Chicago-Kent Law Review

Volume 91
Issue 2 *Causation, Liability and Apportionment: Comparative Interdisciplinary Perspectives*

Article 15

5-16-2016

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

Gregory M. Huffman
IIT Chicago-Kent College of Law

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

GREGORY M. HUFFMAN*

INTRODUCTION

> Books and films are the intellectual vitamins that fuel the growth of individual thought. The whole process of intellectual growth is one of privacy—of quiet, and reflection. This intimate process should be protected from the disruptive intrusion of a roving eye.[1]
>
> — Alfred "Al" A. McCandless, former Congressman

> We all want to live in a society that values privacy. And we rightfully want both the Government and business to live in a society that respects this basic right. But privacy is not a generalized right. And it is up to the legislature to define and give meaning to privacy.[2]
>
> — Chuck Grassley, Senator

The Video Privacy Protection Act ("VPPA") prohibits video tape service providers from disclosing their consumers' video rental or sale records.[3] Specifically, the VPPA prohibits a video tape service provider from knowingly disclosing personally identifiable information ("PII") concerning any of their consumers to third parties.[4] Although the VPPA was enacted in the era of video cassette tapes, Congress was well aware of the need to continue to protect consumer privacy as technologies evolve.[5] The

* J.D., December 2016, Chicago-Kent College of Law, Illinois Institute of Technology.

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

2. 100 CONG. REC. S16, 314 (daily ed. Oct. 14, 1988) (statement of Sen. Grassley).

3. 18 U.S.C.A. § 2710(b)(1) (West 2015).

4. *Id.* Any person aggrieved by such a disclosure may bring a civil action in federal court to recover actual damages (in an amount not less than $2,500 in liquidated damages), punitive damages, reasonable attorneys' fees, and litigation costs, as well as any other appropriate preliminary or equitable relief. *Id.* § 2710(c)(1)–(2). Exceptions are made for disclosures: made to the consumer; with the consumer's written consent; pursuant to a court order or warrant; or incident to the ordinary course of business of the video tape service provider. *Id.* § 2710(b)(2).

5. Counsel for the American Civil Liberties Union testified during a joint congressional hearing that: "[t]hese precious rights have grown increasingly vulnerable with the growth of advanced infor-

VPPA broadly defines the term "video tape service provider" 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*."[6] As such, the statute is applicable to not only video cassette tapes but also other media forms. Further, the statute defines a "consumer" as "any renter, purchaser, or subscriber of goods or services from a video tape service provider,"[7] and recites 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."[8]

Interestingly, there was minimal litigation under the VPPA during the first two decades of its existence.[9] However, the arrival of streaming video via web browsers and mobile applications has raised new questions of statutory interpretation.[10] Because the VPPA was originally enacted to protect the brick-and-mortar video store renter, one of these new questions was whether the VPPA even applies to disclosures by online video content providers.[11]

In 2012, the United States District Court for the Northern District of California was the first court to consider this question, and ruled that the VPPA does in fact apply to online video content providers.[12] In *In re Hulu*, the court declined to accept the argument that Hulu[13] is not a "video tape service provider."[14] At the same time, the court found that even a user who visited Hulu's website to watch video content, but was not a *paid* subscriber, should be considered a "consumer" under the VPPA.[15] Two years later,

mation technology. The new technologies not only foster more intrusive data collection, but make possible increased demands for personal, sensitive information." S. REP. NO. 100-599, at 7.

6. 18 U.S.C.A. § 2710(a)(4) (emphasis added).

7. *Id.* § 2710(a)(1).

8. *Id.* § 2710(a)(3).

9. *See* Evan Wooten & Zachariah DeMeola, *A New Chapter in Video Privacy Protection Act's History*, LAW360 (June 23, 2014, 10:40 AM), http://www.law360.com/articles/550346/a-new-chapter-in-video-privacy-protection-act-s-history.

10. *See id.*

11. *See id.*

12. *See In re* Hulu Privacy Litig., No. C 11-03764 LB, 2012 WL 3282960 (N.D. Cal. Aug. 10, 2012).

13. According to Hulu's website, "Hulu is an online video service that offers a selection of hit TV shows, clips, movies and more." *Overview*, HULU, http://www.hulu.com/about (last visited Mar. 1, 2015).

14. *In re Hulu*, 2012 WL 3282960, at *6 (reasoning that Hulu should be considered a video tape service provider for pleading purposes "given Congress's concern with protecting consumer privacy in an evolving technological world").

