"HELLO, MY NAME IS USER #101": DEFINING PII UNDER THE VPPA

Yarden Z. Kakon†

I. INTRODUCTION

During Judge Robert Bork's 1987 Supreme Court nomination hearings, a Washington D.C. newspaper obtained a list of 146 videotapes the Bork family previously rented from their local video store. Using this list, the newspaper published a profile of Judge Bork that described his video rental history. The Senate Judiciary Committee was outraged by the newspaper's acquisition and publication of Bork's rentals, and Congress quickly thereafter adopted an act that would protect video-watching histories. The Video Privacy Protection Act (VPPA) was born. The VPPA enhanced the concept of privacy for individuals in their daily lives by defining the right to be protected against unauthorized disclosures of personal information held by videotape providers.[1]

The VPPA creates a private cause of action.[2] To state a claim under the VPPA, a plaintiff must allege that "[a] video tape service provider . . . knowingly disclose[d], to any person, personally identifiable information concerning any consumer of such provider."[3] The VPPA defines personally identifiable information (PII) as "includ[ing] information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."[4]

Congress passed the VPPA "[to] preserve personal privacy with respect to the rental, purchase or delivery of video tapes or similar audio-visual materials."[5] However, with the shift from video rental stores to online streaming, what does the VPPA mean today? Federal courts have struggled to

DOI: https://doi.org/10.15779/Z384X54G9X

† J.D. Candidate, 2019, University of California, Berkeley, School of Law.

1. *See* S. REP. NO. 100-599 (1988).

2. 18 U.S.C. § 2710 (2012); *see* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 278 (3d Cir. 2016).

3. 18 U.S.C. § 2710(b)(1).

4. *See* § 2710(a)(3)(4) ("video tape service provider" means "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").

5. *See* S. REP. NO. 100-599 (1988) at 1.

apply the VPPA to modern day technology and practices.[6] In particular, courts have struggled to define the bounds of PII under the statute.[7] The majority of courts have adopted a narrow definition of PII, holding that disclosed information cannot constitute PII if it requires additional information to identify the person.[8] In contrast, a minority of courts have held that PII may include information that requires an entity to use "reasonable and foreseeable" additional resources to identify the user.[9]

The problem of PII is uniquely challenging in the context of the VPPA because the cause of action itself is predicated on whether a third party or entity can actually identify the user, based on his or her video-watching history. While a chatty cashier may have disclosed Judge Bork's rental history, current processes for storing and disclosing video-watching history are far more complex. More specifically, courts are divided regarding whether digital identifiers—forms of identification used generally to link a user to a specific device or browsing activity—constitute PII.

This Note seeks to understand the scope of PII under the VPPA and propose the best approach to analyzing whether specific digital identifiers should constitute PII. Part II introduces digital identifiers and discuss the technical concepts that are key to understanding the arguments made in current PII litigation.[10] Part III reviews the VPPA's legislative history and discuss congressional intent. Part IV provides an overview of case law defining

6. Gregory M. Huffman, *Video-Streaming Records and the Video Privacy Protection Act: Broadening the Scope of Personally Identifiable Information to Include Unique Device Identifiers Disclosed with Video Titles*, 91 CHI.-KENT. L. REV. 737 (2016).

7. *Id.*

8. *See* Eichenberger v. ESPN, Inc., 876 F.3d 979, 985 (9th Cir. 2017) ("We adopt the Third Circuit's 'ordinary person' standard. The 'ordinary person' test better informs video service providers of their obligations under the VPPA."); *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 267 (3d Cir. 2016) ("[P]ersonally identifiable information applies only to the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior."); Ellis v. Cartoon Network, Inc., 2014 WL 5023535, at *3 (N.D. Ga. Oct. 8, 2014), *aff'd on other grounds*, 803 F.3d 1251 (11th Cir. 2015) ("PII not disclosed where the third party to whom an Android ID and viewing history were provided had to 'collect information from other sources' to identify the plaintiff."); Locklear v. Dow Jones & Co., 101 F. Supp. 3d 1312, 1318 (N.D. Ga. 2015), *abrogated on other grounds*, 803 F.3d 1251 (11th Cir. 2015) ("[A] Roku serial number, without more, is not akin to identifying a particular person, and therefore, is not PII." (quotations omitted)).

9. *See* Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 486 (1st Cir. 2016) ("PII can embrace information reasonably and foreseeably likely to reveal . . . videos [the plaintiff] has obtained." (quotations omitted)); *see also In re* Vizio, Inc., Consumer Privacy Litig., 238 F. Supp. 3d 1204, 1225 (C.D. Cal. 2017).

10. *Infra* Part II.

the scope of PII with respect to digital identifiers.[11] Part V will compares my analysis of legislative intent with that of the courts discussed in Part IV.[12] Part VI then revisits the current approaches in light of the legislative history. Lastly, Part VII concludes.

II. DIGITAL IDENTIFIERS AND RE-IDENTIFICATION

Almost every interaction that a user makes on the Internet is collected, recorded, and stored as data.[13] One reason an entity may collect data is to enhance the user's experience on that site.[14] For instance, Netflix analyzes user preferences to recommend movies, and Google reviews search queries to improve search results.[15] Furthermore, some entities will also choose to sell or share their aggregated data with third parties, such as analytics or marketing companies.[16] Services such as Live Ramp offer their clients a way to sort and analyze data in order to re-identify users to enable better marketing strategies.[17] In a recent trend of VPPA cases, plaintiffs are suing defendants for alleged unauthorized sharing of their PII, in the form of digital identifiers, with third-party marketing firms.[18]

A. DIGITAL IDENTIFICATION

To best tailor marketing to individual consumers, companies must understand consumer behavior across various platforms. Thus, companies must find ways to link consumers to their many devices, services, websites, and applications. Companies can associate multiple devices with the same person using cross-device tracking, connecting a single user across multiple devices through the user of digital identifiers.[19] Digital identifiers come in many forms and companies have adopted several techniques to use these identifiers to precisely identify a person and link his or her activities to specific services, devices or websites, and sometimes across devices and applications.[20]

---

11. *Infra* Part IV.
12. *Infra* Part V.
13. Boris Lubarsky, *Re-Identification of "Anonymized Data"*, 1 GEO. L. TECH. REV. 202, 202 (2017).
14. *Id.*
15. *Id.*
16. *Id.*
17. *Applying Identity Link*, LIVE RAMP, https://liveramp.com/applying-identitylink/ [https://perma.cc/5ZDU-3LB4] (last visited Feb. 20, 2019).
18. *See, e.g.*, *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 281 (3d Cir. 2016), *cert. denied sub nom.* C. A. F. v. Viacom Inc., 137 S. Ct. 624 (2017).
19. FEDERAL TRADE COMMISSION STAFF REP., *Cross-Device Tracking* (Jan. 2017) at 2.
20. *Id.* at 2–3.

