2, at 49 (explaining how different data sets can be easily correlated and used to generate a detailed profile of information about a person); FTC DATA BROKER REPORT, *supra* note 29, at vii ("Data brokers acquire a vast array of detailed and specific information about consumers; analyze it to make inferences about consumers, some of which may be considered sensitive; and share the information with clients in a range of industries," all of which occurs "behind the scenes, without consumers' knowledge."); Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES, Feb. 16, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (According to a 2012 *New York Times* article detailing how corporations analyze data for advertising purposes, Target Corporation can determine from a woman's buying patterns that she is pregnant and would use that information to send the woman ads and coupons for baby-related items. The story described a Minnesota father who complained to a Target store that Target had sent his teenage daughter baby-related coupons, only to find out later that Target was right.).

46 SCHNEIER, *supra* note 2, at 55-56.

47 *Id.* at 56.

48 *Id.*

49 *See id.* at 58.

50 *Id.* at 56.

permitting specific individuals to be tracked by multiple companies and data brokers virtually everywhere they go on the Internet.[51]

The same type of data mining occurs through smartphones, mostly through apps,[52] which often permit transaction-based data collection and location tracking.[53] The "Angry Birds" app, for example, collects location data even when the app is not being used.[54] This, in turn, has led to mobile tracking services enabling companies to communicate messages tailored to specific consumers based on location.[55]

Often, users have no choice but to permit data collection,[56] although they sometimes have a choice regarding how the data is used. For instance, the VPPA was revised in 2012 to allow consumers to easily share information about their video preferences through social media sites.[57] This amendment allowed consumers to provide one-time consent via the Internet (replacing the previous requirement of written consent for each individual disclosure), which covers a two-year period and enables companies like Netflix to automatically disclose the titles of videos that subscribers watch without receiving fresh consent for each individual disclosure.[58]

Although giving individuals the ability to control what they choose to make public is a step in the right direction, these days consumers often click through most consent requests and ignore the "fine print" regarding a company's privacy policies. Upon download, many cell phone apps request consent to view all accounts on a phone, to track the phone's location, and to track who the user communicates with on the phone, all of which seem unnecessarily invasive.[59] For example, when a smartphone user downloads the "TomTom Sports" app from Play Store and opens the app for the first time, the user is promptly informed that "[TomTom] Sports would like to access [the user's] location," which, the app explains, is necessary "for Bluetooth to work reliably . . . [and] to pair and sync [the user's] TomTom Sports device with the app."[60] After clicking "Ok" (rather than "Cancel"), the

---

51 *Id.*

52 SCHNEIER, *supra* note 2, at 57.

53 *Id.* at 3.

54 *Id.* at 57.

55 FTC DATA BROKER REPORT, *supra* note 2, at 5.

56 For example, when a user logs into Bloomberg Law (bna.com), the user is promptly informed: "This site uses cookies. By continuing to browse the site you are agreeing to our use of cookies." Bloomberg Law, https://www.bna.com, (last visited November 16, 2017).

57 *See* S. REP. NO. 112-258, at 2-3 (2012).

58 *Id.* at 21 (comparing the old and new statutory language); *see also* Video Privacy Protection Act, 18 U.S.C. § 2710(b)(2)(B) (2012); Kathryn Elizabeth 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, 432-34 (2013) (describing the 2012 amendments); Peterson, *supra* note 5.

59 SCHNEIER, *supra* note 2, at 57.

60 TOMTOM GO APP, https://www.tomtom.com/en_gb/sat-nav/sat-nav-app/go-mobile/ (last visited Nov. 16, 2017).

user is then asked to permit TomTom to "access this device's location."[61] Next, the user is informed that "[TomTom] Sports would like to access [her] external storage," which, the app explains, is necessary "to pair and sync [her] TomTom Sports device with the app."[62] After clicking "Ok," TomTom Sports then asks for permission to "access photos, media, and files on [the user's] device," to "make and manage phone calls," to "send and view SMS [text] messages," and to "access [the user's] contacts."[63]

After selecting "Allow" or "Deny" for each of the above questions, the user may then begin the process of pairing a device, such as a GPS-enabled running watch.[64] At this point, the app notifies the user, for the second time, that "[TomTom] Sports would like to access [her] external storage," which, the app reiterates, is necessary for the pairing process.[65] To actually pair a device, the option "Ok" must be clicked, after which the user is again asked to consent to TomTom's access of "photos, media, and files on [her] device."[66] The options "Deny" and "Allow" are again offered, but only the "Allow" selection permits the user's device to be synced with the app; thus, the user must "Allow" to begin using the app in a meaningful way.[67]

The typical app installation process, which is often extensive, can be quite confusing for consumers, and many consumers find it easier to consent to most requests simply to get an app operating as quickly as possible.[68] This is true regardless of whether the company promises to use its customers' data only for specific and legitimate business purposes—some do, but others do not.[69]

---

61 *Id.*

62 *Id.*

63 According to TomTom's Privacy Statement:

> When you install the TomTom Sports phone application, . . . your Android or iOS device may ask you for the following permissions:
> * Access to your Android or iOS address book, phone call history, and text messages. This is required to enable phone notifications for compatible TomTom Sports devices.
> * Access to your location on your Android device. This is required by Android to enable Bluetooth connectivity between your Android device and your TomTom Sports device for information upload.
> * Access to your camera and photos. This is required to enable sharing on social media.
> None of the information accessed above will be sent to TomTom. You can choose to enable access to these features at any time in the settings of your TomTom Sports mobile application.

TOMTOM, PRIVACY STATEMENT, https://www.tomtom.com/en_us/privacy/sports/ (last visited Nov. 16, 2017).

64 TOMTOM GO APP, *supra* note 60.

65 *Id.*

66 *Id.*

67 *Id.*

68 *All Things Considered: Why Do We Blindly Sign Terms of Service Agreements?*, (Nat'l Pub. Radio radio broadcast Sept. 1, 2014, 4:07 PM), https://www.npr.org/2014/09/01/345044359/why-do-we-blindly-sign-terms-of-service-agreements ("We agree all the time to terms for software and websites, and we do it blindly.").

69 Because TomTom operates according to European privacy laws, the company's privacy protections are quite robust relative to other businesses. According to TomTom, the company "will only

Once a smartphone app is installed, a user can usually access detailed terms regarding what types of data are collected by the company and how the company uses that data, often through a link to the company's "Privacy Policy."[70] Although the installation process is less extensive than the TomTom Sports app, the Netflix smartphone app contains an exemplary Privacy Policy that contains detailed information regarding how the company tracks its users' activities.[71] The Netflix "Privacy Statement" explains the company's "practices . . . regarding the collection, use, and disclosure of [personal] information . . . by the Netflix family of companies."[72] The Privacy Statement ("Policy") includes policies on the following topics, among others: "collection of information," "use of information," "disclosure of information," "access to [the user's] account and profiles, and "use of cookies and internet advertising."[73]

Under the "collection of information" category, the Policy explains that Netflix "automatically" collects information about the user and his or her use of the Netflix services, including, most notably, "title selections, watch history, and search queries; . . . device IDs or other unique identifiers; . . . statistics on page views, referral URLs, IP address (which may [reveal one's] general location), browser and standard web server log information; [and] information collected via the use of cookies."[74] The Policy adds that Netflix "might supplement the information described above with information [it] obtain[s] from other sources, including from both online and offline data providers," such as "demographic data, interest based data, and Internet browsing behavior."[75]

The "disclosure of information" category explains that Netflix shares user information among its "family of companies"[76] for data processing and storage, providing access to services, customer support, and content

---

use user information for the purpose and duration for which it was obtained." *See* TOMTOM, PRIVACY STATEMENT GENERAL, https://www.tomtom.com/en_us/privacy/general/#Datawecollectsports/ (last visited Nov. 16, 2017). *Cf.* SCHNEIER, *supra* note 2, at 59 (stating that Facebook has regularly updated its Privacy Policy to obtain more and more access to user data).

70 *See e.g.* TOMTOM, PRIVACY STATEMENT, *supra* note 63; NETFLIX, PRIVACY STATEMENT, https://help.netflix.com/legal/privacy?locale=en&docType=privacy (last visited Jan. 2, 2018) [hereinafter NETFLIX PRIVACY STATEMENT].

71 The author accessed the NETFLIX PRIVACY STATEMENT after installing the Netflix app on his Android smartphone on March 3, 2017. The same policy can be accessed through the Netflix website at the following link: https://help.netflix.com/legal/privacy?locale=en&docType=privacy (last visited Jan. 2, 2018).

72 NETFLIX PRIVACY STATEMENT, *supra* note 70.

73 Each of these is a section header within the Policy. *Id.*

74 *Id.* at 1.

75 *Id.*

76 *See* NETFLIX, NETFLIX SUPPORT, https://help.netflix.com/support/2101 (last visited Nov. 16, 2017).

development.[77] Such information is also shared with "other companies, agents or contractors [that] perform services on [Netflix's] behalf," including those pertaining to "marketing, advertising, communications, infrastructure and IT services."[78] However, the Policy explains, Netflix "do[es] not authorize [third-party service providers] to use or disclose [a user's] personal information except in connection with providing their services."[79]

Under the heading, "access to [the user's] account and profiles," the Policy warns that "[i]f [a user] . . . allow[s] others to have access to [her] account, they will be able to see [her] information (including in some cases personal information) such as [her] watch history, ratings, reviews and account information."[80]

Finally, under the heading "cookies and internet advertising," the Policy explains that Netflix and its third-party service providers use cookies and similar technologies for various reasons, including "to make it easy to access [the company's] services by remembering [the user] when [she] return[s], . . . to learn more about [its] users and their likely interests, and to deliver and tailor marketing or advertising."[81] Advertising cookies, the Policy explains, "use information about [a user's] visit to this and other websites, such as the pages [she] visits, [her] use of [Netflix's] service or [her] response to ads and emails, to deliver ads that are more relevant to [her]," noting further that "[m]any of the advertising cookies associated with [Netflix's] service belong to [its] Service Providers."[82] The Policy then provides a link to additional information about cookies and information-gathering by third parties,[83] which in turn includes a long list of businesses responsible for "advertising" cookies.[84]

---

77 This type of disclosure, to the extent it includes "personally identifiable information" under the VPPA, is likely covered by the VPPA exception allowing a video tape service provider to disclose personally identifiable information "to any person if the disclosure is incident to the ordinary course of business of the video tape service provider." *See* Video Privacy Protection Act, 18 U.S.C. § 2710(b)(2)(E) (2012).

78 *See* NETFLIX, NETFLIX SUPPORT, *supra* note 76.

79 This type of disclosure is again likely permissible under the VPPA's ordinary course of business exception. *See* 18 U.S.C. § 2710(b)(2)(E).

80 NETFLIX PRIVACY STATEMENT, *supra* note 70. This policy is reminiscent of *Mollett v. Netflix, Inc.*, 795 F.3d 1062, 1066-67 (9th Cir. 2015) (rejecting VPPA claim where Netflix disclosed personally identifiable information directly to the holder of the Netflix account, who then allowed third parties to view the otherwise private disclosures, because Netflix's disclosures were made directly to the consumer himself pursuant to 18 U.S.C. § 2710(b)(2)(A)).

81 NETFLIX PRIVACY STATEMENT, *supra* note 70.

82 *Id.*

83 *Id.* The Policy further states: "At this time, we do not respond to Web browser 'do not track' signals." *Id.*

84 *See* EVIDON, *Interest Based Ads / Cookie Choice Tool*, http://info.evidon.com/pub_info/1932?v=1 (last visited Jan. 2, 2018). The following Advertising cookies are listed: AOL Advertising, DoubleClick, DoubleClick Bid Manager (formerly Invite Media), Facebook, Facebook Business (formerly Facebook Custom Audience), Facebook Social Graph, Facebook Social

As the TomTom and Netflix illustrations exemplify, modern corporate data collection is pervasive and extensive. In addition, although information regarding such practices is often readily available in a company's privacy policy, such information is difficult to comprehend, and the average consumer likely lacks a clear understanding of how her data is used and shared.[85] Finally, although there are many uses for consumer data, such data is most valuable in targeted advertising, creating incentives for companies to acquire it as easily as possible.[86]

II. VIDEO PRIVACY PROTECTION ACT: HISTORY AND REQUIREMENTS

For decades, the Supreme Court has recognized "the threat to privacy implicit in the accumulation of vast amounts of personal information,"[87] particularly with respect to digital data.[88] One aspect of personal privacy concerns a person's movie and video selections, which is governed by the VPPA.[89] Although the VPPA covers only films and videos, representing just a slice of the personal privacy pie, the ability of data brokers to aggregate such data with other types of personal information makes the statute a key piece of the consumer privacy puzzle.[90] Before examining recent judicial interpretations of the statute, Section A considers and analyzes the text of the VPPA itself. Section B then explores the VPPA's legislative history.