15. *Id.* at *8 ("If Congress wanted to limit the word 'subscriber' to 'paid subscriber,' it would have done so.").

the court went on to address a particular disclosure involving cookies[16] sent from a Hulu user's browser to Facebook.[17] The cookies were automatically transmitted to Facebook when loading[18] a Facebook Like button on the user's watch page, and included: (1) a Facebook User ID, which identified the user on Facebook; and, (2) the name of the video the user was watching.[19] The court determined that the disclosure of a Facebook User ID could be considered PII, depending on several unresolved issues of material fact, and consequently denied Hulu's motion for summary judgment as to the disclosure of the Facebook User IDs.[20]

The decisions in the *In re Hulu* litigation caught the attention of litigators across the country, prompting many new VPPA class action lawsuits.[21] For example, lawsuits were filed in early 2014 against ESPN,[22] CNN,[23] Dow Jones,[24] and Walt Disney Co.,[25] among others, alleging violations of the VPPA. The alleged violations in these new lawsuits do not simply involve disclosures of users' names and titles of videos watched by the users.[26] Instead, the online video content providers have allegedly disclosed the unique device identifiers[27] of their users' devices (e.g., a MAC address or other unique serial number assigned to a device) and the titles of videos watched on the devices to third-party database marketing companies.[28]

16. In the computer context, a cookie is "a file that may be added to your computer when you visit a Web site and that contains information about you (such as an identification code or a record of the Web pages you have visited)." *Cookie*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/cookie (last visited Mar. 1, 2015).

17. *See In re* Hulu Privacy Litig., No. C 11-03764 LB, 2014 WL 1724344 (N.D. Cal. Apr. 28, 2014).

18. "The analysis would be different if the Facebook cookies were sent when a user pressed the Like button. Information transmitted as a necessary part of a user's decision to share his views about his videos with friends on Facebook would not support a VPPA violation." *Id.* at *13.

19. *Id.*

20. *Id.* at *14–17 (denying motion for summary judgment).

21. *See* Wooten & DeMeola, *supra* note 9.

22. Complaint, Eichenberger v. ESPN, Inc., No. 14-cv-463 (W.D. Wash. Mar. 28, 2014).

23. Class Action Complaint, Perry v. Cable News Network, Inc., No. 14-cv-1194 (N.D. Ill. Feb. 18, 2014) [hereinafter CNN Complaint].

24. Complaint, Locklear v. Dow Jones & Co., No. 14-cv-744 (N.D. Ga. Mar. 13, 2014).

25. Complaint, Robinson v. Walt Disney Co., No. 14-cv-4146 (S.D.N.Y. June 9, 2014) [hereinafter Walt Disney Complaint].

26. *See, e.g.*, *id.*

27. A unique device identifier, sometimes referred to simply as a unique identifier, is a type of identifier (e.g., a number or code) assigned to a device that is guaranteed to be unique such that the identifier can be used to distinguish the device among all other instances of the device. *See, e.g.*, *Privacy & Terms – Key Terms*, GOOGLE, http://www.google.com/policies/privacy/key-terms/#toc-terms-unique-device-id (last visited Mar. 1, 2015); *Device Identifiers*, APPLICATION PRIVACY, http://www.applicationprivacy.org/learn-resources/unique-device-identifier-udid-2/ (last visited Mar. 1, 2015).

28. *See, e.g.*, Walt Disney Complaint, *supra* note 25.

These database marketing companies then collect and aggregate data from various other sources to create digital dossiers, or consumer profiles, for millions of individuals, and sell the digital dossiers to advertisers, retailers, and government agencies for a profit.[29]

A key issue going forward will therefore be whether the scope of PII under the VPPA is broad enough to cover a disclosure of a unique device identifier of a user's device, as opposed to a direct indication of a user's name, and the title of one or more videos watched on the device. With this issue in mind, this Note explores the scope of PII under the VPPA, with a particular emphasis on disclosures of unique device identifiers. Part I outlines the relevant technical aspects of unique device identifiers and explains their role in database marketing. Part II reviews the background and history of the VPPA and discusses recent case law. Finally, Part III argues that unique device identifiers should be protected as PII when disclosed in conjunction with one or more video titles.

I. UNIQUE DEVICE IDENTIFIERS PLAY AN INCREASINGLY IMPORTANT ROLE IN THE FIELD OF DATABASE MARKETING

To help appreciate the issue outlined above regarding disclosures of unique device identifiers, it is worthwhile to illustrate a few examples of unique device identifiers and provide a brief overview of the use of unique device identifiers in the field of database marketing.

A. Definition and Examples of Unique Device Identifiers

As discussed generally in the introduction, a unique device identifier is a type of identifier (e.g., a number or code) assigned to a device that is guaranteed to be unique such that the identifier can be used to distinguish the device among all other instances of the device.[30] For example, in the context of computing devices, a manufacturer may assign a unique number to each manufactured computing device.

One well-known example of such a unique device identifier is a media access control ("MAC") address.[31] MAC addresses are numeric codes generated according to standards set by the Institute of Electrical and Electronics Engineers ("IEEE") and assigned to network interfaces for use as

29. *See* Alice E. Marwick, *How Your Data Are Being Deeply Mined*, N.Y. REV. BOOKS (Jan. 9, 2014), http://www.nybooks.com/articles/archives/2014/jan/09/how-your-data-are-being-deeply-mined.