Some digital identifiers are supplied by hardware manufacturers, such as Google or Apple.[21] An example of a hardware manufacturer-supplied digital identifier is a device's Android ID, which is a "persistent unique identifier," meaning it is unique to a specific device and user.[22] Another form of an assigned digital identifier is an Internet Protocol (IP) address, which is a designation that links all of your Internet activity to where you're using it from.[23] Generally, an IP address functions like a home address for a computer or device.[24] Other forms of digital identifiers can be created while browsing websites on the Internet, like a cookie.[25] A cookie is information saved by the web browser and is stored on the device by either the site visited, first party cookies, or someone else, third-party cookies.[26] A cookie's purpose is to allow the website to keep track of a user's identity over time in order to customize a user's browsing experience.[27] However, cookies, by the nature of their use, can be used to track users for other reasons.[28] Once an entity has access to multiple databases of identifiers, either through the collection of first-party services or third-party tracking on other platforms,[29] it can create individualized profiles of users that combine the data collected.[30] This allows marketing and analytic companies to develop an understanding of users' digital activities by collecting

21. Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 138 (D. Mass. 2015), *rev'd,* 820 F.3d 482 (1st Cir. 2016).

22. *User Data & Identity*, ANDROID DEVELOPERS, https://developer.android.com/training/articles/user-data-ids.html [https://perma.cc/36KH-KPCA] (last visited Feb. 20, 2019).

23. John-Michael Bond, *What Is an IP address—and How Do You Find It*, DAILY DOT, https://www.dailydot.com/debug/what-is-an-ip-address/ [https://perma.cc/WE84-H5BZ] (last visited Feb. 20, 2019).

24. *Id.*

25. *Online Tracking*, FED. TRADE COMMISSION (June 2016), https://www.consumer.ftc.gov/articles/0042-online-tracking [https://perma.cc/328L2T7W].

26. *Id.*

27. *Id.*

28. *See id.*

29. *See* FED. TRADE COMM'N, CROSS-DEVICE TRACKING: A FEDERAL TRADE COMMISSION STAFF REPORT 1 (2017) ("Cross-device tracking is most easily performed by first-party services with a direct relationship with the consumer—for example, an email service that a consumer logs onto from different devices. However, third-party companies are tracking consumers with increasing accuracy, correlating user behavior across multiple platforms.").

30. *See id.* ("[C]ompanies can analyze an individual consumer's activities based not only on her habits on one browser or device, but on her entire 'device graph'—the map of devices that are linked to her, her household, or her other devices.").

detailed information about the consumer from a variety of sources.[31] This incentivizes entities to aggregate increasingly more diverse data from users for a clearer picture of their habits.

B. LEVELS OF IDENTIFIABILITY

As discussed in *In re Nickelodeon Consumer Privacy Litigation* ("*Nickelodeon*"), information that may qualify as personally identifiable runs on a spectrum of identifiability.[32] At one end of the spectrum lies direct identifiers—information such as a name, phone number, or physical address that can identify an individual on its own, or by reference to readily available databases.[33] Direct identifiers can be further divided into public direct identifiers and private direct identifiers. Information that identifies an individual via reference to a public source (public direct identifier) is considered more identifiable than information that requires reference to a private source, such as a credit reporting agency or government bureau (private direct identifier).[34] For example, a telephone number would be considered a public direct identifier and a social security number would be a private direct identifier. Under the VPPA, public direct identifiers are the most obvious cases of PII because an individual can be directly identified if this information was associated with publicly available video watching history.[35]

Second, on the other end of the spectrum lie indirect identifiers—information that indirectly links back to an individual, but may be used together or in conjunction with other information to identify an individual. In the context of VPPA litigation, disputed forms of indirect identifiers include GPS coordinates, unique device identifiers, like an Android ID, and IP addresses.[36] Entities use these indirect digital identifiers to track users in lieu of directly identifiable information, even though directly identifiable information may be collected simultaneously. Therefore, digital identifiers function as pseudonyms.

Pseudonymization is the process of substituting data with alternative labels that may either be randomly assigned or determined by an algorithm.[37] For example, instead of assigning John Doe to a row of data, an entity will use an

31. *See id.* (After creating an analysis of an individual consumer's activities, "[c]ompanies then can use this data for analytics or personalized advertising").
32. *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 282–83 (3d Cir. 2016).
33. *Id.*
34. *See id.*
35. *See id.*
36. *See infra* Part III.
37. *See* Lubarsky, *supra* note 13, at 206.

identification (ID) number, such as 344032. Thus, pseudonymization allows an entity to preserve the usefulness of the data without revealing directly identifiable information.[38]

Pseudonymization only acts as a superficial barrier to identification, as entities can re-identify a user by aggregating multiple datasets.[39] There are two instances where re-identification can occur. First, re-identification can occur when the recipient of pseudonymous data has access to additional information that can reveal a user's identity. Re-identification is less probable when the additional information is private, but there is a serious threat of re-identification when the information is publicly available. For instance, in order to connect a Facebook "User ID" with an individual, all one needs to do is enter the "User ID" after "facebook.com," and the resulting URL will take you to that individual's profile.[40]

A common example of digital pseudonyms are device IDs, such as an "Android ID."[41] An Android ID is randomly assigned, but remains constant for the lifetime of the device unless a factory reset is performed.[42] While device IDs, like Android IDs, are not as public as Facebook IDs, this information can lead to re-identification if the holder of the information has already acquired and can cross-identify multiple databases. Therefore, regardless of whether the additional information is publicly available or privately acquired, the more databases an entity has access to, the more likely a person or entity will be able to re-identify data. The preceding information will be important to keep in mind when assessing the facts of the VPPA cases discussed in Part IV.

III. LEGISLATIVE HISTORY BACKGROUND

The House of Representatives and Senate both made efforts to enact a video privacy protection act following the Robert Bork disclosure. The House's first initiative was H.R. 3523, introduced by Representative Alfred McCandless in October of 1987.[43] This proposed version of the act did not use the term PII.[44] PII was first included in H.R. 4947, introduced by

38. *See id.*

39. *See id.* at 206–07.

40. For example, founder of Facebook Mark Zuckerberg's User ID is 4. Therefore, facebook.com/4 can be used to identify Zuckerberg.

41. Emily McLaughlin, *Device ID (Device Identification)*, SEARCHCIO, http://searchcio.techtarget.com/definition/device-ID-device-identification [https://perma.cc/ 8J7M-SBNS] (last visited Feb. 20, 2019).