Plugins, Facebook for Developers (formerly Facebook Connect), Google AdWords, Google Tag Manager, IPONWEB, Lotame, Optimizely, Signal (formerly BrightTag), SiteScout, Twitter, and Yahoo!

85 *See supra* notes 63, 69 and accompanying text.

86 *See* SCHNEIER, *supra* note 2, at 61-66 (discussing the data broker industry and personalized advertising).

87 Whalen v. Roe, 429 U.S. 589, 605 (1977).

88 *Cf.* Riley v. California, 134 S. Ct. 2473, 2489 (2014) (recognizing that a modern cell phone contains many types of private information–including addresses, notes, prescriptions, bank statements, and videos, among other things–that collectively reveal a great deal more about an individual's private life than any isolated record, and noting that "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions," whereas "the same cannot be said of a photograph or two of loved ones tucked into a wallet"). *See generally* Stanley v. Georgia, 394 U.S. 557, 565 (1969) ("If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch.")

89 *See* Video Privacy Protection Act, 18 U.S.C. § 2710 (2012).

90 *Cf.* Dirkes v. Borough of Runnemede, 936 F. Supp. 235, 238-39 (D.N.J. 1996) (examining the general right to privacy and recognizing the need for courts to "strive to protect th[e] aspect of an individual's right to privacy [protected by the VPPA] in the face of technological innovations that threaten this fundamental right").

A. *The VPPA's Text*

The VPPA is a short statute.[91] The statute begins with a list of definitions,[92] and then includes a general prohibition against disclosure of video transactions, exceptions to the disclosure rule,[93] and various additional provisions covering matters such as civil suits and preemption.[94]

The prohibition portion of the statute imposes civil liability on "[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider."[95] The statute defines the terms "video tape service provider," "personally identifiable information," and "consumer," and these definitions, which have been the focus of most VPPA litigation, are critical in determining the statute's reach.[96]

The VPPA defines the term "video tape service provider," in part, 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."[97] The term "consumer" is defined as "any renter, purchaser, or subscriber of goods or services from a video tape service provider."[98] Lastly, the VPPA states that "the term 'personally identifiable information' *includes* information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."[99]

A few things are notable about the statute's text and structure. First, the term "video tape service provider" is broadly defined to include those that rent or sell "prerecorded video cassette tapes or similar audio visual materials."[100] Given the phrase, "similar audio visual materials," providers of

---

91 *See* 18 U.S.C. § 2710 (only spans two pages).

92 *Id.* § 2710(a).

93 *Id.* § 2710(b).

94 *Id.* § 2710(c)-(f). These additional provisions authorize civil actions for persons "aggrieved by any act of a person in violation of [the statute]." *Id.* § 2710(c). A rule of evidence stating that personally identifiable information obtained in a manner not authorized by the statute "shall not be received in evidence." *Id.* § 2710(d). A provision requiring destruction of personally identifiable information "no later than one year from the date the information is no longer necessary for the purpose for which it was collected." *Id.* § 2710(e). A final provision stating that the statute's provisions "preempt only the provisions of State or local law that require disclosure prohibited by this section." *Id.* § 2710(f).

95 *Id.* § 2710(b)(1).

96 *See* McCabe, *supra* note 58, at 422 (recognizing that the VPPA's definitions "are central to the function of the VPAA in today's digital age and serve as the crux of the debate over privacy concerns with respect to digital video materials").

97 18 U.S.C. § 2710(a)(4). The term "video tape service provider" also includes "any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure." *Id.*

98 *Id.* § 2710(a)(1).

99 *Id.* § 2710(a)(3) (emphasis added).

100 *Id.* § 2710(a)(4).

digital videos, including smartphone apps that offer videos, almost certainly fall within this definition.[101]

Second, for the VPPA to apply, "personally identifiable information" must be disclosed.[102] This term contains two parts: (1) "information which identifies a person," and (2) information indicating that such person "requested or obtained specific video materials or services from a video tape service provider."[103] Thus, the statute is not violated by disclosing identifying information in isolation, such as a list of customer names; rather, a prohibited disclosure must also include information regarding an individual's video rentals or purchases.[104] "There are, in other words, three distinct elements here: the consumer's identity; the video material's identity; and the connection between them."[105]

Third, the statute prevents disclosure of a particular person's video transactions, as opposed to those of an anonymous person.[106] This narrow focus is confirmed by the statute's purpose and history, including the disclosure that occurred in the Robert Bork case.[107]

Fourth, the term "personally identifiable information" is broadly defined to include "information which identifies a person."[108] The definition "does not say 'identify by name' and thus plainly encompasses other means of identifying a person."[109]

---

101 *See, e.g.*, Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1253 n.1 (11th Cir. 2015) (conceding this requirement).

102 *See* 18 U.S.C. § 2710(b)(1).

103 *Id.* § 2710(a)(3).

104 *Cf. id.* § 2710(b)(2)(D) (allowing disclosures of the names and addresses of consumers where the consumer is given the opportunity to prohibit such disclosure, and the disclosure does not identify the title, description, or subject matter of any video tapes or other audiovisual materials).

105 *In re* Hulu Privacy Litig., 86 F. Supp. 3d 1090, 1095 (N.D. Cal. 2015).

106 *See In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 285 (3d Cir. 2016), *cert. denied*, 137 S.Ct. 624 (2017) (examining the VPPA's legislative history and determining that the statute "'protects personally identifiable information that identifies a specific person and ties that person to particular videos that the person watched'" (quoting *In re* Hulu Privacy Litig., No. C 11-03764 LB, 2014 WL 1724344, at *8 (N.D. Cal. April 28, 2014))); *In re Hulu Privacy Litig.*, 2014 WL 1724344, at *7 ("[C]onsidering the ordinary meaning of the plain language of the [VPPA], the language supports the conclusion that the disclosure must be pegged to an identifiable person (as opposed to an anonymous person)."); Eichenberger v. ESPN, Inc., No. C14-463 TSZ, 2015 WL 7252985, at *4 (W.D. Wash. May 7, 2015) ("The focus of this statute . . . is on whether the disclosure by itself identifies a particular person as having viewed a specific video.").

107 *See* S. REP. NO. 100-599, at 5-6, 12 (1988). ("Th[e] [statutory] definition makes clear that personally identifiable information . . . is information that identifies a particular person as having engaged in a specific transaction with a video tape service provider."). *See also In re Nickelodeon*, 827 F.3d at 284 ("Congress's purpose in passing the Video Privacy Protection Act was quite narrow: to prevent disclosures of information that would, with little or no extra effort, permit an ordinary recipient to identify a particular person's video-watching habits."); *In re Hulu Privacy Litig.*, 2014 WL 1724344, at *8.

108 18 U.S.C. § 2710(a)(3).

109 *In re Hulu Privacy Litig.*, 2014 WL 1724344, at *7. *See also* Locklear v. Dow Jones & Co., 101 F. Supp. 3d 1312, 1316 (N.D. Ga. 2015) (recognizing that "a person can be identified by more than just

Fifth, the prohibition portion of the statute contains a "knowledge" requirement that effectively narrows its scope.[110] Although there is not much litigation on the issue, the term "knowledge" has been read to require knowing transmission of private information.[111] Thus, according to one court, knowledge requires more than mere voluntariness in the minimal sense of being aware of one's actions and not acting "because of some mistake or accident."[112] Rather, "knowingly" means "consciousness of transmitting the private information," as opposed to "merely [] transmitting [source] code."[113]

Finally, the VPPA does not prohibit all disclosures of personally identifiable information.[114] The statute's multiple exceptions cover disclosures made directly "to the consumer;"[115] those made to third parties pursuant to the consumer's consent;[116] those made in response to a warrant or court order;[117] and those made to "any person if the disclosure is incident to the ordinary course of business of the video tape service provider."[118] Accordingly, to plead a plausible VPPA claim, a plaintiff must allege that (1) a defendant is a "video tape service provider;" (2) the defendant disclosed "personally identifiable information" concerning one of its "consumers" to "any person"; (3) the disclosure was made "knowingly," requiring "consciousness of transmitting the private information";[119] and (4) the disclosure does not fall within one of the statute's exceptions.[120]

B. *The VPPA's Legislative History*

According to the Senate Report accompanying the statute, the VPPA "reflects the central principle . . . that information collected for one purpose

---

their name and address"); Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 486 (1st Cir. 2016) (same).

110 *See* 18 U.S.C. § 2710(b)(1).

111 *See id.*; *In re* Hulu Privacy Litig., 86 F. Supp. 3d 1090, 1095 (N.D. Cal. 2015).

112 *In re Hulu Privacy Litigation*, 86 F. Supp. 3d at 1095 (internal quotations omitted).

113 *Id.*

114 *See* Mollett v. Netflix, Inc., 795 F.3d 1062, 1066 (9th Cir. 2015).

115 18 U.S.C. § 2710(b)(2)(A). *See also Mollett*, 795 F.3d at 1066 (finding certain Netflix disclosures fell within this exception).

116 18 U.S.C. § 2710(b)(2)(B).

117 *Id.* § 2710(b)(2)(C), (F).

118 *Id.* § 2710(b)(2)(E). In addition, subsection (b)(2)(D) allows the disclosure of a consumer's name and address to any person by a video tape service provider if the consumer has been notified and has had the opportunity to stop the disclosure. *Id.* § 2710(b)(2)(D). However, the disclosure cannot "identify the title, description, or subject matter of any video tapes or other audio visual material" unless the disclosure is "for the exclusive use of marketing goods and services directly to the consumer." *Id.*

119 *See In re* Hulu Privacy Litig., 86 F. Supp. 3d 1090, 1097 (N.D. Cal. 2015).

120 *See Mollett*, 795 F.3d at 1066. *See also In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 267, 279 (3d. Cir. 2016) (stating the requirements of a VPPA claim).

may not be used for a different purpose without the individual's consent."[121] To that end, the VPPA "prohibits video [providers] from disclosing . . . information that links the customer or patron to particular materials or services," except in the specific circumstances authorized by the statute.[122]

As originally contemplated, the VPPA would have covered both videos and books.[123] On August 3, 1988, Representative Al McCandless, the sponsor of the first Video Privacy bill, stated that "people ought to be able to read books and watch films without the whole world knowing," adding that "[b]ooks and films are the intellectual vitamins that fuel the growth of individual thought," and that "[t]his intimate process should be protected from the disruptive intrusion of a roving eye."[124] Despite the connection between books and films, the bill's provisions relating to books were eventually dropped from the statute.[125]

In a lengthy explanation of the VPPA's purpose and design, particularly as it relates to the types of transactional data collection made possible by new technologies, Senator Patrick Leahy explained that the new law was designed to ensure that "the movies we view will be protected against unlawful disclosure,"[126] adding that the law "is a timely response to the need to protect private activities in an era of increasing information collection and dissemination."[127] In a striking passage, particularly given that his remarks were made nearly thirty years ago, the Senator explained the impact of "computerized information" on data accumulation and the possibility of "elaborate dossiers" being compiled through large amounts of transactional data.[128] According to Senator Leahy:

> When people rent video tapes they might reasonably expect that their names will be exchanged with other video dealers as video purchasers. They might even expect to receive special notices about [certain types of films] if they have joined specialized film groups. What they do not expect, and what the law should not allow, is that a detailed list of their previous rentals–the titles of the films, the dates they were rented–will be disclosed to other[s], without their consent.
>
> . . . Our information society is generating an enormous record of personal activity. Every stop at an ATM machine, every car rental transaction, and, now it seems, every purchase at a grocery store places us in space and time. It provides a history of our comings and goings. People can find out where you were, what you were doing, and possibly who you were with.

---

121 S. REP. NO. 100-599, at 8 (1988).

122 *Id.* at 7.

123 *In re Nickelodeon*, 827 F.3d at 284-85.

124 S. REP. NO. 100-599, at 7 (1988).

125 *Id.* at 8 (explaining that "the committee was unable to resolve questions regarding the application of such a provision for law enforcement").

126 134 CONG. REC. 10,259 (remarks of Senator Patrick Leahy) (1988).

127 *Id.*

128 *Id.* at 10,260.