30. *See Privacy & Terms – Key Terms*, *supra* note 27.

31. *Standard Group MAC Addresses: A Tutorial Guide*, IEEE STANDARDS ASS'N, http://standards.ieee.org/develop/regauth/tut/macgrp.pdf (last visited Mar. 1, 2015).

network addresses for wired and wireless network technologies.[32] Other examples include Apple's UDID (a 40-character combination of letters and numbers assigned to devices such as iPads and iPhones) and Google's Android ID (a unique alphanumeric identifier assigned to mobile devices operating an Android operating system).[33]

B. The Role of Unique Device Identifiers in Database Marketing

In the advertising industry, many marketers prefer to use direct marketing methods, whereby marketing materials are provided directly to potential customers, rather than running general advertisements over the Internet, television, or radio.[34] One reason for favoring direct marketing over general (or non-direct) marketing is that direct marketing can be more cost-effective than non-direct marketing.[35] For instance, according to a 2010 study, "each dollar spent on direct marketing yields, on average, a return on investment of $11.73, versus a return on investment of $5.23 from non-direct marketing expenditures."[36]

One of the potential challenges for any direct marketing campaign is identifying a list of potential customers to target, since marketers do not want to waste their money marketing to customers that would not be interested in the product being marketed.[37] Database marketing, a form of direct marketing, offers an appealing solution to this problem.

Database marketing uses databases storing information about customers or potential customers to generate targeted lists of customers.[38] In practice, these databases often include customer data that is gleaned from records of past transactions, or information that customers provide when creating an online account profile, signing up for a company's loyalty card, filling out a credit application, filling out a product warranty card, entering a sweepstakes, or subscribing to a newsletter or magazine, among other

32. *Id.*

33. *See, e.g.*, Jennifer Valentino-DeVries, *Unique Phone ID Numbers Explained*, WALL ST. J.: DIGITS (Dec. 19, 2010, 9:40 PM), http://blogs.wsj.com/digits/2010/12/19/unique-phone-id-numbers-explained.

34. *See, e.g.*, *Direct Marketing*, INVESTOPEDIA, http://www.investopedia.com/terms/d/direct-marketing.asp (last visited Mar. 1, 2015).

35. *See, e.g.*, Dana Larson, *Is Direct Marketing Still an Effective Tactic?*, BLUEWATER (Oct. 1, 2010), http://www.bluewaterbrand.com/2010/10/is-direct-marketing-still-an-effective-tactic.

36. *Id.*

37. *See, e.g.*, *Database Marketing: Explore the Strategy of Database Marketing*, MARKETING-SCHOOLS.ORG, http://www.marketing-schools.org/types-of-marketing/database-marketing.html (last visited Mar. 1, 2015).

38. *See id.*

possibilities.[39] Database marketing typically involves using statistical techniques to mine this data and develop models of customer behavior, which can then be used to predict future behavior and identify a group of customers that are more likely to be receptive to a particular new product or service.[40]

While a company can easily collect data regarding its existing customers from its customers' transactions with the company, the company may wish to obtain data regarding other potential customers, such as their names, home addresses, or email addresses. In some instances, a company may purchase additional data from another business.[41] Alternatively, the company may purchase additional data from a third-party private company that specializes in collecting, aggregating, and brokering personal data.[42]

Since little is known about the inner-workings of many of these private companies, there is growing concern over their data-collection methods and the extent of personal data stored in their databases:

> Using techniques ranging from supermarket loyalty cards to targeted advertising on Facebook, private companies systematically collect very personal information, from who you are, to what you do, to what you buy. Data about your online and offline behavior are combined, analyzed, and sold to marketers, corporations, governments, and even criminals. *The scope of this collection is similar to, if not larger than, that of the NSA, yet it is almost entirely unregulated . . . .*[43]

To appreciate the amount of data being aggregated, consider that Acxiom, one of the largest companies in the database marketing industry, has "23,000 computer servers that process more than 50 trillion data transactions per year" and "claims to have records on hundreds of millions of Americans, including 1.1 billion browser cookies . . . and an average of 1,500 pieces of data per consumer."[44] These records are often referred to as "digital dossiers," which Acxiom analyzes to determine whether a particular customer "fit[s] into a number of predefined categories such as 'McMansions and Minivans' or 'adult with wealthy parent.'"[45]

The collection of unique device identifiers plays an important role for third-party companies like Acxiom, who rely on unique device identifiers

39. *See id.*

40. *See id.*

41. For instance, Barnes and Noble bought customer records from Borders when Borders went out of business. *Id.*

42. *See* Marwick, *supra* note 29.

43. *Id.* (emphasis added).