42. *Id.*

43. H.R. 3523, 100th Cong. (1987).

44. *Id.*

Representative Robert W. Kastenmeier in June of 1988.[45] Senator Patrick J. Leahy simultaneously introduced S. 2361 to the Senate, which was ultimately enacted as the VPPA.[46]

The purpose of the VPPA is clearly stated in Senate Report No. 100-599 ("the Senate Report") as "[t]o preserve personal privacy with respect to the rental, purchase, or delivery of video tapes or similar audio visual materials."[47] Congress was aware of, and concerned about, the broader trends in the digital economy. Specifically, that consumers were routinely subjected to ongoing data collection and data was increasingly disseminated for advertising and profiling purposes.[48]

Congress feared that data collection without proper control could significantly erode privacy interests.[49] At the introduction of S. 2361, Senator Paul Simon warned that as "the computer age revolutionized our world . . . we must protect . . . our right to privacy."[50] Senator Robert Kastenmeier expressed that the VPPA was "an effort to keep up . . . with changing technology and changing social patterns with respect to the use of materials which ought to be clearly private."[51] In addition, Senator Leahy stated that "information pools," i.e., datasets, themselves created privacy interests that "directly affect the ability of people to express their opinions . . . and to enjoy the freedom and independence that the Constitution was established to safeguard."[52]

Congress wanted to use the VPPA to address concerns about the growth of routine disclosures during the then-evolving digital age. Congressional intent is important because it illustrates that the VPPA was meant to address not only Bork-like cases concerning individualized disclosure, but also more

45. H.R. 4947, 100th Cong. (1988).

46. S. 2361, 100th Cong. (1988).

47. S. Rep. NO. 100-599 (1988) at 1.

48. *See id.* at 6 ("The Act allows consumers to maintain control over personal information divulged and generated in exchange for receiving services from video tape service providers.").

49. *See id.* ("[E]very day Americans are forced to provide to businesses and other personal information without having any control over where that information [is stored] . . . . [T]he trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance.").

50. *See id.*

51. *Video and Library Privacy Protection Act of 1988: Hearing on H.R. 4947 & S. 2361 Before the Subcomm. on Courts, Civil Liberties & the Admin. of Justice of the H. Comm. on the Judiciary & the Subcomm. on Tech. & the Law of the S. Comm. on the Judiciary*, 100th Cong. (1988) at 19.

52. S. REP. NO. 100-599 at 6.

recent cases consisting of collective database disclosures.[53] Therefore, while the sponsors of the VPPA could not have anticipated the drastic changes in video rental and sharing methods, they did consider the practice of data collection generally, and its impact on privacy.

IV. CURRENT APPROACHES TO PII

This Part will describe current approaches that courts have adopted to define PII under the VPPA. Specifically, the two main issues that courts have addressed are: (1) what constitutes PII; and (2) how identification occurs. These two issues address the two statutory components of PII: (1) an *identifier* associated with personal information; and (2) a *link* between the identifier and the person. Courts generally agree that PII expands beyond just the users' names but are split over the exact scope of that expansion. The First and Third Circuit tests have emerged as dominant competing approaches.

A. THE NARROW APPROACH: THIRD CIRCUIT IN *NICKELODEON*

The Third Circuit in *In re Nickelodeon Consumer Privacy Litigation* ("*Nickelodeon*") took a narrow approach for determining whether digital identifiers can constitute PII. In a multidistrict consolidated class action, Plaintiffs, children younger than 13, brought a VPPA claim against Defendants, Viacom and Google, for unlawfully collecting personal information about them on the Internet, including what videos they were watching on Viacom's websites.[54] Plaintiffs all visited and used "Nick.com," Defendant's website, to watch videos.[55] In the registration process, Plaintiffs were told that personal information would not be collected.[56] Plaintiffs alleged

53. *Infra* Part V; *see* S. REP. NO. 100-599 at 5–6 (Senator Leahy denounced the disclosure of Judge Bork's video-watching, stating,

> [I]n an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones . . . it would be *relatively easy at some point* to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone. I think that is wrong. I think that really is Big Brother, and I think it is something that we have to guard against.

(emphasis added).).

54. *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 267 (3d Cir. 2016), *cert. denied sub nom.* C. A. F. v. Viacom Inc., 137 S. Ct. 624 (2017).

55. *Id.* at 268.

56. *See id.* at 269.

that Defendants were unlawfully using "cookies[57] to track children's web-browsing and video-watching habits on Viacom's websites," and sending the information to a third party, Google, without permission.[58] The court focused on the following information as relevant for its PII analysis: (1) a user's IP address;[59] (2) a user's browser and operating system settings;[60] and (3) the computing device's "unique device identifier."[61] Plaintiffs alleged that Google could aggregate this data in order to determine the user by device and "track the same computer across time."[62]

The *Nickelodeon* court articulated a narrow approach for PII by ultimately concluding that PII covers only "the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching history."[63] The court relied primarily on legislative history after determining that the text of the statute is ambiguous.[64] The court concluded that Congress had a narrow purpose in passing the VPPA with the intention of only preventing disclosure of information "that would, with little or no extra effort, permit an ordinary recipient to identify a particular person's video-watching habits."[65] The court also noted that it did not think Congress passed the Act intending "for the law to cover factual circumstances far removed from those that motivated its passage."[66] The court found that since the Act was trimmed down from covering video and library material to only video, this hinted that Congress intended a narrow interpretation of PII.[67] Therefore, the court considered the legislators' initial focus on both libraries and video stores to indicate that "the Act was meant to prevent disclosures of information capable

57. *Id.* (explaining that "[a]n Internet 'cookie' is a small text file that a web server places on a user's computing device. Cookies allow a website to 'remember' information about a user's browsing activities . . . ").

58. *Id.*

59. *Id.* at 281 ("[A] number assigned to each device that is connected to the Internet that permits computer-specific online tracking.").

60. A user's browser "comprises a so-called 'browser fingerprint.' " *Id.* at 282 ("The plaintiffs claim that these [browser fingerprint] profiles are so detailed that the odds of two people having the same browser fingerprint are 1 in 286,777.").

61. *Id.*

62. *Id.*

63. *Id.*

64. *Id.* at 284.

65. *Id.*

66. *Id.*

67. *Id.* at 284–85. ("This becomes apparent by tracing the Video Privacy Protection Act's legislative history . . . [t]he then-extant Senate bill would have punished both disclosures relating to video tape service providers and disclosures relating to library borrowing records.").

of identifying an *actual person's* reading or video-watching habits."[68] Lastly, the court also found that since Congress did not amend the 1988 definition of PII during its 2013 amendment process, this illustrated that Congress preferred a narrow interpretation: "the Act serves different purposes, and protects different constituencies, than other, broader privacy laws."[69]

Two notable cases followed the *Nickelodeon* approach: *In re Hulu Privacy Litigation* and *Robinson v. Disney Online*.[70] In *Hulu*, Plaintiffs, Hulu users, brought a VPPA claim against Defendant Hulu, an online provider of on-demand video content through hulu.com.[71] Plaintiffs alleged that Hulu violated the VPPA by wrongfully disclosing their video viewing selections and PII to Facebook, a third party.[72]

Plaintiffs were all registered Hulu users.[73] Hulu assigned each new registered user a "User ID," which is a unique numerical identifier.[74] Videos on hulu.com are displayed through a video player on a webpage that Hulu calls "watch pages."[75] These watch pages included a "Like Button" feature provided by Facebook that allowed information to be transmitted to Facebook whenever the Like Button loaded on the page.[76] In fact, loading the Like Button prompted the user's browser to send Facebook the "user's numeric Facebook ID (from the c_user cookie),"and "the title of the video that the user was watching (contained in the Hulu watch-page address)."[77] Facebook could only identify the user by name if the "Hulu user had logged into

68. *Id.*

69. *See id.* at 288 ("Congress has recently revisited the Video Privacy Protection Act and, despite the passage of nearly thirty years since its enactment, left the law almost entirely unchanged.").