> Who is to say that someday this information could not be compiled and elaborate dossiers on individual activity prepared?[129]

After reiterating his concern with "the trail of information generated by every transaction," Senator Leahy articulated "the principle this bill embodies," namely, that "[a] person maintains a privacy interest in the transactional information about his or her personal activities," such that "[t]he disclosure of this information should only be permissible under well-defined [statutory] circumstances."[130]

What is striking about Senator Leahy's comments is his concern with the accumulation of transactional data, what is known as metadata, and his broader concern of "elaborate dossiers" being compiled on individual consumers through transaction-oriented data.[131] In addition, the Senator's comments reflect an acute concern for ensuring "privacy in an evolving technological world."[132] On at least two occasions, Senator Leahy referred to the bill's protections as "comprehensive,"[133] and some of the bill's language, such as the term "similar audio visual materials,"[134] reflects his desire to extend the statute beyond the specific, tangible film formats of the day (e.g., VHS tapes).[135]

Senator Leahy's remarks were accompanied by similar remarks by Senators Grassley and Simon. Also emphasizing the need to keep pace with technology, Senator Simon declared:

> There is no denying that the computer age has revolutionized our world. . . . Yet as we continue to move ahead, we must protect time honored values that are so central to this society, particularly our right to privacy. The advent of the computer means not only that we can be more efficient than ever before, but that we have the ability to be more intrusive than ever before. Every day Americans are forced to provide to businesses and others personal information without having any control over where that information goes. Computer records are kept on where we travel, what we eat, what we buy, what we watch, and what we read. These records are a window into our loves, likes, and dislikes. . . .
>
> No doubt in the days and years ahead we will continue to make much progress in developing new technologies. While I am fully supportive of innovation and growth, I remain committed to protecting those principles which are so central to America. The legislation being introduced

---

129 *Id.* at 10,259-60.

130 *Id.* at 10,260. Thereafter, the text of the bill was read into the record; the bill contained, at least with respect to the provisions governing videos, nearly identical provisions as the final version of the VPPA. *See id.* at 10,260-61.

131 134 CONG. REC. 10,260-61 (1988) (remarks of Senator Patrick Leahy).

132 *In re* Hulu Privacy Litig., No. C 11–03764 LB, 2012 WL 3282960, at *6 (N.D. Cal. Aug. 10, 2012) (reading the Senate Report this way).

133 134 CONG. REC. 10,259 (remarks of Senator Patrick Leahy).

134 Video Privacy Protection Act, 18 U.S.C. § 2710(a)(4) (2012).

135 *See In re Hulu Privacy Litig.*, 2012 WL 3282960, at *6.

> today strikes the necessary balance to ensure that our privacy will not be lost as we move ahead.[136]

These remarks were made in 1988, largely in response to the disclosure of Judge Bork's video rentals from an earlier technological era. Yet, these comments are striking in their forward-looking nature, including their emphasis on future technologies and the clear desire of the bill's sponsors to account for technological change "to ensure that our privacy will not be lost as we move ahead."[137]

III. JUDICIAL INTERPRETATIONS OF THE VPPA

The VPPA was enacted in 1988,[138] and the first VPPA case was decided in 1996,[139] barely twenty years ago. Although case law interpreting the statute is sparse, the litigation that has occurred in recent years has been extensive, with much of that involving hotly-disputed motions to dismiss under Rule 12(b)(6) of the Federal Rules of Civil Procedure.[140]

Broadly, the cases have revolved around four key issues involving the prohibition portion of the VPPA, which generally prohibits a "video tape service provider" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider."[141] The first and simplest issue, discussed in Section A, is whether a company that streams digital videos online qualifies as a "video tape service provider" under the statute.[142] The second issue, discussed in Section B, concerns the statutory definition of "subscriber," including whether it covers non-paying customers, such as those who download a smartphone app for free.[143] Section C examines the third issue, which involves the scope of the term "personally identifiable information," including whether it covers static digital identifiers.[144] Section D considers the final issue: whether a plaintiff may sue the party that receives personally identifiable information, as well as the party

---

136 134 CONG. REC. 10,259 (remarks of Senator Paul Simon).

137 *Id.*

138 Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (1988) (codified as amended at 18 U.S.C. § 2710 (2012)).

139 Dirkes v. Borough of Runnemede, 936 F. Supp. 235 (D.N.J. 1996).

140 *See, e.g.*, Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 489 (1st Cir. 2016).

141 Video Privacy Protection Act, 18 U.S.C. § 2710(b)(1) (2012).

142 *Id.* § 2710(a)(4).

143 *See* Ellis v. Cartoon Network Inc., 803 F.3d 1251, 1257 (11th Cir. 2016).

144 *See In re* Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 267, 282-84 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 624 (2017).

that wrongfully discloses it.[145] Aside from the first issue, all of these issues involve current splits among the courts.[146]

A. *Video Tape Service Provider"*

As noted, the VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifiable information" concerning one of its consumers,[147] and defines "video tape service provider" to include those that rent, sell, or deliver both "prerecorded video cassette tapes" and "similar audio visual materials."[148] Given the phrase, "similar audio visual materials," businesses that provide digital videos, including smartphone apps that offer video services, almost certainly fall within this definition.[149]

One of the first judicial opinions on this issue involved the extensive *Hulu Privacy Litigation* case.[150] In that case, Magistrate Judge Laurel Beeler of the United States District Court for the Northern District of California examined whether Hulu, which operates a website called Hulu.com that provides digital video content,[151] engaged in selling or distributing "similar audio visual materials" under the VPPA.[152] On that issue, Hulu argued that the statute "only regulates businesses that sell or rent physical objects . . . and not businesses that transmit digital content over the Internet."[153] Relying on the Senate Report's statement that "video tape service provider" means a person "engaged in the business of . . . delivery of prerecorded video cassette tapes or similar audio visual materials, such as laser discs, open-reel movies, or CDI technologies,"[154] plaintiffs argued that the phrase "similar audio visual

---

145 *See id.* at 267; Daniel v. Cantrell, 375 F.3d 377, 381-82 (6th Cir. 2004).

146 For the second issue *see e.g.*, Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 489 (1st Cir. 2016); *Ellis*, 803 F.3d 1251. For the third issue *see e.g.*, *In re Nickelodeon*, 827 F.3d at 267, 282-84; Locklear v. Dow Jones & Co., 101 F. Supp. 3d 1312 (N.D. Ga. 2015). For the fourth issue *see e.g.*, Sterk v. Redbox Automated Retail, LLC, 672 F.3d 535, 536 (7th Cir. 2012); *Daniel*, 375 F.3d at 381-82.

147 18 U.S.C. § 2710(b).

148 *See id.* § 2710(a)(4). The term "video tape service provider" also includes "any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure." *Id.*

149 *See, e.g.*, *In re* Hulu Privacy Litig., No. C 11–03764 LB, 2012 WL 3282960, at *4-*6 (N.D. Cal. Aug. 10, 2012) (examining plaintiffs' VPPA claim based on their use of hulu.com to view video content and finding that Congress intended to cover new technologies for pre-recorded video content, such as videos delivered in digital form); *Ellis*, 803 F.3d at 1253 n.1 (finding this requirement indisputably met); *Locklear*, 101 F. Supp. 3d at 1312 (applying the VPPA to internet-based video streaming), *abrogated on other grounds by Ellis*, 803 F.3d 1251 (11th Cir. 2015).

150 *In re Hulu Privacy Litig.*, 2012 WL 3282960, at *4-*6.

151 *See id.* at *2.

152 *See id.* at *4.

153 *Id.* (internal quotations omitted).

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

materials" broadly covers new technologies for pre-recorded video content.[155]

Agreeing with the plaintiffs, Judge Beeler declared that "a plain reading of a statute that covers videotapes and 'similar audio visual materials' is about the video content, not about how that content was delivered (e.g., via the internet or a bricks-and-mortar store)."[156] Moreover, Judge Beeler believed the Senate Report, particularly Senator Leahy's comments, reflected Congress's concern with protecting the "confidentiality of private information about viewing preferences," regardless of the media format involved, which explained the Senate Report's reference to laser discs, open-reel movies, and CDI technologies.[157] Thus, Judge Beeler found that Congress included the phrase "similar audio visual materials" to ensure the VPPA's protections would extend to new technologies, including purely digital distribution of video content.[158] After the *Hulu* decision, there appears to be no real dispute on this point.[159]

B. *Subscriber"*

The VPPA protects only "consumers,"[160] defined as "any renter, purchaser, or subscriber of goods or services from a video tape service provider."[161] Accordingly, litigation has focused on whether a plaintiff qualifies as a "renter," "purchaser," or "subscriber"—terms that are themselves not defined in the statute.[162]

Two leading cases on this issue are *Yershov v. Gannett Satellite Information Network, Inc.*,[163] a 2016 decision of the United States Court of Appeals for the First Circuit, and *Ellis v. Cartoon Network, Inc.*,[164] an Eleventh Circuit opinion decided about six months before *Yershov*.

Yershov and *Ellis* each involved a free smartphone app downloaded through Google Play Store.[165] In each case, plaintiffs alleged that they accessed and viewed videos on the app; that the app provider kept a record

---

155 *In re Hulu Privacy Litig.*, 2012 WL 3282960, at *5.

156 *Id.* at *5.

157 *Id.* at *6.

158 *See id.*

159 *See, e.g.*, Ellis v. Carton Network, Inc., 803 F.3d 1251, 1253 n.1 (11th Cir. 2015) (finding this requirement indisputably met).

160 Video Privacy Protection Act, 18 U.S.C. § 2710(b) (2012).

161 *Id.* § 2710(a)(1).

162 18 U.S.C. § 2710(a). *See also* Locklear v. Dow Jones & Co., 101 F. Supp. 3d 1312, 1315 (N.D. Ga. 2015) (recognizing that the VPPA does not define the terms "renter" or "subscriber").

163 820 F.3d 482 (1st Cir. 2016).

164 803 F.3d 1251 (11th Cir. 2015).

165 *See* Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 484 (1st Cir. 2016); *Ellis*, 803 F.3d at 1253.

of a user's video viewing history by tying that information to the user's Android ID number; and that the app provider then sent that information to a third-party data analytics company capable of pinpointing user identities.[166] The district courts in both cases reached opposite results on whether the plaintiffs were "consumers" under the statute, with the *Yershov* district court finding that the plaintiffs were not "consumers" and the *Ellis* district court finding that they were.[167] Each of these decisions were subsequently reversed on appeal.[168]

Ellis, the first of the two cases decided on appeal, involved Cartoon Network's free CN app, which plaintiff Mark Ellis downloaded to his smartphone to watch video clips.[169] According to the complaint, Cartoon Network kept records of the videos Ellis watched by tying that data to his Android ID, a unique sixty-four-bit number assigned to an individual device.[170] Thereafter, without Ellis's consent, Cartoon Network shared both his views and Android ID with Bango, a third-party data analytics company that specializes "in tracking individual behaviors across the Internet and mobile applications."[171] According to the complaint, Bango can "'automatically' link an Android ID to a particular person by compiling information about that individual from other" sources, such that when Cartoon Network sends Bango the Android ID of a CN app user along with his video viewing history, Bango associates that video history with a particular person.[172]

Ellis sued Cartoon Network under the VPPA, alleging in part that he was a "subscriber" of Cartoon Network, and thus a "consumer" under the statute.[173] The district court found that Ellis was a "subscriber" because he

---

166 *See Yershov*, 820 F.3d at 484; *Ellis*, 803 F.3d at 1253-54.

167 *See Yershov*, 820 F.3d at 484; *Ellis*, 803 F.3d at 1252 (summarizing district court orders); *see also* Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 146-48 (D. Mass. 2015), *rev'd on other grounds*, 820 F.3d 482 (1st Cir. 2016) (finding that a "common thread" of being a "subscriber" to digital content in the modern world is "some or all of the following: payment, registration, commitment, delivery, and/or access to restricted content;" and that to download and use the USA Today App, a user need not pay any money, register for an account, or otherwise commit in any way, such that the person is not a "subscriber" but merely a "user"); *Ellis v. Cartoon Network, Inc.*, No. 1:14-CV-484-TWT, 2014 WL 5023535, at *2 (N.D. Ga. Oct. 8, 2014) (finding that plaintiff, Mark Ellis, was "arguably a subscriber," and therefore a "consumer" under the VPPA, because he had downloaded the Cartoon Network app on his smartphone and used it to watch video clips).

168 *See Yershov*, 820 F.3d at 484; *Ellis*, 803 F.3d at 1252.

169 *See Ellis*, 803 F.3d at 1257.

170 *See id.* at 1254.