44. *Id.*

45. *Id.*

to create their digital dossiers.[46] These companies allegedly use unique device identifiers to establish correlations between particular individuals and their mobile devices.[47] Once a correlation between a particular individual and his/her mobile device is established, the individual's actions on the mobile device can be combined with data regarding the individual's offline actions (e.g., transactions at brick-and-mortar retail stores, home ownership, family income, marital status, zip code, favorite television shows, etc.).[48] Further, if an individual uses multiple devices, the unique device identifiers of each of her devices can be used to link the individual's activities across each of her devices.[49] Furthermore, the unique device identifier of an individual's mobile device can also be used to help track which businesses the individual visits.[50]

II. THE BACKGROUND, LEGISLATIVE HISTORY, AND RECENT CASE LAW OF THE VPPA

In 1987, while the Senate was holding hearings on the nomination of then-Judge Robert Bork to the Supreme Court, a newspaper in Washington, D.C. obtained Judge Bork's rental records from a local video store, and published an article describing Judge Bork's viewing history.[51] At the time, members of the Senate Judiciary Committee were outraged.[52] As Senator Patrick Leahy explained:

> It is nobody's business what . . . Robert Bork . . . watch[es] on television or read[s] or think[s] about when [he is] home. I am concerned because in an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, 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.[53]

46. *See, e.g.*, CNN Complaint, *supra* note 23, at 15–21.

47. *Id.*

48. *Id.*; *see also* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1850–51 (2011).

49. *See* CNN Complaint, *supra* note 23, at 15–21.

50. *See, e.g.*, Kate Crawford, *When Big Data Marketing Becomes Stalking: Data Brokers Cannot Be Trusted to Regulate Themselves*, SCI. AM. (Mar. 18, 2014), http://www.scientificamerican.com/article/when-big-data-marketing-becomes-stalking1.

51. S. REP. NO. 100-599, at 5 (1988).

52. *Id.*

53. *Id.* at 5–6.

Just over one year later, Congress passed the VPPA.[54] The following is a review of the background and legislative history surrounding the VPPA, as well as recent case law interpreting the term PII.

A. The Historical Background Leading to the Enactment of the VPPA

In 1987, Representative Al McCandless introduced House Bill 3523 "to preserve personal privacy with respect to the rental or purchase of video tapes by individuals."[55] House Bill 3523 was unsuccessful, but several Senators introduced a related bill, Senate Bill 2361 during the following spring.[56] At the same time, Representatives Robert Kastenmeier and McCandless introduced another video privacy protection bill, House Bill 4947, in the House of Representatives.[57] Both Senate Bill 2361 and House Bill 4947 initially sought protection with respect to not only video rental records, but also records concerning the use of library materials and services.[58]

The concurrent bills in the House and Senate were an effort to put an end to the increase in what Representative Kastenmeier referred to as "troublesome invasions of privacy—by both private individuals and the Government."[59] While speaking about this bill in front of the House, Representative Kastenmeier not only mentioned the Judge Bork incident described above, but also cited another controversial invasion of privacy: the FBI's Library Awareness Program.[60] Apparently, the FBI had been attempting to coerce librarians into disclosing circulation records and reporting any patrons with suspicious library activity.[61]

In addition to addressing the privacy issue, these federal bills were an effort to create a "uniform national standard" with respect to the disclosure of video store and library records.[62] Prior to the introduction of House Bill 4947 and Senate Bill 2361, several states had already enacted laws prohibiting the disclosure of library records and/or video store records.[63] After a

54. *See* Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (1988).
55. H.R. 3523, 100th Cong. (1987).
56. S. 2361, 100th Cong. (1988) (enacted).
57. H.R. 4947, 100th Cong. (1988).
58. *See id.* § 2(a)(2); S. 2361 § 2(a)(2).
59. 134 CONG. REC. E2227 (daily ed. June 29, 1988).
60. *Id.*
61. *Id.*
62. *Id.*
63. *Id.*

joint hearing on both House Bill 4947 and Senate Bill 2361,[64] Congress elected to move forward with Senate Bill 2361, which was eventually enacted as the VPPA.[65] All of the provisions related to library records were removed from the bill, however, due to disagreement regarding the application of the bill to law enforcement efforts.[66]

The VPPA followed in the footsteps of many other federal privacy protection statutes that protect records containing information about individuals, such as the Fair Credit Reporting Act (records maintained by credit reporting bureaus),[67] the Family Educational Rights and Privacy Act of 1974 (educational records maintained by schools and colleges),[68] the Privacy Act of 1974 (records stored by federal agencies),[69] the Tax Reform Act of 1976 (individual tax returns),[70] the Right to Financial Privacy Act of 1978 (records maintained by banks),[71] the Privacy Protection Act of 1980 (records maintained by press offices),[72] the Cable Communications Policy Act of 1984 (records maintained by cable providers),[73] and the Electronic Communications Privacy Act of 1986 (records of electronic communications by cellular phone, email, etc.).[74]

It is interesting to compare the VPPA's approach to defining PII with those of other federal privacy protection statutes. As mentioned above, the VPPA prohibits a video tape service provider from knowingly disclosing PII concerning any of its consumers.[75] The VPPA also clarifies that "the term 'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or

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

65. S. REP. NO. 100-599, at 1 (1988).

66. *Id.* at 8.