70. *In re* Hulu Privacy Litig., 86 F. Supp. 3d 1090 (N.D. Cal. 2015), *appeal dismissed* (Oct. 28, 2015); Robinson v. Disney Online, 152 F. Supp. 3d 176 (S.D.N.Y. 2015).

71. *In re Hulu Privacy Litig.*, 86 F. Supp. 3d at 1091–92.

72. *Id.* at 1091.

73. *Id.* at 1092 ("A Hulu user does not need to register for a Hulu account to watch videos on hulu.com using a personal computer . . . . To register for a Hulu account, the user enters a first and last name, birth date, gender, and an email address . . . . Users are not required to provide their legal first and last name during registration.").

74. *Id.*

75. *Id.*

76. *Id.* at 1093–94 ("Hulu added a Facebook 'Like' button to each hulu.com watch page. . . . Certain information was transmitted from hulu.com to Facebook via the 'Like' button . . . Hulu sent Facebook the watch page's address . . . the address for each watch page included the title of the video displayed on that watch page.").

77. *Id.* at 1094.

Facebook using certain settings in the previous four weeks."[78] Hulu did not send Facebook the Hulu User ID or the Hulu user's name.[79]

The court found that Defendant Hulu could not have transmitted PII to Facebook because there was an absence of evidence that "Hulu *actually knew* that Facebook might combine information that identified Hulu users with separate information specifying which video that user was watching" to identify the user.[80] The holding was based on the court's multiple narrow interpretations of the VPPA. First, the court found that "the connection" between a person's identity and video materials must be made before disclosure to a third party, and therefore must be "immediate" when a third party receives it, in order to constitute PII.[81] In addition, the court placed emphasis on the connection element, finding that it is a "necessary element of the VPPA."[82] Lastly, the court found that unless a Plaintiff has evidence that the Defendant knew that the third party had "the code" to identify a person and would make "the connection," it could not be held liable under the VPPA because it did not *knowingly* disclose PII.[83]

The *Hulu* court made its finding based on the conclusion that the VPPA was enacted for Bork-like cases, characterized by an "obvious" connection between "a specific user and the material he requested."[84] This led the court to conclude that the connection element distances "Internet-streaming case[s] from the situations for which the VPPA was enacted."[85] Unlike in *Nickelodeon* and *Robinson*, the *Hulu* court did not conduct an analysis of the legislative

78.

> If the Hulu user had logged into Facebook using certain settings within the previous four weeks, the Like button would cause a "c_user" cookie to be sent to Facebook; c_user contains (among other things) the logged-in user's Facebook user ID expressed in a numeric format . . . . Facebook can identify this number as a particular Facebook user . . . . Hulu did not send Facebook the Hulu User ID or the Hulu user's name when the user's browser executed the code to load the Like button.

(emphasis added). *Id.* at 1094.

79. *Id.*

80. *Id.* at 1091 (emphasis added).

81. *Id.* at 1095.

82. *Id.* at 1096.

83. *Id.*

84. *Id.*

85. *Id.*

history and based its findings purely on the court's interpretation of the text and the Bork scenario.[86]

The Southern District of New York also followed the narrow approach in *Robinson*.[87] Plaintiff James Robinson brought a VPPA claim against Defendant Disney Online for allegedly disclosing PII to Adobe, a third-party analytics company, without Plaintiff's consent.[88] Plaintiff watched Disney's video content through the Roku Channel Store, an "online digital media platform."[89] Plaintiff claimed that Disney's Roku channel was programmed to send Adobe users' PII, including "a record of every video clip viewed by the user" accompanied by a "hashed serial number" that was unique and constant for the lifetime of the user's device.[90] Plaintiff argued that this constituted PII because Adobe had the capability to use aggregated data to "personally identify . . . users and associate their video viewing selections with a personalized profile in its databases."[91]

The *Robinson* court held that information disclosed by Disney did not amount to PII because the "information [Disney] disclosed itself" could not have identified Plaintiff.[92] The court defined PII as information which must *itself* identify a particular person as having viewed specific video materials.[93] The court rejected Plaintiff's argument that "Adobe's ability to identify Robinson by linking this disclosure with other information" should be considered as evidence that there was a disclosure of PII.[94] The court stated that it "agrees with the *Yershov* court that PII, in this statutory context, includes more than just names and addresses."[95] However, beyond this agreement, the court sided with the majority approach in *Yershov* that adopted a narrow

86. *See id.* at 1095–1105.

87. Robinson v. Disney Online, 152 F. Supp. 3d 176 (S.D.N.Y. 2015).

88. *Id.* at 177–78.

89. *Id.* at 178.

90. *Id.*

91. *See id.* ("Robinson does not argue that the information disclosed by Disney—a 'record of [his viewing] activities . . . along with the hashed serial number associated with [his] Roku device' . . . constitutes PII in its own right.").

92. *See id.* at 184.

93. *Id.* at 183.

94. *See id.*

95. *Id.* at 181 (finding "it would be difficult to read the language of the statute otherwise").

definition of PII, holding that disclosed information cannot constitute PII if it requires additional information to identify the person.[96]

The *Robinson* court mainly relied on previous case law while conducting an analysis of legislative history. First, the court found that the legislative history clearly conveys that PII needs to identify a particular person in connection with his or her viewing history.[97] Second, the court found that the VPPA's definition of "particularized" proved Congress intended to create a narrow scope for PII, critiquing *Yershov*'s definition as "overly expansive."[98] The court emphasized that entities now, more than ever, have greater capabilities to identify users with "the impact of modern digital technologies."[99]

Next, the court refused to take into consideration third parties' capabilities to manipulate disclosed data, finding that this would shift the purpose of the statute by imposing too much uncertain liability on entities.[100] The court found that since "nearly any piece of information can, with enough effort on behalf of the recipient, be combined with other information so as to identify a person," a broad scope for PII would be "limitless."[101] Second, the court was concerned that considering third-party capabilities would create a knowledge requirement for entities removing "any real limitation of liability."[102] Lastly, the court was concerned that third-party context considerations would improperly create liability "even where the ability of third-party recipients to compile identifying information was unknown to them."[103] Thus, the court found that these considerations are unsupported by the statutory text.[104]

---

96. *See id.* at 180.

97. *See id.* at 179–80 ("As explained in the Senate Report issued in advance of the statute's enactment, 'personally identifiable information' is intended to be transaction-oriented. It is information that identifies a particular person as having engaged in a specific transaction with a video tape service provider.") (citing S. REP. NO. 100-599 at 12).

98. *Id.* at 18.

99. *Id.* at 181.

100.

> It would render meaningless the requirement that the information identify a specific person as having rented or watched specific videos, as all information would, with some work, be identifying, and would transmute a statute focused on disclosure of specific information to one principally concerned with what third parties might conceivably be able to do with far more limited disclosures.

Id.