171 *Id.*

172 *Id.*

173 *Id.*

had downloaded the Cartoon Network app on his smartphone and used it to watch video clips.[174] The Eleventh Circuit Court of Appeals disagreed.[175]

The Eleventh Circuit began its analysis with the ordinary meaning of the term "subscriber," including its common dictionary definitions.[176] The court first found that "payment is not a necessary element of a subscription,"[177] but was instead just a factor to consider, reasoning that "[t]he term 'subscriber' is not preceded by the word 'paid' in [the VPPA] and there are numerous periodicals, newsletters, blogs, videos, and other services that a user can sign up for (i.e., subscribe to) and receive for free."[178] Nevertheless, the court determined that one does not become a "subscriber" by "merely downloading [an] app for free and watching videos at no cost."[179] Borriwing largely from the reasoning of the *Yershov* district court (which was subsequently overturned by the First Circuit Court of Appeals), the Eleventh Circuit held that a "'subscription' involves some type of commitment, relationship, or association (financial or otherwise) between a person and an entity."[180]

Turning to the merits, the court found that Ellis was not a "subscriber" of Cartoon Network or the CN app because he (1) did not sign up for or establish an account with Cartoon Network; (2) did not pay for use of the CN app; (3) did not become a registered user of Cartoon Network or the CN app; (4) did not receive a Cartoon Network ID or establish a Cartoon Network profile; (5) did not sign up for any periodic services or transmissions; and (6) did not establish any relationship that would give him access to exclusive content.[181] In the Eleventh Circuit's view, merely downloading an app for free and using it to view content involves "no ongoing commitment or relationship between the user and [the app owner]," and is simply "the equivalent of adding a particular website to one's Internet browser as a favorite, allowing quicker access to the website's content," which does not make one a "subscriber."[182]

Although the Eleventh Circuit in *Ellis* relied heavily on the reasoning of the *Yershov* district court, *Yershov* was later overturned by the First Circuit

---

174 Ellis v. Cartoon Network, Inc., No. 1:14–CV–484–TWT, 2014 WL 5023535, at *2 (N.D. Ga. Oct. 8, 2014).

175 Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1257-58 (11th Cir. 2015).

176 *See id.* at 1255.

177 *Id.* at 1256.

178 *Id. See also In re* Hulu Privacy Litig., 2012 WL 3282960, at *8 (recognizing that "[i]f Congress wanted to limit the word 'subscriber' to 'paid subscriber,' it would have said so").

179 *Ellis*, 803 F.3d at 1256.

180 *Id.* (citing Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 147 (D. Mass. 2015), *rev'd on other grounds*, 820 F.3d 482 (1st Cir. 2016)).

181 *See id.* at 1257.

182 *See id.* Having reached this result, the court affirmed the district court's order dismissing Ellis's amended complaint, and thus expressed no view on the district court's reading of the term "personally identifiable information." *Id.* at 1258.

Court of Appeals.[183] Like *Ellis*, *Yershov* involved a free smartphone app, the USA Today Mobile App.[184] Similar to *Ellis*, the *Yershov* plaintiffs alleged that each time a user viewed a video clip on the app, Gannett, the producer of the USA Today newspaper, sent Adobe the title of the video viewed and the user's unique Android ID.[185] Distinct from *Ellis*, however, Gannett allegedly also sent the GPS coordinates of the user's smartphone at the time the video was viewed.[186] According to the plaintiffs, Adobe would take this and other information gathered from various sources to create user profiles that included, for example, the user's name and address, age and income, household structure, and online navigation and transaction history, all of which allowed Adobe to build "digital dossiers" on specific users and permitted Adobe's clients to more accurately target advertisements.[187] As with the plaintiffs in *Ellis*, Yershov alleged that he never consented to the disclosure of any personal information to third parties.[188]

After finding that the complaint adequately alleged Gannett disclosed "personally identifiable information" in the form of "which USA Today videos Yershov ha[d] obtained,"[189] an issue addressed in the next section, the court turned to the "closer question" of whether Yershov was a "consumer" in relation to Gannett, which in turn depended on whether he was a "subscriber" under the VPPA.[190] As in *Ellis*, the *Yershov* court began its analysis with the "plain and ordinary meaning" of the word "subscriber," as conveyed by its dictionary definition.[191] Because a "subscriber" is generally defined as "one who subscribes," the court considered common definitions of the term "subscribes," highlighting one that appeared to be most "on point technologically."[192] According to that definition, "subscribe" means "'[t]o receive or be allowed to access electronic texts or services by subscription,' with 'subscription' defined, in turn, to include '[a]n agreement to receive or be given access to electronic texts or services.'"[193] According to the *Yershov* court:

> This is just what we have here: Gannett offered and Yershov accepted Gannett's proprietary mobile device application as a tool for directly receiving access to Gannett's electronic text and videos without going through other distribution channels, much like how a newspaper

183 *Yershov*, 820 F.3d at 490.

184 *Id. at* 484.

185 *Id.* at 484-85.

186 *Id.* at 484.

187 *Id.* at 484-85.

188 *Id.* at 485.

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

190 *Id.* at 487.

191 *Id.*

192 *Id.*

193 *Id.* (quoting THE AMERICAN HERITAGE DICTIONARY 1726 (4th ed. 2000)).

> subscriber in 1988 could . . . retrieve a copy of the paper in a box at the end of his driveway without having to go look for it at a store.[194]

Recognizing that some definitions of "subscribe" include the element of payment, the court then clarified that payment was not required under the VPPA.[195] Persuasively, the court reasoned that "if the term 'subscriber' required some sort of monetary payment, it would be rendered superfluous by the two terms preceding it"—renter and purchaser—because "a person in 1988 who exchanged payment for a copy of a video either retained ownership of the video outright, thereby becoming a 'purchaser' of the video, or received temporary possession of the video for a set period of time, thereby becoming a 'renter.'"[196] Accordingly, the court felt that Congress would not have included "subscribers" as a category of "consumers" had it intended to protect only persons who pay for videos.[197]

In addition, the court felt that Congress did not wish to impose different disclosure rules on transactions involving no payment, including, for example, where a customer in 1988 obtained several videos from a new commercial supplier at no charge or with money back.[198] Reading the statute as one intended to flex with the times, the court thus declared: "[B]ecause we think that Congress cast such a broadly inclusive net in the brick-and-mortar world, we see no reason to construe its words as casting a less inclusive net in the electronic world when the language does not compel that we do so."[199]

Finally, the court distinguished *Ellis* because, unlike in that case, Yershov had to provide Gannett with personal information in order to use the USA Today app—including his Android ID and his mobile device's GPS location at the time he viewed a video, each linked to his viewing selections—such that "access was not free of a commitment to provide consideration in the form of that information, which was of value to Gannett."[200] Disagreeing with the *Ellis* court's analogy between installing a cell phone app and adding a particular website as a favorite,[201] the First Circuit further felt that "by installing the App on his phone, thereby establishing seamless access to an electronic version of USA Today, Yershov established a relationship with Gannett that is materially different from what would have been the case had USA Today simply remained one of millions of sites on the web that Yershov might have accessed through a web browser."[202] Finally, the court emphasized that its holding was narrow (given

---

194 *Id.*

195 Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 487-88 (1st Cir. 2016).

196 *Id.* at 487.

197 *Id.*

198 *Id.* at 488.

199 *Id.*

200 *Id.* at 488-89.

201 *See* Ellis v. Carton Network, Inc., 803 F.3d 1251, 1257 (11th Cir. 2015).

202 *Yershov*, 820 F.3d at 489.

the Rule 12(b)(6) context),[203] and that its analysis could change depending on, for example, whether Gannett classified those who access its content through the app differently from those who accessed only its website.[204]

In some respects, *Yershov* and *Ellis* are in tension on the "subscriber" issue. For example, their views differ regarding whether downloading an app shows no greater "commitment" than simply bookmarking a website in one's Internet browser.[205] An important distinction between the cases is that the *Yershov* plaintiff had to provide not just his Android ID but also his mobile device's GPS location at the time he viewed a video, which, as it pertained to his "subscriber" status, was deemed "consideration" in the form of valuable information, and which more broadly elevated plaintiff's privacy claim.[206] For this reason, the court likely felt that dismissing the case at an early stage was unwarranted. However, *Yershov* is not the only case to have reached this result on the "subscriber" issue, and thus should not be treated as an anomaly.[207]

C. *Personally Identifiable Information"*

Courts in recent years have considered whether the VPPA applies to various static digital identifiers, such as a smartphone Android ID;[208] device serial numbers, such as that associated with a Roku device;[209] and IP

---

203 *Id.* (noting that "Our actual holding . . . need not be quite as broad as our reasoning suggests. We need simply hold, and do hold, only that the transaction described in the complaint . . . plausibly pleads a case that the VPPA's prohibition on disclosure applies.").

204 *Id.* (identifying other issues, including those pertaining to the issue of personally identifiable information, such as whether Yershov is correct about the extent to which Adobe foreseeably can identify him).

205 *See id.* at 488-89; *Ellis*, 803 F.3d at 1256.

206 *Yershov*, 820 F.3d at 488-89.

207 *See, e.g.*, Locklear v. Dow Jones & Co., 101 F. Supp. 3d 1312, 1315-16 (N.D. Ga. 2015) (finding plaintiff had pled sufficient facts to qualify her as a "subscriber" under the VPPA by alleging that she downloaded the *Wall Street Journal Live Channel* on Roku and used it to watch videos). *But see* Perry v. Cable News Network, Inc., No. 1:14-CV-02926-ELR, 2016 WL 4373708, at *3 (N.D. Ga. Apr. 20, 2016) (relying on *Ellis* to find that plaintiff—who merely downloaded the CNN App on his iPhone and used the app to read news stories and watch video clips—was not a "subscriber" because "there is no indication that he had any ongoing commitment or relationship with Defendants, such that he could not simply delete the CNN App without consequences").

208 *See Yershov*, 820 F.3d at 484.

209 *See* Robinson v. Disney Online, 152 F. Supp. 3d 176, 184 (S.D.N.Y. 2015) (concluding that plaintiff's "anonymized Roku serial number" disclosed by Disney does not identify a specific person; rather, "it identifies a specific device, and nothing more"). Roku is a digital media-streaming device that delivers videos, news, games, and other content to consumers' televisions via the Internet. *See also Locklear*, 101 F. Supp. 3d at 1313.

addresses.[210] This has proven to be the most significant statutory interpretation issue involving the VPPA.

As a starting point, courts agree that the VPPA's category of "personally identifiable information" includes more than a user's name and address.[211] The question is whether the VPPA applies to other forms of identification unique to the digital era.[212] On that issue, plaintiffs have argued that digital identifiers should be subject to the VPPA because third parties to whom disclosures are made, including companies like Adobe or Google, can easily identify individual users by linking such disclosures with existing personal information obtained elsewhere.[213] By analogy, plaintiffs have argued that when a referee calls a foul on "No. 12 on the offense," everyone with a game program can quickly determine that person's identity.[214] The same is true for many digital identifiers, where companies such as Adobe and Google "have the game program," so to speak, enabling them to easily link different forms of identifying information.[215]

Most courts have rejected plaintiffs' arguments and have instead read the term "personally identifiable information" narrowly to require disclosure of information which *by itself* identifies a particular person.[216] Under this restrictive view, if the third-party recipient of a disclosure must refer to other sources to identify the individual at issue, no disclosure of "personally identifiable information" has occurred.[217] Cases adopting this approach often involve device serial numbers, including a Third Circuit Court of Appeals decision (*In re Nickelodeon Consumer Privacy Litigation* ("*Nickelodeon*")[218] and three recent district court decisions (*Robinson v. Disney Online*,[219]

---

210 *See In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 281 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 624 (2017). *See also id.* at 269, 281-82 (identifying other such identifiers).

211 *See, e.g.*, *Yershov*, 820 F.3d at 486; *Robinson*, 152 F. Supp. 3d at 180-81 (agreeing that PII "includes more than just names and addresses; it would be difficult to read the language of the statute otherwise"); *Locklear*, 101 F. Supp. 3d at 1316 (same). *See also Robinson*, 152 F. Supp. 3d at 182 (believing that "Congress considered names and addresses to be sufficiently identifying without more").

212 *See Robinson*, 152 F. Supp. 3d at 180 (describing the issue as "the scope of information encompassed by PII, and how, precisely, this information must identify a person").

213 *See id.*

214 *See Yershov*, 820 F.3d at 486.

215 *See id.*

216 *See, e.g.*, Perry v. Cable News Network, Inc., No. 1:14-CV-02926-ELR, 2016 WL 4373708, at *5 (N.D. Ga. Apr. 20, 2016); *Robinson*, 152 F. Supp. 3d at 179; *In re* Hulu Privacy Litigation, No. 11–cv–3764 (LB), 2014 WL 1724344, at *7 (N.D. Cal. Apr. 28, 2014).

217 *See* Locklear v. Dow Jones & Co., 101 F. Supp. 3d 1312, 1318 (N.D. Ga. 2015) (summarizing cases adopting this interpretation).

218 *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 284 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 624 (2017).

219 152 F. Supp. 3d 176, 182 (S.D.N.Y. 2015).