67. Fair Credit Reporting Act, Pub. L. No. 91-508, §§ 601–622, 84 Stat. 1127 (1970) (codified at 15 U.S.C. §§ 1681–1681x (2012)).

68. Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, § 513, 88 Stat. 571 (codified as amended at 20 U.S.C. § 1232g (2012)).

69. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (2012)).

70. Tax Reform Act of 1976, Pub. L. No. 94-455, § 1202, 90 Stat. 1667 (codified as amended at 26 U.S.C. § 6103 (2012)).

71. Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, §§ 1100–1122, 92 Stat. 3697 (codified as amended at 12 U.S.C. §§ 3401–3422 (2012)).

72. Privacy Protection Act of 1980, Pub. L. No. 96-440, 94 Stat. 1879 (codified as amended at 42 U.S.C. § 2000aa (2012)).

73. Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2794 (codified as amended at 47 U.S.C. § 551 (2012)).

74. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C., including 18 U.S.C. § 2510 (2012)).

75. 18 U.S.C.A. § 2710(b)(1) (West 2015).

services from a video tape service provider."[76] However, the VPPA itself does not provide any other guidance regarding what types of data are or are not covered by PII.[77] In this manner, the VPPA is similar to other federal privacy protection statutes, such as the Right to Financial Privacy Act, which defines one or more classes of protected data, "but do[es] not provide useful guidance on how to determine which data element falls within which class."[78] Meanwhile, other more recent statutes, such as the Children's Online Privacy Protection Act of 1998 ("COPPA")[79] and the Driver's Privacy Protection Act of 1994,[80] expressly identify data elements considered to be protected.[81]

B. The Legislative History of the VPPA: A Broad, Expansive Interpretation of Personally Identifiable Information

Analyzing the legislative history of the VPPA shows that Congress intended for the term PII to be broadly interpreted. The initial House bill aimed at protecting video privacy, House Bill 3523, did not include any mention of PII.[82] Instead, the bill merely prohibited disclosure of "the identity of the individual who rented or purchased" a video tape.[83] The broader term PII, and its original definition, first appeared in a version of Senate Bill 2361: "[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."[84] This definition was subsequently amended to strike the words "or library"[85] and limit the materials or services to "video materials or services."[86] But

76. *Id.* § 2710(a)(3).

77. *See* Scot Ganow & Sam S. Han, *Model Omnibus Privacy Statute*, 35 U. DAYTON L. REV. 345, 352 (2010).

78. *Id.* at 360. For example, the Right to Financial Privacy Act protects an individual's financial records; "'financial record' means an original of, a copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer's relationship with the financial institution." 12 U.S.C. § 3401(2) (2012).

79. Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, §§ 1301–1308, 112 Stat. 2681-728 (codified at 15 U.S.C. §§ 6501–6506 (2012)).

80. Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, §§ 300001–300003, 108 Stat. 2099 (codified as amended at 18 U.S.C. §§ 2721–2725 (2012)).

81. *See* Ganow & Han, *supra* note 77, at 361–63.

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

83. *Id.* § 2(a)(2).

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

85. 134 CONG. REC. S16216 (daily ed. Oct. 14, 1988).

86. 134 CONG. REC. H10410 (daily ed. Oct. 19, 1988) ("The definition of personally identifiable information includes the term 'video' to make clear that simply because a business is engaged in the sale or rental of video materials or services does not mean that all of its products or services are within the scope of the bill.").

this first definition of PII is otherwise identical to the definition of PII found in the VPPA today.[87]

A few of the congressional records surrounding the VPPA shed light on the meaning and scope of the term PII. By way of example, in his section-by-section analysis of Senate Bill 2361, Representative Kastenmeier, a sponsor of the related House bill, explained that "[u]nlike the other definitions in this subsection, subsection (a)(3) uses the word 'includes' to establish a minimum, but not exclusive, definition of personally identifiable information."[88] As another example, Senate Report 599 on Senate Bill 2361 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."[89] Senate Report 599 also mentions that "[t]he Act allows consumers to maintain control over personal information divulged and generated in exchange for receiving services from video tape service providers."[90]

Moreover, the purpose and motivation for enacting the VPPA also provides support for a broad reading of PII. As discussed above, one of the primary impetuses for the VPPA was the disclosure in a Washington, D.C. newspaper of then-Judge Robert Bork's rental records from a local video store.[91] And the VPPA was intended to address that incident as well as other less-newsworthy incidents.[92] Furthermore, Senate Report 599 clearly identifies the purpose of the VPPA as "[t]o preserve personal privacy with respect to the rental, purchase, or delivery of video tapes or similar audio visual materials."[93] Similarly, representative Kastenmeier eloquently summed up the purpose of the VPPA as follows:

> Every day, people are asked to disclose information about themselves that someone then squirrels away in a computer. Every time we provide such information, we're giving a piece of ourselves to someone else. The Video Privacy Protection Act of 1988 ensures that video service providers will respect the privacy of that with which we have entrusted them.[94]

87. The 2013 amendment to the VPPA did not change the definition of PII. *See* Video Privacy Protection Act Amendments Act of 2012, Pub. L. No. 112-258, 126 Stat. 2414 (2013).