101. *Id.*

102. *Id.*

103. *Id.* at 180.

104. *Id.* at 181. The court wrote:

B. THE BROAD APPROACH: FIRST CIRCUIT IN YERSHOV

In *Yershov*, Plaintiff Alexander Yershov brought a VPPA claim against Defendant Gannett Satellite Information Network, Inc. ("Gannett"), a newspaper publisher, for allegedly disclosing information about the Plaintiff to a third party, Adobe Systems Incorporated ("Adobe").[105] Plaintiff was watching videos from his phone on a "proprietary mobile software application" ("App") offered by Gannett.[106] Gannett never sought Plaintiff's consent to disclose his information associated with the App to third parties.[107] Plaintiff alleged that each time he viewed video content on the App, Gannett gave the following information to Adobe: (1) the title of the video viewed; (2) the GPS coordinates of the device at the time the view was viewed; and (3) certain identifiers associated with the user's device, such as its unique Android ID."[108] An Android ID is an unique identifier that allows third parties "to identify and track specific users across multiple electronic devices, applications, and services."[109] Adobe uses this collected information to provide Gannett with marketing analytics.[110]

The district court in *Yershov* criticized the narrow approach adopted by the Third Circuit in *Nickelodeon* for taking an "unrealistic view of the nature of personal identifiers, and how readily different databases or pieces of

> But such a principle would necessarily either read into the VPPA a requirement that providers not only know the nature of the information actually disclosed by them, but also know the informational capabilities of any third-party recipient, or, to the extent 'knowing' is limited to knowledge of disclosure, hold providers liable even where the ability of third-party recipients to compile identifying information was unknown to them. Both constructions are unsupported by the statutory text.

Id.

105. *Id.* at 484.

106. *Id.* ("The App allows users to access news and entertainment media content, including videos, on their mobile devices.").

107. *Id.*

108. *Id.* (emphasis added).

109. *Id.*

110. *Id.* For more context:

> Adobe is an unrelated third party that offers data analytics and online marketing services to its clients by collecting information about consumers and their online behavior . . . . Adobe takes this and other information culled from a variety of sources to create user profiles comprised of a given user's personal information, online behavioral data, and device identifiers.

Id.

information can be linked together."[111] Similarly, the First Circuit concluded that "the language [of the statute] reasonably conveys . . . that PII is not limited to information that explicitly names a person."[112] Therefore, the First Circuit affirmed the district court's finding that information that does not identify a specific person can still constitute PII when a third party has access to information that might thereafter enable it to identify the user.[113]

In *Yershov*, the First Circuit adopted a broad approach for determining the scope of PII: PII can embrace "information reasonably and foreseeably likely to reveal . . . videos [the plaintiff] has obtained."[114] However, an identifier can fall outside the scope of PII when "the linkage of information to identity becomes too uncertain, or too dependent on too much yet-to-be-done, or unforeseeable detective work." The First Circuit's broad approach allows courts to use "reasonable inferences" based on evidence of a particular third party's resources. Thus, the First Circuit considered evidence that Adobe, as opposed to an abstract reasonable person, had access to resources that would allow for re-identification of the transmitted data.[115] These reasonable inferences were made in the plaintiff's favor, potentially including the recipient of the data and what kind of resources they have available.[116] For instance, the First Circuit recognized that Adobe has the capability "to link the GPS address and device identifier information to a certain person by name, address, phone number, and more."[117] This led the First Circuit to agree with the district court, finding that both the plaintiff's phone GPS coordinates and Android ID constituted PII.[118]

The First Circuit focused primarily on the text of the statute.[119] First, the court concluded that the language "reasonably conveys . . . that PII is not limited to information that explicitly names a person."[120] Second, the court

111. Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 145–46 (D. Mass. 2015), *rev'd*, 820 F.3d 482 (1st Cir. 2016) (responding to the decision in *In re* Nickelodeon Consumer Privacy Litig., MDL No. 2443 (SRC), 2014 WL 3012873 (D.N.J. July 2, 2014)).

112. *Yershov*, 820 F.3d 482 at 486.

113. *Id.* (finding that information "effectively revealing the name of the video viewer" is sufficient to constitute PII under the VPPA).

114. *Id.* at 486.

115. *Id.* at 486.

116. *Id.*

117. *Id.*

118. *Id.* at 486.

119. *See id.*

120. *Id.* at 486 ("[N]evertheless, the language reasonably conveys the point that PII is not limited to information that explicitly names a person. Had Congress intended such a narrow

found that Congress's use of the word "includes" also indicated a broad interpretation because "the proffered definition [of PII] falls short of capturing the whole meaning."[121] Lastly, the court relied on legislative history, concluding that not only can "[m]any types of information other than a name [ ] easily identify a person," but context must be taken into consideration in the analysis of PII.[122]

The Central District of California followed *Yershov*'s broad approach to PII in *In re Vizio, Inc., Consumer Privacy Litigation* ("*Vizio*").[123] In *Vizio*, Plaintiffs, users of Vizio Smart TVs, brought a claim against Defendant Vizio, manufacturer of cutting edge televisions called "Smart TVs," for using software to automatically "collect and report consumer's content viewing histories" and then disseminating this information to third-parties without users' consent.[124] Vizio's Smart TVs used a software called "Smart Interactivity" to collect users' video watching practices and "detailed information about the consumers digital identity," including "consumers' IP addresses, zip codes, MAC addresses, product model numbers, hardware and software versions, chipset IDs, region and language settings."[125] Plaintiffs argued that this array of data falls within the statutory definition of PII, asserting that Vizio's disclosure constituted a "constellation of information" that provided a " 'game plan' to associate individuals with their viewing habits."[126]

The *Vizio* court held that "highly specific viewing behavior data on a massive scale with great accuracy" could lead to re-identification and thus

and simple construction, it would have had no reason to fashion the more abstract formulation contained in the statute.").

121. *See id.* ("[M]oreover, the language Congress did use to define PII begins with the word 'includes' . . . . That word normally implies that the proffered definition falls short of capturing the whole meaning.") (citing 18 U.S.C. § 2710(a)(3)) (citing *In re* Fahey, 779 F.3d 1, 5–6 (1st Cir. 2015)).

122. *Id.* ("[W]e also have the benefit of the Senate Report expressly stating that the drafters' aim was "to establish a minimum, but not exclusive, definition of personally identifiable information." (citing S. REP. NO. 100–599)); *see id.* (The *Yershov* court provides the following example to illustrate how an identifier can be linked back to a person and the importance of context when determining likelihood: "Revealing a person's social security number to the government, for example, plainly identifies the person. Similarly, when a football referee announces a violation by 'No. 12 on the offense,' everyone with a game program knows the name of the player who was flagged.").

123. *In re* Vizio, Inc., Consumer Privacy Litig., 238 F. Supp. 3d 1204 (C.D. Cal. 2017).

124. *Id.* at 1212.