Locklear v. Dow Jones & Company,[220] and *Eichenberger v. ESPN, Inc.*).[221] Not all courts agree with the restrictive view, however, including the First Circuit Court of Appeals in *Yershov*.[222]

*As d*iscussed at length in the previous Section, plaintiffs in *Yershov* alleged that each time a user viewed a video on the USA Today Mobile App, its owner, Gannett, sent Adobe the title of the video viewed, the user's Android ID, and the GPS coordinates of the user's smartphone.[223] Adobe then allegedly combined this information with data gathered elsewhere to create detailed digital dossiers on specific users.[224]

Both the district court and the First Circuit Court of Appeals found that the information disclosed was indeed "personally identifiable information" under the VPPA.[225] To the district court, the question was not even close.[226] Examining the VPPA's definition of "personally identifiable information," which encompasses "information which identifies a person as having [obtained a video]," the First Circuit found that Congress clearly did not intend to limit the term to information that explicitly names a person because, had Congress wished to do so, it would not have used the more abstract language found in the statute.[227] The court also noted that the definition begins with the word "includes," which implies that the definition does not capture the whole meaning,[228] and relied on the Senate Report's statement that the drafters' aim was "to establish a minimum, but not exclusive, definition of personally identifiable information."[229] Finally, the court noted that "[m]any types of information other than a name can easily identify a person," including, for example, a social security number that is revealed to the government.[230]

Turning to the merits, the court found that the combination of Android ID and GPS coordinates "effectively reveal[s] the name of the video viewer."[231] "Given how easy it is to locate a GPS coordinate on a street map, [such a disclosure alone] would enable most people to identify [the likely]

---

220 101 F. Supp. 3d 1312, 1317-18 (N.D. Ga. 2015).

221 Eichenberger v. ESPN, Inc., No. 14–cv–463 (TSZ), 2015 WL 7252985, at *3–5 (W.D. Wash. May 7, 2015) (finding that "the term 'personally identifiable information,' by its ordinary meaning, refers to information that identifies an individual and does not extend to anonymous IDs, usernames, or device numbers," such that disclosure of the plaintiff's "Roku serial number, without more, does not constitute PII[.]").

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

223 *Id.* at 484.

224 *Id.* at 484-85.

225 *Id.* at 484.

226 *See* Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 140-46 (D. Mass. 2015), *rev'd on other grounds*, 820 F.3d 482 (1st Cir. 2016).

227 *Yershov*, 820 F.3d at 485.

228 *Id.* at 486.

229 *Id.*

230 *Id.*

231 *Id.*

address[] of the viewer," such as that of the Bork family.[232] Moreover, the specific recipient, Adobe, is significant. According to the court, "when Gannett makes such a disclosure to Adobe, it knows that Adobe has the 'game program,' so to speak, allowing it to link the GPS address and device identifier information to a certain person by name, address, phone number, and more," such that "the linkage of information to identity . . . is both firm and readily foreseeable to Gannett."[233] Thus, the First Circuit found that the information allegedly disclosed was "reasonably and foreseeably likely to reveal" the specific USA Today videos the plaintiffs had viewed.[234]

A few months after the First Circuit's decision in *Yershov*, the Third Circuit Court of Appeals reached essentially the opposite outcome in *Nickelodeon*.[235] *Nickelodeon* involved a class action brought by children younger than age thirteen who alleged that defendants Viacom and Google unlawfully collected information about them on the Internet, including what videos they watched on Viacom's websites, such as Nick.com, a website geared towards children that offers video streaming.[236]

Plaintiffs' VPPA claim was based on the use of cookies by Viacom (which employs first-party cookies) and Google (which employs third-party cookies). The companies use cookies to track web browsing and video viewing on Viacom's websites.[237] Plaintiffs alleged that Viacom discloses to Google, and Google collects and tracks, all of the following information about children who visit Viacom's websites: (1) the child's username/alias;[238] (2) the child's gender; (3) the child's birthdate; (4) the child's IP address; (5) the child's browser settings; (6) the child's unique device identifier; (7) the child's operating system; (8) the child's screen resolution; (9) the child's browser version; (10) the child's detailed URL requests and video materials requested and obtained from Viacom's children's websites; and (11) the DoubleClick persistent cookie identifiers used by Google to track a person

---

232 *Id.*

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

234 *Id.*

235 *In re* Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 267 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 624 (2017).

236 *Id.*

237 *Id.* at 269 (summarizing the more detailed allegations involving cookies).

238 According to plaintiffs, a child registers to use Nick.com by signing up for an account and choosing a username and password. *Id.* at 268. During the registration process, a child provides his or her birthdate and gender to Viacom, and Viacom then assigns the child a code based on that information. *Id.* At the time suit was filed, Viacom's registration form included a message to children's parents: "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to!" *Id.* at 269. It is unclear whether this particular warning is still utilized by Viacom. In addition, although the proposed classes in the case were spread over different time periods, plaintiffs noted that Viacom "revamped its Nick.com website" in August 2014 so that it "no longer discloses the particular video viewing or game histories of individual users of Nick.com to Google." *Id.* at 270-71.

across any website on which Google displays ads.[239] According to plaintiffs, the purpose of this information gathering is to sell child targeted advertising.[240]

A key allegation in the plaintiffs' complaint was the ease by which advertising companies identify web users' true identities based on their online browsing habits.[241] Citing the work of computer science professor Arvind Narayanan, plaintiffs argued that "re-identification" of web users based on seemingly anonymous data is possible based on users' commercial transactions, web browsing, search histories, and other factors.[242] They also argued that companies can use "browser fingerprinting" to identify website visitors based on the configuration of a user's browser and operating system.[243] Thus, plaintiffs argued, Google and Viacom "are able to link online and offline activity and identify specific users" with ease.[244]

After finding that Google, the recipient of Viacom's data, was not a proper defendant under the VPPA,[245] the court examined whether the remaining defendant, Viacom, disclosed "personally identifiable information" about the children who viewed videos on its websites.[246] The court specifically considered three identifiers that allegedly permitted Google to track the same computer across time: (1) the user's IP address; (2) the user's browser and operating system settings (i.e., the "browser fingerprint"); and (3) a computing device's "unique device identifier," the sixty-four-bit number that is randomly generated when a user initially sets up his device.[247]

Plaintiffs argued that if a Google user were to run a Google search from his or her computer, and if that person's child were to visit Nick.com and watch a video on the same device, Google could match the data—based on IP address, browser fingerprint, or unique device identifier—to determine that the same computer was involved in both transactions.[248] Thus, plaintiffs argued that Viacom, by permitting Google to use cookies on its website, effectively disclosed "information which identifies [a particular child] as having requested or obtained specific video materials or services from a video tape service provider," thereby violating the VPPA.[249] In response, Viacom argued that static digital identifiers, such as IP addresses, alone do

---

239 *Id.* at 269.

240 *Id.* at 269-70.

241 *In re* Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 269-70 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 624 (2017).

242 *Id.* at 270.

243 *Id.*

244 *Id.*

245 *Id.* at 279-81.

246 *Id.* at 281.

247 *In re* Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 281-82, 282 n.124 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 624 (2017).

248 *Id.* at 282.

249 *Id.*

not identify a particular person, but instead only identify the location of a connected computer, which does not constitute personally identifiable information.[250]

The court agreed with Viacom.[251] Effectively limiting the VPPA's reach, the court adopted the "average"[252] or "ordinary" recipient test for what constitutes personally identifiable information, requiring proof that "an ordinary person" could readily identify a specific individual with the information provided,[253] thereby rejecting the alternative approach focused on whether the *particular recipient* at issue could *theoretically combine* such static digital identifiers with other information to identify an individual.[254] In the Third Circuit's view, "Congress's purpose in passing the [VPPA] was quite narrow: to prevent disclosure of information that would, *with little or no extra effort*, permit an *ordinary recipient* to identify a particular person's video-watching habits."[255] In addition, the court felt that Congress did not intend the VPPA to cover "factual circumstances far removed from those that motivated its passage,"[256] which involved disclosures of information readily capable of identifying an *actual person's* video-watching history without much effort,[257] as in the case of the Robert Bork disclosure.[258] According to the court, "[t]he classic example will always be a video clerk leaking an individual customer's video rental history," and "[e]very step away from that 1988 paradigm will make it harder for a plaintiff to make out a successful claim."[259]

Although the Third Circuit conceded that "[s]ome disclosures predicated on new technology, such as the dissemination of precise GPS coordinates or customer ID numbers, may suffice,"[260] in the court's view, "[t]o an average person, an IP address or a digital code in a cookie file would likely be of little help in trying to identify an actual person."[261] The court noted, for example, that a subpoena is usually necessary to connect an IP

---

250 *Id.*

251 *Id.* at 286 ("[W]e ultimately do not think that the definition of personally identifiable information in the [VPPA] is so broad as to cover the kinds of static digital identifiers at issue here.").

252 *Id.* at 283.

253 *In re* Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 290 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 624 (2017) ("In 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.").

254 *Id.* at 283-84.

255 *Id.* at 284 (emphasis added).

256 *Id.*

257 *Id.* at 285.

258 *Id.* at 290.

259 *In re* Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 290 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 624 (2017).

260 *Id.*

261 *Id.* at 283.

address with an actual person in copyright litigation.[262] Accordingly, this type of disclosure is distinct from that in *Yershov*, which involved disclosure of GPS coordinates, because "GPS coordinates contain more power to identify a *specific person* than . . . an IP address, a device identifier, or a browser fingerprint."[263] For these reasons, the court determined that plaintiffs had failed to state a viable claim under the VPPA.[264]

Many courts agree with the Third Circuit that no valid VPPA claim exists when the third-party recipient of video data allegedly uses information from other sources to determine the user's identity.[265] This view of the statute, however, is unrealistically narrow in light of modern business practices. For example, the court in *Robinson*, which endorsed this narrow view, agreed that defendant Disney "could not disclose . . . [plaintiff's Roku device serial number], along with a code that enabled [third-party recipient] Adobe to decrypt the hashed serial number . . . and still evade liability."[266] Yet, for purposes of deciding defendant's motion to dismiss, the *Robinson* court earlier assumed "that Adobe ha[d] actually identified" plaintiff by "linking" Disney's disclosures with "existing personal information" obtained elsewhere; in other words, the court assumed that Adobe had previously secured the "code" itself.[267] Accordingly, Disney's disclosure accomplished the same result as if Disney had disclosed both the Roku serial number and the code, making its actual disclosure equally problematic.

Also, although the *Nickelodeon* court sought to distinguish *Yershov*, the information disclosed in the two cases is functionally identical, and should be treated the same for purposes of VPPA protection.[268] *Yershov* involved the disclosure of the named plaintiff's cell phone identification number and his

---

262 *Id.*

263 *Id.* at 289 (emphasis in original). The court advanced additional justifications for its ruling. For example, the court noted that Congress did not alter the VPPA's original definition of personally identifiable information, despite having amended the statute in 2012, which the court believed revealed Congress's intent *not* to modernize the statute in light of on-demand cable services and Internet streaming services. *See id.* at 288-89.

264 *Id.* at 290. *See also* C.A.F. v. Viacom, Inc., 137 S. Ct. 624 (2017) (denying certiorari in the case).

265 *See, e.g.*, Eichenberger v. ESPN, Inc., No. 14–cv–463 (TSZ), 2015 WL 7252985, at *5-*6 (W.D. Wash. May 7, 2015) (finding that the disclosure of the plaintiff's "Roku serial number, without more, does not constitute PII[.]"); Robinson v. Disney Online, 152 F. Supp. 3d 176, 181-83 (S.D.N.Y. 2015) (rejecting plaintiff's argument that the VPPA was violated when defendant disclosed plaintiff's viewing history and Roku device serial number to third-party recipient, Adobe, enabling it to combine these disclosures with existing personal information obtained elsewhere); Locklear v. Dow Jones & Co., 101 F. Supp. 3d 1312, 1318 (N.D. Ga. 2015) (rejecting plaintiff's argument because "third party mDdialog had to take further steps, i.e., turn to sources other than [the disclosing party], to match the [plaintiff's] Roku number to [p]laintiff").

266 *Robinson*, 152 F. Supp. 3d at 182-83.

267 *Id.* at 180.

268 *See In re Nickelodeon*, 827 F.3d at 269; Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 484 (1st Cir. 2016).

GPS coordinates at the time he viewed a particular video,[269] whereas *Nickelodeon* involved unique device identifiers and IP addresses (among other identifiers).[270] Thus, both cases involved disclosure of an individual's unique device identifier, which may alone identify an individual user, coupled with the digital equivalent of a physical address—GPS coordinates, on the one hand, and IP addresses, on the other. In combination, these identifiers are capable of identifying particular individuals.[271] GPS coordinates, like physical addresses, may identify a particular residence,[272] and courts agree that a physical address undoubtedly constitutes personally identifiable information under the VPPA, even though a physical address alone often does not pinpoint a particular person at that location.[273] IP addresses are not much different because, as with physical addresses, no two Internet-connected devices have the same IP address.[274] This, in turn, makes it quite easy for recipients of data—particularly sophisticated recipients like Google and law enforcement—tied to an IP address to identify a specific Internet user's identity.[275] For this reason, in a case decided a few years before

---

269 *Yershov*, 820 F.3d at 484.

270 *In re Nickelodeon*, 827 F.3d at 269.

271 *See id.*; *Yershov*, 820 F.3d at 484-85.