88. 134 CONG. REC. H10410.

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

90. *Id.* at 8.

91. *Id.* at 5.

92. *Id.* at 5–6.

93. *Id.* at 1.

94. 134 CONG. REC. H10411 (daily ed. Oct. 19, 1988).

C. Recent Case Law: A Narrow Interpretation of PII at Odds with the Broad Interpretation Supported by the Legislative History

As discussed in the introduction, the Northern District of California recently interpreted the scope of PII.[95] *In re Hulu* involved the disclosure of a Facebook User ID.[96] Unlike a unique device identifier which is assigned to a particular device, a Facebook User ID is assigned to a particular user.[97] Nevertheless, it is interesting to consider the rationale of the court in *In re Hulu* since the litigation involved interpreting the scope of PII under the VPPA.

The facts of *In re Hulu* indicate that when a user was logged in to Facebook on her browser and the user's browser loaded a Hulu web page to watch a video, the user's browser sent to Facebook a cookie that identified the user's Facebook User ID.[98] The user's browser also executed code that provided the web page's URL, which included the title of the video, to Facebook.[99] Therefore, one of the issues before the court was whether a disclosure of a Facebook User ID and a title of a video qualifies as PII under the VPPA.[100]

The court began its analysis by noting that "[t]he [VPPA's] plain language . . . does not say 'identify by name' and thus plainly encompasses other means of identifying a person."[101] Further, the court determined that the ordinary meaning of the plain language suggests that "the disclosure must be pegged to an identifiable person (as opposed to an anonymous person)."[102]

Because the court found the statute's plain language to be "ambiguous about whether it covers unique anonymous user IDs," it turned to the legislative history for guidance.[103] In particular, the court noted the Judge Bork incident as one of the motivations for the VPPA, and analyzed portions of Senate Report 599 discussed above.[104] The order from the district court quoted several portions from the section-by-section analysis of Senate Re-

95. *See In re* Hulu Privacy Litig., No. C 11-03764 LB, 2014 WL 1724344 (N.D. Cal. Apr. 28, 2014).

96. *Id.* at *7. A Facebook User ID is a unique number assigned to a Facebook user. *See, e.g.*, Alyson Shontell, *How to Find Your Facebook Number*, BUS. INSIDER (June 1, 2011, 3:04 PM), http://www.businessinsider.com/how-to-find-your-facebook-number-2011-6.

97. *See* Shontell, *supra* note 96.

98. *In re Hulu*, 2014 WL 1724344, at *5.

99. *Id.*

100. *Id.* at *6.

101. *Id.* at *7.

102. *Id.*

103. *Id.*

104. *Id.* at *8.

port 599 that elaborates on the statutory definition of PII, including a few lines from page seven which describe PII as "information that links the customer or patron to particular materials or services."[105] After quoting a few other passages from Senate Report 599, the court stated that "[t]he plain language of the statute suggests, and the Senate Report confirms, that the statute protects personally identifiable information that identifies a specific person and ties that person to particular videos that the person watched," and cited to page seven of Senate Report 599 for support.[106] Thus, it appears that the court was particularly persuaded by Senate Report 599's description of PII as "information that links the customer or patron to particular materials or services."[107]

The court opted not to rely on the legislative history alone, and looked to precedent from other cases to support its interpretation.[108] Interestingly, because of the lack of precedent directly addressing the disclosure of unique identifiers under the VPPA, the court looked to the scope of PII under the Cable Act of 1984.[109] Specifically, the court examined a case in which Comcast had given to some of its new customers used cable converter boxes that still included prior customers' pay-per-view purchase records.[110] The information stored on the cable converter boxes did not directly indicate the names or addresses of prior customers, but included hexadecimal codes[111] that Comcast, but not the new customers, could decode to identify specific customers.[112] Therefore, to an unsuspecting new customer, the hexadecimal code was not PII.[113]

The court summed up the rule from the cable converter case as follows: "an anonymous unique ID *without* more does not constitute PII. But . . . if an anonymous unique ID were disclosed to a person who could understand it, that might constitute PII."[114] In other words, "context could

105. *Id.*

106. *Id.*

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

108. *In re Hulu*, 2014 WL 1724344, at *9.

109. *See* 47 U.S.C. § 551 (2012). The Cable Act is similar to the VPPA in that the Cable Act protects PII regarding cable subscribers. *See, e.g.*, *In re Hulu*, 2014 WL 1724344, at *10.