125. *Id.*

126. *Id.* at 1212, 1223.

qualifies as PII.[127] The court came to this conclusion adopting the *Yershov* court's "reasonably and foreseeably likely to reveal" approach.[128] While the court did review statutory language and legislative history, it mostly relied on prior case law.[129] First, the court found that both statutory language and congressional intent illustrated that Congress intended PII to "encompass more than a person's name and physical address."[130] Next, in determining how to conduct the PII link analysis, the court turned to case law, weighing *Nickelodeon*'s narrow approach against *Yershov*'s broad approach and finding the latter more persuasive.[131] First, the court criticized the *Nickelodeon* court for not spending enough time evaluating the statutory text.[132] Second, the court found that the *Nickelodeon* court relied too heavily on "Congress's decision *not* to amend the statute substantially in 2002."[133] Lastly, the court critiqued *Nickelodeon*'s "ordinary person" approach as being too narrow, because excluding evidence regarding a person's ability to consult additional materials would raise serious doubt about whether traditional identifiers, such as social security numbers, could constitute PII.[134]

---

127. *Id.* at 1225.

128. *Id.*; *see also* Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 486 (1st Cir. 2016).

129. *See In re Vizio, Inc.*, 238 F. Supp. 3d at 1223–26.

130.

> The suffix 'able' means 'capable of,' so 'personally identifiable information' plainly extends beyond a consumer's name . . . . The statutory structure confirms that Congress intended 'personally identifiable information' to encompass more than a person's name and physical address. In the original Act, Congress included both an opt-out and opt-in disclosure process. If a consumer opted in to a disclosure, a video tape service provider could reveal any type of personally identifiable information. But if the consumer had to opt out of the disclosure, the video tape service provider could disclose only the consumer's name and address.

Id. at 1224 (citing Video Privacy Protection Act of 1988, S. 2361, 100th Cong. § 2 (1988)).

131. *Id.* at 1224–26

132. *Id.* at 1224–25.

133. *Id.* at 1225 ("*In re Nickelodeon* relied heavily on Congress's decision not to amend the statute substantially in 2002. As the Supreme Court has instructed, this kind of '[p]ost-enactment legislative history (a contradiction in terms) is not a legitimate tool of statutory interpretation.' ") (citing Bruesewitz v. Wyeth LLC, 562 U.S. 223, 242 (2011)).

134. *Id.* at 1225 ("[U]nder the Third Circuit's 'ordinary person' test it would be highly questionable whether even social security numbers would constitute personally identifiable information because, as the Third Circuit itself recognized, this information 'might not be easily matched to . . . persons without consulting another entity, such as a credit reporting agency or government bureau.' ") (citing *In re* Nickelodeon Privacy Litig., 827 F.3d 262, 283 (3d Cir. 2016), *cert. denied sub nom.* C. A. F. v. Viacom Inc., 137 S. Ct. 624 (2017)).

V. LEGISLATIVE HISTORY ANALYSIS

The courts in *Yershov* and *Nickelodeon* both found the VPPA to be ambiguous and turned to the legislative history, yet the courts reached opposite conclusions about the definition of PII.

The Supreme Court in *Twentieth Century Music Corp. v. Aiken* instructed that "[w]hen technological change has rendered its literal terms ambiguous, [a law] must be construed in light of [its] basic purpose."[135] Since courts have consistently found the plain language of the VPPA to be ambiguous with regards to PII, a large part of this Note's analysis centers on understanding the purpose of the statute as related to PII. In order to understand the purpose of the statute, this Part uses legislative history as an indicator of Congressional intent.

A. PII WAS INTENDED TO BE BROADLY INTERPRETED

Professor Huffman illustrates with multiple observations how the VPPA's legislative history depicts that Congress did not want to limit what kind of information would qualify for protection under the statute.[136] First, the initial bill proposed by the House for adoption, H.R. 3523, merely prohibited disclosure of "the identity of the individual who rented or purchased" video materials.[137] The term PII was not implemented in this version of the Act.[138] However, in a succeeding proposal, H.R. 4947, the term PII was included without a definition.[139] S. 2361 broadened the scope of disclosed information by using the term PII along with the following definition, substantially similar to the one adopted in the VPPA: "[T]he term 'personally identifiable information' includes information which identifies a person as having requested or obtained specific materials or services from a video tape service provider or library."[140]

This definition of PII illustrates that Congress was unsatisfied with statutory language that would only protect direct unauthorized disclosure of a person's identity without considering other avenues in which a person's identity could be determined. It also shows Congress's recognition of a logical difference between an identifier and a person's identity, laying the foundation

135. Twentieth Century Music Corp. v. Aiken, 422 U.S. 151, 156 (1975) (interpreting the Copyright Act).

136. *See* Huffman, *supra* note 6.

137. H.R. 3523, 100th Cong. (1987).

138. *Id.*

139. H.R. 4947, 100th Cong. (1988).

140. S. 2361 § 2(a)(2), 100th Cong. (1988) (enacted).

for a potential link between the two. By using the word "includes," the statute conveys that PII should not be limited to information that explicitly names a person.[141] In fact, the Senate Report of the VPPA expressly states that "[u]nlike the other definitions . . . paragraph (a)(3) uses the word 'includes' to establish a minimum, but not exclusive, definition of personally identifiable information."[142] By establishing a minimum, Congress left the door open for not only defining what could qualify as identifiable information, but also how that information could identify a person. Failure to draw this key distinction creates confusion about the interpretation of the scope of PII.

B. HOW TO "IDENTIFY" UNDER THE VPPA IS UNCLEAR AND CREATES CONFUSION IN THE COURTS

While Congress intended the definition of PII to be broadly interpreted, it provided no guidance on what it means to "identify" an individual. Therefore, courts constructed their own rules for deciding what qualifies as a sufficient link between an identifier and a person's identity, which has led to a circuit split as illustrated in Part IV.[143]

The Senate Report states that "[t]he bill prohibits video stores from disclosing 'personally identifiable information'—information that links the customer or patron to particular materials or services."[144] This confirms again that Congress was less concerned with the form that the personal information was disclosed in—for example, a name versus a number ID—than with whether the information *actually linked* back to the person in a way that would reveal the person's identity. The problem is that Congress did not instruct how to determine whether a link between a digital identifier and a person's identity is certain enough to qualify as PII.[145] Meanwhile, technology has drastically changed the way individuals are identified and what identifiers are used.[146] Thus, the confusion over PII lies in the ambiguity of when a link between the specific digital identifiers disclosed and the person's identity is sufficiently strong enough to qualify the disclosed information as PII.

---

141. *See infra* note 142.

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

143. *See, e.g.*, Robinson v. Disney Online, 152 F. Supp. 3d 176, 180 (S.D.N.Y. 2015) (noting "Less clear is . . . how, precisely, this information[,] [discussed in the definition of PII,] must identify a person").

144. *Id.* at 7.

145. Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 486 (1st Cir. 2016) (finding "[t]he definition of that term ('identifies a person as having [obtained a video]') adds little clarity beyond training our focus on the question whether the information identifies the person who obtained the video" (quoting 18 U.S.C. § 2710(a)(3) (2012)).

146. *See supra* Part III.