272 *See In re Nickelodeon*, 827 F.3d at 289 (quoting the First Circuit's statement in *Yershov* that "[g]iven how easy it is to locate a GPS coordinate on a street map, this disclosure would enable most people to identify what are likely the home and work addresses of the viewer"). *Cf.* 16 C.F.R. § 312.2 (2018) (defining "personal information" under COPPA to include "[a] home or other physical address including street name and name of a city or town;" as well as "[g]eolocation information sufficient to identify street name and name of a city or town.").

273 *See Yershov*, 820 F.3d at 486 (agreeing that PII "includes more than just names and addresses"); Robinson v. Disney Online, 152 F. Supp. 3d 176, 180-81 (S.D.N.Y. 2015). Related privacy statutes also deem physical addresses personally identifiable. The Family Education and Records Privacy Act of 1974 ("FERPA"), for example, prohibits educational entities from releasing or providing access to "any personally identifiable information in education records," 20 U.S.C. § 1232g(b)(2), and the regulation implementing the statute, 34 C.F.R. § 99.3, provides a definition of personally identifiable information that includes the student's name and address. *See also* Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972, 3982 (Jan. 17, 2013) (to be codified at 16 C.F.R. § 312.2) (rejecting the argument that "precise geolocation information allows only contact with a specific device, not the individual using the device," and stating, "[b]y that same flawed reasoning, a home or mobile telephone number would also only permit contact with a device.").

274 *See* United States v. Vosburgh, 602 F.3d 512, 517-18 n.3 (3d Cir. 2010). *See also* United States v. Forrester, 512 F.3d 500, 510 n.5 (9th Cir. 2008) ("Every computer or server connected to the Internet has a unique IP address."); Peterson v. Nat'l Telecomm. & Inform. Admin., 478 F.3d 626, 629 (4th Cir. 2007) (explaining that "[e]ach computer connected to the Internet is assigned a unique numerical [IP] address"); White Buffalo Ventures, LLC v. Univ. of Texas at Austin, 420 F.3d 366, 369 n.6 (5th Cir. 2005) (describing an IP address as "a unique 32–bit numeric address" that essentially "identifies a single computer"). Also, recall that the Netflix "Privacy Statement," for example, explains that the company collects information about each customer's use of the Netflix services, including, most notably, title selections and watch history, as well as the user's "IP address (which may tell us your general location)." NETFLIX PRIVACY STATEMENT, *supra* note 70.

275 *See, e.g.*, *Vosburgh*, 602 F.3d at 527 (recognizing that law enforcement entities, in conjunction with Internet Service Providers, can link a user's IP address to a specific household or residence).

Nickelodeon, *United States v. Vosburgh*, even the Third Circuit Court of Appeals found that "IP addresses are fairly 'unique' identifiers."[276]

Vosburgh involved allegations of child pornography tied to an IP address.[277] In that case, the court declared that "[t]he unique nature of the IP address assigned to [the individual at issue] made his attempts to access the [Internet Link] fairly traceable to his Comcast account *and the physical address* to which that account was registered."[278] For this reason, the court had no trouble finding that the user's IP address sufficiently connected him to criminal activity emanating from *his residence* for which he was deemed personally responsible (as opposed to a roommate, for example).[279] Aside from the unsympathetic nature of the defendant in *Vosburgh*, it is unclear why the Third Circuit did not follow this same rationale in *Nickelodeon*. Moreover, *Vosburgh* involved review of a magistrate's probable cause determination, which requires a mere "fair probability" of wrongdoing,[280] whereas *Nickelodeon* involved review of a Rule 12(b)(6) motion to dismiss under the relatively relaxed "plausibility" standards related to such motions.[281] Thus, the level of proof required in each case is not much different.

Another flaw in the *Nickelodeon* court's reasoning is the court's requirement that, to be personally identifying information, the disclosed data must *itself* identify a particular person.[282] First, very little data is *directly* identifying in this way. A list of movie rentals under the name, "John Smith," for example, would not allow an ordinary person to identify the particular "John Smith" from among thousands of people with the same name. Indeed, such a test would preclude a finding that even a home address or social security number, in isolation, is personally identifiable information. This

---

276 *Id.*

277 *Id.*

278 *Id.* (emphasis added).

279 *Id.* at 526-31 (upholding magistrate's probable cause determination based, in part, on evidence of IP address taking computer user to a particular address).

280 *See* Illinois v. Gates, 462 U.S. 213, 238 (1983) (adopting the fair probability standard for probable cause determinations); *Vosburgh*, 602 F.3d at 527 (applying the fair probability standard). In the context of probable cause determinations, the Supreme Court simply talks in terms of whether there is a "fair probability" of criminal activity and refuses to define probable cause via a numerical value. Nevertheless, the Court has provided guidance on this issue from time to time. *See* Texas v. Brown, 460 U.S. 730, 742 (1983) (stating that the probable cause standard does not "demand any showing that such a belief [of criminal activity] be correct or more likely true than false.").

281 *See* Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) ("The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully."); Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007) (requiring "only enough facts to state a claim to relief that is plausible on its face").

282 *See In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 284 (3d Cir. 2016), *cert. denied*, 137 S.Ct. 624 (2017) ("Our review of the legislative history convinces us that Congress's purpose in passing the [VPPA] was quite narrow: to prevent disclosures of information that would, with little or no extra effort, permit an ordinary recipient to identify a particular person's video-watching habits.").

cannot be correct.[283] As the *Yershov* district court (whose opinion was affirmed on this particular point) explained:

> [Opinions like *Nickelodeon*] seem to take an unrealistic view of the nature of personal identifiers, and how readily different databases or pieces of information can be linked together. The courts appear to frame the issue in large part by referring to these identifiers as "anonymous identifiers," which is unhelpful and possibly misleading . . . . [A] social security number or a date of birth, in isolation, is anonymous. However, it would be absurd to conclude that a social security number is not [personally identifiable information] simply because there is no publicly-available database linking those numbers with names.[284]

Likewise, by focusing its analysis on the "ordinary person" as the hypothetical recipient of data, cases like *Nickelodeon* fail to recognize the disclosure at issue for what it is. This is particularly true when the recipient is a company whose business includes building portfolios tied to individual persons, where success requires the ability to connect devices to individuals.[285] Connecting individuals to devices can, in fact, be accomplished quite easily. For one, consumers often identify themselves on their devices, for example, by logging into an account or using an e-mail address, thus enabling "companies [to] associate a consumer's activity on one device with activity they observe on other devices associated with that account."[286] In addition, linking readily available information can be effective at identifying an individual. For example, if Adobe is provided information that links an Android ID and GPS information to a specific video, as in *Yershov*, and links that information to data from other sources—such as GPS information linked to residential addresses, and residential addresses linked to names—it would be easy for Adobe to link the disclosed information to a particular person.[287] For this reason, connecting an Android ID to a person's

---

283 *Compare id.*, *with* 16 C.F.R. § 312.2 (2018) (defining "personal information" under COPPA as "individually identifiable information about an individual collected online," which includes, among others, the following: (1) A first and last name; (2) A home or other physical address including street name and name of a city or town; . . . (4) A screen or user name where it functions in the same manner as online contact information, as defined in this section; (5) A telephone number; (6) A Social Security number; (7) A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier; . . . (9) Geolocation information sufficient to identify street name and name of a city or town").

284 Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 145-46 (D. Mass. 2015), *rev'd on other grounds*, 820 F.3d 482 (1st Cir. 2016).

285 *See* FTC DATA BROKER REPORT, *supra* note 29, at 39-40. *Cf. In re* Hulu Privacy Litig., No. C 11-03764 LB, 2014 WL 1724344, at *11 (N.D. Cal. Apr. 28, 2014) (recognizing that "if an anonymous, unique ID were disclosed to a person who could understand it [such as a business that holds the "key" to de-anonymizing information], that might constitute PII").

286 *See* FED. TRADE COMM'N, CROSS-DEVICE TRACKING, *supra* note 41, at 3.

287 *See Yershov*, 104 F. Supp. 3d at 146.

name may not be difficult, especially for sophisticated third parties.[288] Thus, the *Nickelodeon* court's analysis seems shortsighted in the modern age.[289]

At a deeper level, what is striking about opinions like *Nickelodeon* is that courts seem to go to great lengths to reject VPPA claims premised on new technologies, and it is important to understand why. One potential explanation involves the ultimate use of the plaintiffs' data in cases like *Nickelodeon* to develop more effective advertising targeted to each particular plaintiff[290] vis-à-vis the ultimate use of the data disclosed in Robert Bork's case—essentially, to *publicly* embarrass the judge, a far more invasive use of the disclosed information.[291] In essence, the *Nickelodeon* court appears to have interpreted the term "personally identifiable information" narrowly not because the term requires a narrow interpretation, but rather to restrict the VPPA to the circumstances that led to its enactment.[292] Indeed, when the end result in *Vosburgh* was to affirm a criminal's conviction, the same court had no trouble finding that IP addresses are unique enough to identify a particular defendant,[293] further indicating that the court's desire to limit the VPPA's reach was the true driving force behind its interpretation.

At bottom, the Third Circuit's opinion in *Nickelodeon* is likely explained by its simple desire to limit VPPA claims to the types of disclosures that led to its enactment, particularly in the absence of explicit language making the statute applicable to modern video delivery formats.[294] This, in turn, suggests the need to amend the VPPA to clearly account for modern identifiers while recognizing what was so troubling about the Bork disclosure (public humiliation), as proposed in Part IV below.

D. *Whether Recipients of Information May be Sued Under the VPPA*

Another important issue under the VPPA is whether a plaintiff may sue not only the party that discloses personally identifiable information, but also

---

288 *See id.*

289 *See id.* at 145-46.

290 *See In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 269-70 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 624 (2017).

291 *See* McCabe, *supra* note 58, at 418-20 (describing the events leading to the VPPA's passage).

292 *See In re Nickelodeon*, 827 F.3d at 284 ("We do not think that, when Congress passed the [VPPA], it intended for the law to cover factual circumstances far removed from those that motivated its passage.").

293 United States v. Vosburgh, 602 F.3d 512, 526-27 (3d Cir. 2010) (recognizing that law enforcement entities, in conjunction with Internet Service Providers, have the ability to identify a user's IP address to a specific household or residence).

294 *See In re Nickelodeon*, 827 F.3d at 288-89 (addressing Congress's apparent reluctance to amend the statute to explicitly account for on-demand cable services and Internet streaming services). *Cf.* Robinson v. Disney Online, 152 F. Supp. 3d 176, 181 (S.D.N.Y. 2015) ("Whatever the impact of modern digital technologies on the manner in which personal information is shared, stored, and understood by third parties like Adobe, the Court cannot ascribe such an expansive intent to Congress in enacting the VPPA.").

the party that receives it. This issue has again generated a split among courts. The Third and Sixth Circuit Courts of Appeals allow VPPA claims only against parties that disclose personally identifiable information.[295] Other courts, including the Tenth Circuit Court of Appeals, also permit recipients to be sued.[296]

The question of who may be sued under the VPPA involves a difficult issue of statutory interpretation.[297] Subsection (b) of the VPPA specifically prohibits a "video tape service provider" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider,"[298] and subsection (c) explicitly declares that "[a]ny person aggrieved by any act of a person in violation of this section may bring a civil action in a United States District Court."[299] When read together, these provisions suggest that the "civil action" referenced in subsection (c) may be brought only against a party that "discloses" personally identifiable information, as only the disclosure of such information is made unlawful in subsection (b). As the Third and Sixth Circuit Courts of Appeals have noted, only a "video tape service provider" can be liable under the plain language of subsection (b), and the only type of conduct that results in liability under that section is the *disclosure* of personally identifiable information, rather than its *receipt*.[300] The Seventh Circuit Court of Appeals endorsed essentially the same reading of the statute in *Sterk v. Redbox Automated Retail, LLC*.[301] Although *Sterk* involved a distinct issue of interpretation,[302] the *Sterk* court

---

295 *See In re Nickelodeon*, 827 F.3d at 267. *Cf.* Daniel v. Cantrell, 375 F.3d 377, 382-83 (6th Cir. 2004) (limiting the liability of individuals to whom personally identifiable information was disclosed to disclosures under 18 U.S.C. 2710(a)(4)).

296 *Cf.* Camfield v. City of Oklahoma City, 248 F.3d 1214, 1220-21 (10th Cir. 2001). The district court had allowed suit against the recipients of personally identifiable information. While this determination was not appealed, the Tenth Circuit Court of Appeals did not *sua sponte* reverse.

297 Sterk v. Redbox Automated Retail, LLC, 672 F.3d 535, 538 (7th Cir. 2012) (noting that the VPPA is "not well drafted," and that "[t]he biggest interpretative problem is created by the statute's failure to specify the scope of subsection (c), which creates the right of action on which this lawsuit is based"); *In re Nickelodeon*, 827 F.3d at 278-79 (noting that the statute is "'not well drafted', requiring us to begin by summarizing a bit of legislative jargon").