110. *In re Hulu*, 2014 WL 1724344, at *10.

111. A hexadecimal code is a number defined in the hexadecimal numbering system. The hexadecimal numbering system is often used in computing systems and has a base of 16. Typically, hexadecimal codes are represented using sixteen distinct symbols: 0-9 representing values zero to nine and A-F representing values ten to fifteen. *See, e.g.*, Tim Fisher, *What Is Hexadecimal? Definition of Hexadecimal & How to Count in Hexadecimal*, ABOUT TECH, http://pcsupport.about.com/od/termshm/g/hexadecimal.htm (last visited Mar. 1, 2015).

112. Pruitt v. Comcast Cable Holdings, LLC, 100 F. App'x 713, 715 (10th Cir. 2004).

113. *Id.* at 716.

114. *In re Hulu*, 2014 WL 1724344, at *11 (emphasis in original).

render [disclosure of a seemingly anonymous unique ID] not anonymous and the equivalent of the identification of a specific person."[115] When applying this reasoning to Hulu's disclosure of Facebook User IDs, the court appropriately classified the unique identifiers as "more than a unique, anonymous identifier."[116] Indeed, one can easily identify a Facebook user's name (and other information) from a Facebook User ID.[117] But because of unresolved issues of material fact as to whether "the information transmitted to Facebook was sufficient to identify individual customers" and Hulu's knowledge[118] of the disclosures, the court stopped short of deeming the disclosure of a Facebook User ID tied to a video title as PII.[119]

Given the scant amount of precedent in this area, other courts were quick to adopt the interpretation of the scope of PII from *In re Hulu*. For instance, in *Ellis v. Cartoon Network, Inc.*, the Northern District of Georgia held that, because an Android ID ("a randomly generated number that is unique to each user and device") does not *without more* identify a specific person, disclosure of an Android ID in conjunction with a user's viewing history on a mobile application is not PII and does not violate the VPPA.[120] Likewise, the District of New Jersey defined PII as "information which must, *without more*, *itself* link an actual person to actual video materials."[121] Consequently, the District of New Jersey reasoned that an alleged disclosure of cookies containing video titles, anonymous user IDs, and data about users' computers did not qualify as PII.[122]

III. THE CASE FOR BROADENING THE SCOPE OF PERSONALLY IDENTIFIABLE INFORMATION TO INCLUDE UNIQUE DEVICE IDENTIFIERS

The final part of this Note outlines several arguments for broadening the scope of PII to include unique device identifiers and then evaluates several potential criticisms of broadening the scope of PII in this manner.

115. *Id.*

116. *Id.* at *14.

117. *See, e.g.*, *Getting Username from Facebook ID*, EXTRAMASTER (Mar. 17, 2013), http://blog.extramaster.net/2013/03/getting-username-from-facebook-id.html.

118. In order to incur liability under the VPPA, a video tape service provider must have "knowingly" disclosed PII. 18 U.S.C.A. § 2710(b)(1) (West 2015).

119. *In re Hulu*, 2014 WL 1724344, at *15–16.

120. Ellis v. Cartoon Network, Inc., No. 1:14-cv-484, 2014 WL 5023535, at *3 (N.D. Ga. Oct. 8, 2014).

121. *In re* Nickelodeon Consumer Privacy Litig., MDL No. 2443(SRC), 2015 WL 248334, at *3 (D.N.J. Jan. 20, 2015) (emphasis in original) (internal quotation marks omitted).

122. *Id.*

A. Broadening the Scope of Personally Identifiable Information to Encompass Unique Device Identifiers Disclosed in Conjunction with Video Titles

Although courts have been reluctant to assert that unique device identifiers constitute PII when disclosed in conjunction with one or more video titles, this type of disclosure should be protected as PII in light of the VPPA's broad definition of PII, technological changes in the way consumers view video content, and the practical alternatives available to video-streaming providers.

As discussed above, the VPPA was meant to protect consumers' "personal information divulged and generated in exchange for" renting or purchasing video materials.[123] And by using the word "includes" when defining PII, subsection (a)(3) of the VPPA establishes a minimum definition of PII that is not exclusive.[124] In other words, PII was meant to cover, at a minimum, "information which identifies a person as having requested or obtained specific video materials or services," but also cover other types of identifying information.[125] The legislative history firmly supports and validates this interpretation.[126] Additionally, the advantage of defining PII in this manner is that the scope of PII "can evolve and remain flexible in response to new developments."[127]

Given the foregoing, the interpretation of PII proffered by the Northern District of California in *In re Hulu*, and subsequently adopted by other courts across the country, is too rigid. PII should not be limited to information that must, *without more*, connect an actual person to actual video materials. This definition may have been suitable during the first decade following the enactment of the VPPA, but it is arguably inappropriate today.