VI. REVISITING RECENT CASES IN LIGHT OF LEGISLATIVE HISTORY AND CURRENT TECHNOLOGICAL INSIGHT

How *should* the legislative history of the VPPA be used to interpret the definition of PII? Part VI compares the VPPA's legislative history with current approaches, in order to illustrate what courts are getting right or wrong and why. As discussed above, courts generally agree that PII identifiers can be broadly interpreted to include more than just a person's name, but the courts have split over what method of identification can be protected by the VPPA—what courts have called the "connection" or "link" required between the disclosure of information and the person.[147]

The big picture divide among courts hinges on whether or not a court believes that an identifier must *itself* directly identify a person in order to constitute PII. Courts that follow a broad approach have held that data does not have to specify an individual if the third party can be found to have additional information that would "foreseeably and reasonably" enable it to identify the user.[148] On the other hand, courts following a narrow approach have held that data must immediately identify a person in order to constitute PII.[149] This Section will be organized based on principles that have divided the courts, leading to their respective approaches.

A. HOW A "CONNECTION" MUST OCCUR BETWEEN IDENTIFIER AND PERSON

Courts are divided on whether the identification of a person can occur after disclosure to a third party or whether it must occur before. Courts following a narrow approach hold that information can only qualify as PII if it can identify a person before the disclosure of data to the third party, making the PII disclosure immediate.[150] On the other hand, courts following a broad approach hold that information can qualify as PII, even if identification occurs after disclosure, if identification of a person is reasonable and foreseeable based on the third party's capabilities.

This Section argues that, based on legislative intent, information should qualify as PII after disclosure. The legislative history heavily weighs in favor of

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

148. *See In re* Vizio, Inc., Consumer Privacy Litig., 238 F. Supp. 3d 1204, 1225 (C.D. Cal. 2017); *Yershov*, 820 F.3d at 486.

149. *See, e.g.*, *In re Hulu*, 86 F. Supp. 3d at 1090; Robinson v. Disney Online, 152 F. Supp. 3d 176 (S.D.N.Y. 2015).

150. *See, e.g.*, *In re Hulu*, 86 F. Supp. 3d.

courts taking a broad perspective on identification of PII. First, by introducing the VPPA with a discussion of how the advancement in data collection and related technology could seriously threaten the privacy of individuals in their daily lives, Congress illustrated that it wanted the VPPA to address incidents of collective disclosure, meaning instances where user data is aggregated and disclosed with other users' data.[151] Second, in light of the Supreme Court's instruction, courts should interpret PII in light of the "basic purpose" of the VPPA, which is to prevent the unauthorized disclosure of a person's identity in connection with her video-watching history.[152] Third, since Congress expressed that PII should not just include direct identifiers, such as a person's name, this illustrates an intent for courts to consider other avenues of identification.[153] Therefore, the basic purpose of the statute would be satisfied if a plaintiff plausibly pleaded that identification can occur in the hands of the third party, regardless of whether the identification occurs before or after disclosure.

In contrast, the courts that took the narrow approach had multiple flaws in their reasoning. First, they wrongly assumed that VPPA cases need to resemble the Bork case that incited the VPPA. The *Hulu* and *Nickelodeon* courts both argued that PII disclosure must be immediate because that is what occurred in the Bork case, and therefore Congress only intended for these types of cases to be protected.[154] However, as previously discussed, the legislative history illustrates that Congress wanted the VPPA to address instances of collective, not just individualized, disclosure, with an eye towards the expanding technological capabilities of information pooling.[155]

Second, narrow approach courts, such as *Robinson*, argued that if the court evaluated the capabilities of third parties, this would impose too much uncertain liability on entities, because they would need to know the "informational capabilities" of third-party recipients.[156] However, while the

151. *See supra* Part V.

152. *See supra* note 135.

153. *See* Part V.

154. *See In re* Nickelodeon Privacy Litig., 827 F.3d 262, 294 (3d Cir. 2016), *cert. denied sub nom.* C. A. F. v. Viacom Inc., 137 S. Ct. 624 (2017) ("The court does not think Congress passed the Act with the intention 'for the law to cover factual circumstances far removed from those that motivated its passage.' "); *see In re Hulu*, 86 F. Supp. 3d at 1096, *appeal dismissed* (Oct. 28, 2015) ("The nature of the third element—the connection—distances this Internet-streaming case from the situations for which the VPPA was enacted. The paradigmatic case, the case that prompted the VPPA, involved a video store's giving a Washington Post [sic] reporter a list of the videos that Circuit Judge Robert Bork had rented.").

155. *See* Part V; note 49.

156. *See* Robinson v. Disney Online, 152 F. Supp. 3d 176, 181 (S.D.N.Y. 2015).

Robinson court declined to "ascribe . . . an expansive intent to Congress in enacting the VPPA,"[157] it conceded that modern-day technology has likely made third-party identification more feasible. The *Robinson* court is correct in recognizing that expanding the scope of PII creates more uncertainty for defendants, but the court's argument for defining a narrow approach does not align with Congressional intent. To the contrary, since Congress expressed fears that improvements in digital technology could threaten user privacy, courts would best follow Congressional intent by interpreting the VPPA broadly.[158] Therefore, instead of viewing the complexity of technology as too unforeseeable for Congress to have anticipated, this Note agrees with the *Vizio* court's finding that the PII analysis should be a factual inquiry.[159]

As discussed in Part II, the more access to different databases a company has, the higher the likelihood that a company will be able to re-identify a user. While re-identification of indirect identifiers is not guaranteed, it is possible, and particularly likely when the information is sent to third party analytics companies, such as many of the recent VPPA litigation defendants.[160] Therefore, the liability is not as unforeseeable as the *Robinson* court claims; if a company is sending user data to an analytics company that has more than ordinary access to multiple databases, the company should understand that re-identification is possible. Likewise, the company should be held liable for exposing its users to this risk. Courts should focus less on decreasing the risk of liability for defendants and more on whether there is a likelihood of re-identification for indirect digital identifiers. This analysis can only occur on a case-by-case basis. The following Section discusses some factors courts should consider when evaluating PII.

1. What Factors Should Courts Consider in Determining the Disclosure of PII

In *Nickelodeon*, the leading narrow approach case, the court set an "ordinary person" test, finding that only information that would readily permit an

157. *See id.*

158. *Video and Library Privacy Protection Act of 1988: Hearing on H.R. 4947 & S. 2361 Before the Subcomm. on Courts, Civil Liberties & the Admin. of Justice of the H. Comm. on the Judiciary & the Subcomm. on Tech. & the Law of the S. Comm. on the Judiciary*, 100th Cong. (1988) at 131 ("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.").

159. *In re* Vizio, Inc., Consumer Privacy Litig., 238 F. Supp. 3d 1204, 1225–26 (C.D. Cal. 2017) ("The Court stresses the posture of this case: Ultimately, Plaintiffs will have to demonstrate that Vizio's disclosures are 'reasonably and foreseeably likely to reveal' what video content Plaintiffs have watched. But this is a factual inquiry ill-suited for resolution on a motion to dismiss.").