298 Video Privacy Protection Act, 18 U.S.C. § 2710(b) (2012). *See also In re Nickelodeon*, 827 F.3d at 279 (stating the requirements of a VPPA claim); Mollett v. Netflix, Inc., 795 F.3d 1062, 1066 (9th Cir. 2015) (same). The VPPA sets a minimum penalty of $2,500 per violation; allows a plaintiff to recover punitive damages, reasonable attorney's fees, and litigation costs; and empowers district courts to provide appropriate equitable relief. 18 U.S.C. § 2710(c); *In re Nickelodeon*, 827 F.3d at 279.

299 18 U.S.C. § 2710(c).

300 *See In re Nickelodeon*, 827 F.3d at 281; *Daniel*, 375 F.3d at 381-82 (noting that an individual who receives personally identifiable information is only liable under the circumstances articulated in 18 U.S.C. § 2710).

301 672 F.3d 535, 538-39 (7th Cir. 2012).

302 *Sterk* involved a distinct issue regarding subsection (e) of the VPPA, 18 U.S.C. § 2710(e), which provides that "[a] person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the

read subsection (c) to pertain only to the provisions preceding it.[303] This reading eliminated a cause of action for perceived violations of subsections (d) and (e), which together prevent information obtained in violation of the VPPA from being received in evidence and require personally identifiable information to be destroyed after the information is no longer necessary for the purpose for which it was collected.[304] In addition, the court stated that "[u]nlawful *disclosure* is the only misconduct listed in the statute for which an award of damages is an appropriate remedy,"[305] thus ratifying what is essentially the view of the Third and Sixth Circuit Courts of Appeals.[306]

Although the most logical reading of the VPPA is that it allows suits only against parties who disclose information improperly, rather than recipients of such information,[307] some courts have endorsed an alternative view, perhaps best articulated by the United States District Court for the Western District of Washington.[308] According to that court, subsection (c) of the VPPA (the provision authorizing civil suits), broadly permits civil suits for "any act of a person in violation of this section,"[309] and while one "violation of this section" occurs when "[a] video tape service provider . . . knowingly discloses . . . personally identifiable information concerning any consumer of such provider,"[310] the statute can also be violated, in that court's view, "when personally identifiable information is *obtained* from a video tape service provider in any manner other than as narrowly provided by the [statute]."[311]

To explain, subsection (b)(2) of the statute provides various exceptions authorizing video tape service providers to disclose personally identifiable information for certain, limited purposes.[312] For example, under the third listed exception, "[a] video tape service provider may disclose personally identifiable information . . . to a law enforcement agency pursuant to a [valid] warrant, . . . a grand jury subpoena, or a court order."[313] Under the Western District of Washington's view, this means that a law enforcement agency

---

purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (b)(2) or (c)(2) or pursuant to a court order." *See Sterk*, 672 F.3d at 536.

303 *See Sterk*, 672 F.3d at 538-39.

304 *Id.*

305 *Id.* at 539 (emphasis added).

306 *See In re Nickelodeon*, 827 F.3d at 267. *Cf. Daniel*, 375 F.3d at 382-83 (limiting the liability of individuals who receive personally identifiable information under 18 U.S.C. § 2710(a)(4)).

307 The statute's basic prohibitions and exceptions are, after all, specifically directed to those who make the types of disclosures at issue. *See* Video Privacy Protection Act, 18 U.S.C. § 2710(b)(1) (2012) (identifying "[a] video tape service provider who knowingly discloses"); *id.* § 2710(b)(2) (noting that "[a] video tape service provider may disclose").

308 Amazon.com LLC v. Lay, 758 F. Supp. 2d 1154, 1167 (W.D. Wash. 2010).

309 18 U.S.C. § 2710(c).

310 *Id.* § 2710(b)-(c).

311 *Amazon.com*, 758 F. Supp. 2d at 1167 (emphasis added).

312 18 U.S.C. § 2710(b)(2)(A)–(F).

313 *Id.* § 2710(b)(2)(C).

violates the VPPA by improperly obtaining personally identifiable information, for example, by coercing a disclosure via an invalid warrant.[314] Although the VPPA does not explicitly make law enforcement personnel civilly liable to the aggrieved person for such conduct,[315] the court deemed it "logical that suits can be brought against those who receive personally identifiable information in violation of the [VPPA]."[316] This is true, in the court's view, even though "video tape service providers" are the only entities expressly included as a person who "can be liable" in subsection (b)(1).[317]

A similarly expansive view of the VPPA was articulated in the first case decided under the statute, *Dirkes v. Borough of Runnemede*.[318] In that case, the plaintiff, a former police officer with the Borough of Runnemede Police Department ("Department"), sued the Department, the Borough of Runnemede ("Borough"), and Lieutenant Emil Busko ("Lt. Busko"), after Lt. Busko obtained from "Videos To Go" the names and rental dates of pornographic videos rented by the plaintiff and his wife.[319] In seeking to obtain this information, Lt. Busko failed to secure a warrant, a subpoena, or court order; rather, he simply requested and received the information from an employee of Videos To Go without question.[320] Lt. Busko subsequently used the information as evidence at plaintiff's disciplinary hearing, which involved an allegation that plaintiff had improperly removed pornographic materials from a decedent's apartment, leading to his termination.[321]

Examining plaintiff's VPPA claim, the court determined that two distinct VPPA violations had occurred.[322] The first violation occurred when Videos To Go violated subsection (b) of the statute by disclosing plaintiff's video rental information to Lt. Busko, while the second violation occurred under subsection (d)[323] when plaintiff's personally identifiable information was received into evidence at his disciplinary hearing.[324] As for whether Lt. Busko, the Department, and the Borough were proper defendants, the court emphasized the "clear intent" of the VPPA "to prevent the disclosure of private information" and enable consumers to maintain control over their private information, adding that "[t]his purpose is furthered by allowing

---

314 *Amazon.com*, 758 F. Supp. 2d at 1167.

315 *Cf.* 18 U.S.C. § 2710(b)(1).

316 *Amazon.com*, 758 F. Supp. 2d at 1167.

317 *Id.*

318 936 F. Supp. 235 (D.N.J. 1996).

319 *Id.* at 236.

320 *Id.*

321 *Id.* at 236-37.

322 *See id.* at 239-40.

323 Video Privacy Protection Act, 18 U.S.C. § 2710(d) (2012) (providing that "[p]ersonally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, or other proceeding").

324 *Dirkes*, 936 F. Supp. at 239-40. *See also id.* at 239 (identifying three distinct ways in which the VPPA can be violated).

parties . . . to bring suit against those individuals who have come to possess (and who could disseminate) the private information in flagrant violation of the purposes of the [VPPA]."[325] Accordingly, the court held that "those parties who are in possession of personally identifiable information as a direct result of an improper release of such information are subject to suit under the [VPPA]," including the three defendants in the case.[326]

Although this Article is primarily focused on the other three issues of VPPA interpretation, it makes sense to allow suits to be brought against not only disclosing parties, such as the video store clerk who willingly leaked the Robert Bork information, but also certain culpable recipients of protected information, such as a police officer who presents a fake warrant to force the disclosure of protected information.[327] In the former case, the video store clerk is most clearly at fault for the privacy invasion, whereas in the latter case, the recipient is truly to blame. Nevertheless, for this view of the statute to be consistently endorsed by courts, the statute's language should be amended to make the point clearer.[328]

IV. PROPOSALS

Nearly all courts agree that the VPPA is unclear and ambiguous, particularly as it relates to modern forms of video dissemination,[329] making the statute ripe for revision. This Part includes the following proposals: Section A suggests defining the VPPA term "subscriber" to encompass modern video delivery formats, including videos viewed through smartphone apps. Section B posits redefining "personally identifiable information" to include static digital identifiers, such as IP addresses and device serial numbers. Section C suggests increasing the VPPA's penalty provisions for particularly egregious disclosures reminiscent of the disclosure that led to the statute's enactment.

---

325 *Id.* at 240.

326 *Id.*

327 Such ruses have occurred, albeit in unrelated contexts. *See, e.g.*, Bumper v. North Carolina, 391 U.S. 543 (1968) (involving a police officer who falsely told a resident he had a search warrant, causing the resident to let him in, leading to a dispute over whether the resident had lawfully consented to the officer's entry).

328 *See Dirkes*, 936 F. Supp. at 240 (recognizing that subsection (c) of the VPPA "does not delineate those parties against whom an action may be instituted"). *See generally* Sterk v. Redbox Automated Retail, LLC, 672 F.3d 535, 538 (7th Cir. 2012) (wrestling with the unclear statutory language).

329 *See In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 284 (3d Cir. 2016), *cert. denied*, 137 S.Ct. 624 (2017) (stating that "the proper meaning of the phrase 'personally identifiable information' is not straightforward"); Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 486 (1st Cir. 2016) (recognizing that the term "'personally identifiable information' is awkward and unclear"). *See generally Sterk*, 672 F.3d at 538 (stating that the VPPA "is not well drafted," and pointing out an obvious typographical error in the statute).

A. *Defining "Subscriber" Within the VPPA*

As noted, the VPPA prohibits video tape service providers from knowingly disclosing personally identifiable information concerning any "consumer of such provider," except in the circumstances authorized by the statute.[330] As such, the VPPA's protections apply only to "consumers,"[331] defined as "any renter, purchaser, or subscriber of goods or services from a video tape service provider."[332]

Regarding the VPPA's application to modern technologies, litigation has focused on the term "subscriber"[333] more specifically as it pertains to downloading a free app on a smartphone,[334] or downloading a channel on a device like Roku.[335] Most courts agree that payment is not required to make one a "subscriber" under the VPPA.[336] With respect to smartphone apps, then, the question becomes whether simply downloading a free app on a smartphone and using the app to watch videos makes one a "subscriber."[337] Here is where the courts disagree. In the Eleventh Circuit's view, downloading an app is akin to adding a particular website to one's Internet browser as a favorite, which falls short of "subscriber" status given that it entails no ongoing "commitment, relationship, or association (financial or otherwise)" between the user and the app owner.[338] In the First Circuit's view, however, installing an app on one's phone "establish[es] seamless access to an electronic version of [the content offered in the app]," thereby "establish[ing] a relationship with [the provider] that is materially different from what would have been the case had [the provider] simply remained one of millions of sites on the web" that could be accessed through a web browser.[339]

At bottom, the disagreement between the First and Eleventh Circuit is difficult to resolve without resorting to hair-splitting distinctions having little to do with whether the VPPA should apply to modern video-delivery formats. To avoid further development of such hair-splitting distinctions among

---

330 Video Privacy Protection Act, 18 U.S.C. § 2710(b)(1) (2012).

331 *Id.*

332 *Id.* § 2710(a)(1).

333 *See supra* Part III.0.

334 *See Yershov*, 820 F.3d at 484; Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1253-54 (11th Cir. 2015).

335 *See, e.g.*, Locklear v. Dow Jones & Co., 101 F. Supp. 3d 1312, 1315-16 (N.D. Ga. 2015) (involving a Roku download).

336 *See Yershov*, 820 F.3d at 488; *Ellis*, 803 F.3d at 1255-56; *Locklear*, 101 F. Supp. 3d at 1316; *In re* Hulu Privacy Litig., No. C 11-03764 LB, 2014 WL 1724344, at *8 (N.D. Cal. Apr. 28, 2014).

337 *See, e.g.*, *Locklear*, 101 F. Supp. 3d at 1315-16 (finding plaintiff had pled sufficient facts to qualify her as a "subscriber" under the VPPA, and therefore a "consumer," by alleging that she downloaded the *Wall Street Journal Live Channel* on Roku and used it to watch video clips).

338 *See Ellis*, 803 F.3d at 1256-57.

339 *See Yershov*, 820 F.3d at 489.

courts, this Article proposes a simple amendment to the VPPA that would define the term "subscriber" to include persons who download, install, and use any mobile application to access videos or similar audiovisual materials on one's smartphone, regardless of whether monetary payment is made. Regarding websites, the proposed definition would also clarify that merely visiting a website to view videos—without having paid for the site's content, registering for an account, establishing a user ID or profile, downloading an app or program, or taking any action to associate the user with the website's owner—does not make one a "subscriber."[340]

Regarding smartphones, this proposed revision is necessary to modernize the VPPA and ensure that its protections cover new technologies, as Congress originally intended.[341] The VPPA is a remedial statute that should be applied broadly, particularly as it pertains to new technologies.[342] Indeed, the Senate Report reflects an acute concern for ensuring privacy as technology progresses, and confirms that Congress was concerned with protecting the confidentiality of private information about viewing preferences regardless of media format.[343] As such, the term "subscriber" should be statutorily defined to include persons who download, install, and use any mobile application to access videos or similar audio visual materials on one's smartphone, regardless of whether monetary payment is made. With these considerations in mind, this Article proposes the following statutory language:

> The term "subscriber" includes, but is not limited to, a cell phone, tablet, laptop, computer, or similar device operator who downloads any video-delivery service or cell phone application and uses such service or application to view videos on the device, regardless of whether monetary payment is made. The term does not include visiting an Internet website to view videos without having paid for the site's content, registering for an account, establishing a user ID or profile, downloading an app or program, or taking any action to associate the user with the website's owner.