160. *See supra* Part II.

ordinary person to identify a specific individual qualifies as PII.[161] On the other hand, the *Yershov* court, which took the broad approach, found that courts should take into consideration "reasonable interferences" based on third party capabilities in determining if information is "reasonably and foreseeably likely to reveal . . . videos [the plaintiff] has obtained."[162]

The narrow approach is too restrictive to capture the purposes intended by Congress. Since Congress wanted a broad interpretation of identifiers, supplemented by the fact the Congress never explicitly limited how PII should be identified, courts would be overstepping their power by setting an ordinary person standard.[163] If Congress wanted PII to only constitute information identifiable by an ordinary person, it could have easily established a reasonable person standard like it has in other statutes. In addition, this notion directly conflicts with Congress wanting the VPPA to address record-keeping technology and surveillance, which is not generally considered knowledge acquired by an ordinary person. In fact, the *Nickelodeon* court cites Representative Robert Kastenmeier, stating: "American citizens should not have to worry that a government agent, or a reporter, or anyone else, will be able to find out what they are reading . . . . These principles apply as much to customers of video stores as to patrons of libraries."[164] This statement inherently expresses that users' privacy ought to be protected not just from the capabilities of ordinary people, but also from more resourceful entities.

The *Nickelodeon* court argues that since Congress did not amend the definition of PII in 2013, this indicates that the Act "serves different purposes, and protects different constituencies, than other, broader privacy laws."[165] However, as found in *Vizio*, this analysis was improper because post-enactment legislative history is not a legitimate tool of statutory interpretation.[166] Additionally, the *Vizio* court provides a strong illustration of how limiting the ordinary person standard can be, arguing that this standard

161. *See In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 290 (3d Cir. 2016), *cert. denied sub nom.* C. A. F. v. Viacom Inc., 137 S. Ct. 624 (2017).

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

163. *See supra* Part III.

164. *See In re* Nickelodeon, 827 F.3d at 285, cert. denied sub nom. C. A. F. v. Viacom Inc., 137 S. Ct. 624 (2017) (citing *Video and Library Privacy Protection Act of 1988: Hearing on H.R. 4947 & S. 2361 Before the Subcomm. on Courts, Civil Liberties & the Admin. of Justice of the H. Comm. on the Judiciary & the Subcomm. on Tech. & the Law of the S. Comm. on the Judiciary*, 100th Cong. 21–22 (1988)).

165. *Id.* at 288.

166. *See supra* note 133.

would exclude social security numbers (SSN) from qualifying as PII because an ordinary person does not have access to a database of SSNs.[167]

Courts such as *Nickelodeon* fail to grasp PII as Congress intended because they analyze PII in the abstract instead of looking at the specific facts of the case to determine whether the recipient of the information would have the capability to use the data in question to reveal the identity tied to the digital identifier. Identifying information means any data that uniquely distinguishes a person out of a group. Therefore, this Note finds that the "reasonably and foreseeably" approach established by the *Yershov* court mostly closely aligns with the purpose of the VPPA because it takes into consideration context surrounding the disclosure of information, rather than ignoring evidence simply because it falls outside the judicially created narrow standard.

For instance, in *Hulu*, the court set the standard that PII must be identifiable before disclosure, and therefore the disclosure of user's viewing history along with Facebook IDs could not constitute PII under the statute. The courts found no PII even though the Facebook IDs were allegedly going to Facebook, which, as the source of the IDs, could easily identify users with its own databases. In addition, as this Note discussed in Part III, Facebook IDs are publicly accessible information, so even an ordinary user could theoretically re-identify the data.[168] This illustrates how taking into consideration context does not always mean entering a "limitless" scope of possibilities.[169]

VII. CONCLUSION

In creating the VPPA, Congress intended to prevent the unauthorized disclosure of a person's video-watching history.[170] As discussed in Part V, Congress wanted a broad interpretation of what could qualify as an identifier of personal information, because it recognized that a basic identifier, like name or telephone number, was not the only way that a person's identity could be revealed.[171] Thus, whether digital identifiers qualify as PII under the VPPA

167. *In re* Vizio, Inc., Consumer Privacy Litig., 238 F. Supp. 3d 1225 (C.D. Cal. 2017).

168. *See supra* note 40.

169. Robinson v. Disney Online, 152 F. Supp. 3d 176, 181 (S.D.N.Y. 2015) (citing *In re* Nickelodeon Consumer Privacy Litig., MDL No. 2443 (SRC), 2014 WL 3012873, at *11 (D.N.J. July 2, 2014)) ("Certainly, this type of information might one day serve as the basis of personal identification after some effort on the part of the recipient, but the same could be said for nearly any type of personal information.").

170. *See supra* Part IV.

171. *Id.*

depends on how closely linked the digital identifiers are to the individual's identity, which requires considering the re-identification capabilities of the party who receives the digital identifiers.

As discussed above, the confusion in the PII analysis is occurring because courts are unclear of what identifies a person under the definition of PII. Legislative history illustrates that Congress enacted the VPPA partially in an effort to address the technological advances occurring in information pooling and databased collections.[172] Therefore, courts should not just brush off digital identifiers as too unclear to qualify as PII, especially since these cases consist of fact patterns similar to the fears expressed by Congress during the passing of the Act.[173]

Under the Supreme Court's instruction, courts should use the "basic purpose" of the VPPA in interpreting PII.[174] Therefore, since the purpose of the Act is to "preserve personal privacy" with respect to video materials and Congress intended a broad interpretation of PII, courts ought to take into consideration specific context in determining whether given the facts a person could be identified in connection to his or her video material.[175] The opposite approach of first trying to define PII in the abstract and then determining whether certain identifiers could fall into that scope, as some courts currently do, fails to address the heart of PII, which is this: can the person *actually* be identified? The ordinary person standard, by explicitly excluding a realm of factors from being considered, is in direct contradiction with the "not exclusive" definition of PII that Congress wanted.[176]

To determine the identifiability of a particular digital identifier, courts may want to consider two factors: (1) the unauthorized recipient and its alleged resources; and (2) whether any additional information required to identify the user is publicly available, or private, but within the unauthorized recipient's access.

During the introduction of the VPPA, Senator Robert W. Kastenmeier said that "[t]he 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."[177] Almost thirty years later, this continues to be true, creating a

172. *See supra* Part III.

173. *See supra* Part IV.

174. *See supra* note 135.

175. *See* S. REP. NO. 100-599 (1988) at 1.

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

177. *Video and Library Privacy Protection Act of 1988: Hearing on H.R. 4947 & S. 2361 Before the Subcomm. on Courts, Civil Liberties & the Admin. of Justice of the H. Comm. on the Judiciary & the Subcomm. on Tech. & the Law of the S. Comm. on the Judiciary*, 100th Cong. 131 (1988).

balancing act between social utility and privacy concerns. With the VPPA, Congress intended to create a statute that would protect privacy interests regardless of technological advancements. Thus, in order to honor the purposes of the Act, courts should conduct case-by-case analyses that consider context and reasonable inferences. My name is Yarden Kakon, but you can call me User 101.