B. *Modernizing the VPPA Definition of "Personally Identifiable Information"*

To solidify the VPPA's application to modern video delivery formats, this Article further proposes an amendment to the VPPA that would define the term "personally identifiable information" to encompass most static digital identifiers.

---

340 *See* Austin-Spearman v. AMC Network Entm't, LLC, 98 F. Supp. 3d 662, 669-70 (S.D.N.Y. 2015) (adopting this view of the VPPA and requiring VPPA plaintiffs to engage in an "ongoing relationship with the provider initiated by the plaintiff's own actions").

341 *See supra* Part III.0.

342 *See In re* Hulu Privacy Litig., No. C 11–03764 LB, 2012 WL 3282960, at *6 (N.D. Cal. Aug. 10, 2012); Dirkes v. Borough of Runnemede, 936 F. Supp. 235, 241 (D.N.J. 1996).

343 *In re Hulu Privacy Litig.*, 2012 WL 3282960, at *6.

One model for such a proposal is the Children's Online Privacy Protection Act ("COPPA"),[344] which prohibits certain disclosures of a child's "personal information" online.[345] COPPA was enacted ten years after the VPPA,[346] and explicitly authorizes the FTC to update the statute's definition of "personal information" to include "any other identifier that the [FTC] determines permits the physical or online contacting of a specific individual."[347] In 2013, the FTC implemented regulations that extend COPPA's definition of "personal information" to include "[a] persistent identifier that can be used to recognize a user over time and across different Web sites or online services," such as "a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier."[348]

This Article's proposal would borrow from the FTC's definition of "personal information" under COPPA to create a new, similar definition of "personally identifiable information" under the VPPA. However, unlike the COPPA definition, this Article's proposed definition would take context into account by making static digital identifiers "personally identifying" only where the *particular recipient* of the information is reasonably likely to identify the particular consumer. The proposed definition of "personally identifiable information" is as follows:

> The term "personally identifiable information" means any information–including but not limited to IP addresses, GPS coordinates, Android ID's, and unique device identifiers–which the recipient of such information may use, either alone or in combination with other information readily available to the recipient, to identify a person or a member of such person's household as having requested or obtained specific video materials or services from a video tape service provider.

In recent cases involving interpretations of the current VPPA definition of "personally identifiable information," courts have usually phrased the issue as a choice between a test that focuses on the "ordinary recipient's" ability to identify a particular person using solely the information disclosed on the one hand, and one that examines whether the *particular recipient* of the data could *theoretically* determine the user's identity on the other.[349] Each of these tests depends on a fiction—the former by ignoring the actual recipient, and the latter by ignoring the true capabilities of that recipient—and are thus similarly flawed. By focusing on the particular recipient of a

---

344 15 U.S.C. §§ 6501-6506 (2012).

345 *See id.* § 6502.

346 *See In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 286 (3d Cir. 2016) (citing Pub. L. No. 105-277, Div. C, Title XIII, §§ 1301–1308, 112 Stat. 2681–728, codified at 15 U.S.C. §§ 6501–6506).

347 15 U.S.C. § 6501(8).

348 16 C.F.R. § 312.2 (2018) (definition of "personal information").

349 *See In re Nickelodeon*, 827 F.3d at 284, 290 ("In 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.").

disclosure and that recipient's actual ability to identify a particular user with information readily available to the recipient, this Article's proposal will force courts to more directly consider the true nature of any particular disclosure. In addition, because this proposed definition will focus on uncovering the *actual ability* of the *actual recipient* to identify the user at issue based on the particular digital identifier, the proposed definition will likely push most cases beyond the motion to dismiss stage, thus enabling discovery to be conducted on the identification question. This, in turn, will provide much needed clarity regarding the true capability of data brokers and companies like Adobe and Google to identify individuals from facially anonymous digital data.[350] If discovery proves that no such identification is possible, the VPPA will not apply, but where it is, the statute will prohibit the disclosure (in the absence of a statutory exception). Under this Article's proposal, it is anticipated that disclosures to data brokers, whose business depends on tying data to individual persons, would generally be covered by the VPPA, whereas similar disclosures to "ordinary persons" would not.[351]

One possible criticism of this Article's proposed definition is that static digital identifiers, such as IP addresses, only permit identification of a device, rather than an individual. The First Circuit Court of Appeals in *Yershov* effectively rejected this argument,[352] and for good reason. After all, the Bork disclosure involved the movies the entire Bork family had rented, yet that did not alter the privacy concerns that led to the VPPA's enactment, reflecting a larger concern with the underlying data rather than the ability to pinpoint any particular movie viewer. In addition, the FTC carefully considered this very argument in 2013, when it considered whether to modernize the definition of "personal information" under COPPA.[353] After receiving public comments on its proposed rule—many positing that digital identifiers only permit contact with a device, not a specific individual[354]—the FTC chose to stand by its proposal, leading to the current COPPA rule, declaring: "The Commission

350 *See* FTC DATA BROKER REPORT, *supra* note 29, at 4 (reporting that, "[f]or decades, policymakers have expressed concerns about the transparency of companies that buy and sell consumer data"); *id.* at 6-7 (noting that "[i]n September 2013, the U.S. Government Accountability Office released a report on the practices of data brokers and concluded that Congress should consider legislation to reflect the challenges posed by changes in technology, the increased market for consumer information, and the lack of transparency of the data broker industry").

351 *See* Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 486 (1st Cir. 2016) (finding that "when Gannett makes such a disclosure to Adobe, it knows that Adobe has the 'game program,' so to speak, allowing it to link the GPS address and device identifier information to a certain person by name, address, phone number, and more," such that "the linkage of information to identity . . . is both firm and readily foreseeable to Gannett").

352 *See id.* (finding that the combination of Android ID and the device's GPS coordinates at the time a video is viewed "effectively reveal[s] the name of the video viewer").

353 *See* Children's Online Privacy Protection Rule, 77 Fed. Reg. 46643 (proposed Aug. 6, 2012) (to be codified at 16 C.F.R. § 312.2), *available at* 2012 WL 3150184. *See also* Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972, 3972 (Jan. 17, 2013) (to be codified at 16 C.F.R. § 312.2).

354 *See* Children's Online Privacy Protection Rule, 78 Fed. Reg. at 3979.

continues to believe that persistent identifiers permit the online contacting of a specific individual . . . [and] is not persuaded by arguments that persistent identifiers only permit the contacting of a device."[355] The FTC further noted that "[m]ultiple people often share the same phone number, the same home address, and the same email address, yet Congress still classified these, standing alone, as 'individually identifiable information about an individual.'"[356] In the VPPA context, Congress should likewise deem it irrelevant, for purposes of defining "personally identifiable information," that multiple persons could utilize the same device.

C. *Remembering Bork: Enhanced VPPA Penalties for Disclosures Likely to be Disseminated to the Public-at-Large*

As argued above, amending the VPPA to encompass digital identifiers such as Android IDs and IP addresses is necessary to bring the statute up to date with modern video delivery methods and directly confront the ability of sophisticated recipients to identify individuals through such identifiers. To accomplish this task as efficiently as possible, this Article proposes amending the VPPA's definition of "personally identifiable information" to encompass any information—including IP addresses, device serial numbers, and unique device identifiers—that permits the recipient of such information to identify either a person or a member of such person's household as having requested or obtained specific video materials or services from a video tape service provider. This proposed amendment, however, does not fully address the apparent, underlying concerns of courts that have dismissed seemingly valid VPPA claims.

Arguably, courts seem to have gone out of their way to dismiss claims under the VPPA that appear to fit within the statute's reach, particularly given the statute's current definition of "video tape service provider."[357] Reading between the lines, this is because most modern VPPA claims bear little resemblance to the disclosure that occurred in the Robert Bork case.[358] The Bork disclosure, which led to the VPPA's enactment, was so troubling because it was *completely public*.[359] Yet, most modern VPPA claims, although technically involving a disclosure of personally identifiable information by one party to another, do not resemble the embarrassing public

---

355 *Id.* at 3980.

356 *Id.*

357 *See* discussion *supra* Part 0.

358 *See* Mollett v. Netflix, Inc., 795 F.3d 1062, 1065 (9th Cir. 2015) (noting that the *Washington City Paper* detailed 146 films that the Bork family had rented from an area video store). *See also* Peterson, *supra* note 5(reporting that, other than the sheer number of movies Bork and his family had rented over the two-year period, the reporter did not uncover anything too shocking, aside, perhaps, from Hitchcock and costume dramas).

359 *See* S. REP. NO. 100-599, at 5 (1988).

disclosure that occurred in the Bork case.[360] Indeed, unlike Bork, most consumers whose information has been disclosed to a third party like Adobe or Google would have no idea that a transfer of information had even occurred. Accordingly, to directly account for the type of public disclosure that occurred in the Bork case, where privacy concerns are heightened,[361] this Article proposes an amendment to the VPPA that would increase the statute's penalty provisions for disclosures of personally identifiable information reasonably likely to be made public.

As Fourth Amendment case law illustrates, privacy invasions can be as simple as a single police officer conducting an unreasonable search and thereby obtaining private information in an unlawful manner.[362] Although the general public may never learn about such a privacy breach, particularly where the prosecution elects not to pursue criminal charges due to the officer's misconduct, the privacy invasion is nevertheless just as real. Thus, limiting the VPPA to cover only disclosures of personally identifiable information reasonably likely to be made public is not the right solution; instead, the VPPA should continue to punish those who disclose information to data brokers, who in turn use such information to build and profit from digital dossiers on individuals, and should increase the penalties associated with a public breach.

Presently, the VPPA sets a minimum penalty of $2,500 per violation; allows a plaintiff to recover punitive damages, reasonable attorney's fees, and litigation costs; and empowers district courts to provide appropriate equitable relief.[363] Under this Article's proposal, the VPPA's penalty provisions would provide a minimum penalty of $7,500 per violation (treble damages) for disclosures of personally identifiable information, like the Robert Bork disclosure, that are reasonably likely to be made public.

---

360 *See Mollett*, 795 F.3d at 1065 (noting that the *Washington City Paper* disclosed 146 films that the Bork family had rented from an area video store).

361 *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890) (discussing the general right to privacy and equating it with "the more general right of the individual to be let alone"); *id.* at 214-15 (arguing that "[t]he design of the law [of privacy] must be to protect . . . persons . . . from being dragged into an undesirable and undesired publicity and to protect all persons . . . from having matters which they may properly prefer to keep private, made public against their will"); *id.* at 218 ("a private communication or circulation for a restricted purpose is not a publication within the meaning of the law").

362 Although there are countless case illustrations, two Supreme Court cases that illustrate the privacy invasion that occurs when police violate a person's Fourth Amendment rights include Riley v. California, 134 S. Ct. 2473 (2014) (finding Fourth Amendment violated in case where defendant was stopped on highway for driving with expired registration tags, officers arrested defendant and searched his car and cell phone's digital contents, including its videos and photographs) and Mapp v. Ohio, 367 U.S. 643 (1961) (involving a search where officers forced open a door to Mapp's house, kept her lawyer from entering, brandished a false warrant, then forced her into handcuffs and searched her entire house for a bombing suspect, finding no suspect but seizing allegedly obscene materials used to prosecute her).

363 *See* Video Privacy Protection Act, 18 U.S.C. § 2710(c) (2012); *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 279 (3d Cir. 2016).

CONCLUSION

When the VPPA was enacted, consumers obtained movies on VHS cassette tapes.[364] Today, "on-demand" television and Internet streaming allow consumers to watch movies and videos on smart televisions, computers, and cell phones. Although the VPPA was designed to preserve privacy with respect to a consumer's choice of "video tapes or similar audio visual materials," arguably permitting the statute to reach more modern video delivery formats, the statute has not been significantly revised since 1988, leaving thirty-year-old statutory cracks through which modern forms of identification have fallen.

To modernize the statute, the outdated VPPA definition of "personally identifiable information" should be replaced with a more modern one that encompasses common static digital identifiers such as a customer number held in a cookie or an IP address. Likewise, the VPPA should be amended to protect individuals who download and use smartphone apps to view movies and videos. Finally, the VPPA's penalty provisions should be amended to increase the penalty for disclosures of personally identifiable information that, like the Robert Bork disclosure, are reasonably likely to be made public.

364 *See* S. REP. NO. 100-599, at 9, 12, 17 (1988).