Many consumers no longer rent or purchase videos at brick-and-mortar video stores, where they were previously asked to provide their names and possibly their addresses in exchange for the right to purchase or rent a video cassette, DVD, Blu-ray, etc. Instead, consumers are now shifting to streaming movies using their televisions, computers, and mobile devices.[128] This new avenue for consuming video content creates new types

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

124. 18 U.S.C.A. § 2710 (a)(3) (West 2015).

125. *Id.*

126. *See* S. REP. NO. 100-599, at 12.

127. Schwartz & Solove, *supra* note 48, at 1829.

128. *See, e.g.*, Chiang-nan Chao & Saibei Zhao, *Emergence of Movie Stream Challenges Traditional DVD Movie Rental—An Empirical Study with a User Focus*, INT'L J. BUS. ADMIN. 22, 22 (2013).

of personal information that must be safeguarded. By way of example, rather than providing only their name and address in exchange for video materials, consumers now provide the unique device identifiers of their video-streaming devices in exchange for video materials. It is against this backdrop that the scope of PII should be defined today.

Rather than only including information that links an actual person to actual video materials *without more*, the scope of PII should simply encompass information that links an actual person to actual video materials.[129] The interpretation requiring the disclosed information *itself* to identify a person does not appreciate the broad definition of PII that is found within the VPPA.[130] Information that itself identifies an actual person is an example of PII that falls within the minimum definition of PII outlined above.[131] And in the context of rental or purchase of physical video materials (e.g., video cassette tapes or DVDs), perhaps such a minimum definition is workable. But when a particular consumer exposes other types of information that can be used to link the particular consumer to videos viewed by the particular consumer, a broader, more inclusive definition of PII is necessary to preserve personal privacy.

In line with the discussion above, a unique device identifier of a device can be correlated with a particular individual, such that videos watched on the device can be linked to the particular individual.[132] For the VPPA to adequately protect the particular individual's personal privacy, the scope of PII needs to be broadened to include the disclosure of the unique device identifier of the individual's device in conjunction with the titles of videos watched on the individual's device. Otherwise, video-streaming providers could continue to escape liability by disclosing unique device identifiers of their consumers' devices to third-party data-aggregation companies, to whom unique device identifiers are just as valuable as names and addresses in terms of correlating video content with particular individuals.[133]

The ease with which third-party data-aggregation companies can correlate unique device identifiers to particular individuals also suggests that the scope of PII should include unique device identifiers disclosed in con-

129. *See* S. REP. NO. 100-599, at 7 (defining PII as "information that links the customer or patron to particular materials or services" without using qualifications such as *without more* or *itself*).

130. *See* 18 U.S.C.A. § 2710(a)(3).

131. *See id.*

132. *See, e.g.*, Schwartz & Solove, *supra* note 48, at 1843–44.

133. *See, e.g.*, CNN Complaint, *supra* note 23, at 15–21.

junction with video titles.[134] Generally, when considering whether a piece of data is "identifying," one important factor is the ease with which the piece of data can be correlated with other pieces of data that ultimately lead to an identification of a particular individual.[135] The easier it is to correlate a piece of data with information that can be used to identify an individual, the more likely that piece of data should be protected.[136] And further, "[a]s the volume of data increases, so too do the chances for identifiability."[137] A company that collects millions of data points regarding millions of individuals, and specializes in correlating pieces of data with particular individuals, can easily correlate a unique device identifier with a particular individual.[138] Therefore, because unique device identifiers can easily be linked to particular individuals, a disclosure of a unique device identifier and a video title should qualify as information which identifies a person as having obtained a specific video (i.e., PII).[139]

Moreover, a broad interpretation of the scope of PII will be in accord with existing concerns regarding consumer privacy expressed by the legislature. Members of Congress have expressed concern about the use of database marketing. Various Senators have warned about the use of consumers' personal information, including the collection and tracking of unique device identifiers.[140] Similarly, recent actions of federal government actors demonstrate concerns over the tracking of unique device identifiers. For example, the Children's Online Privacy Protection Rule, which regulates the disclosure of children's personal information, was recently amended to broaden the scope of personal information.[141] The regulation had always defined "personal information" as "individually identifiable information about an individual collected online, including: . . . persistent identifier[s]," but the meaning of persistent identifiers was extended to

134. *See* Eloise Gratton, *If Personal Information Is Privacy's Gatekeeper, Then Risk of Harm Is the Key: A Proposed Method for Determining What Counts as Personal Information*, 24 ALB. L.J. SCI. & TECH. 105, 175 (2014).

135. *Id.* at 171.

136. *See id.* at 172.

137. *Id.* at 174.

138. *See, e.g.*, Marwick, *supra* note 29.

139. *See* Gratton, *supra* note 134.

140. *See, e.g.*, *Consumer Privacy and Protection in the Mobile Marketplace: Hearing Before the Subcomm. on Consumer Prot., Prod. Safety, & Ins. of the Comm. on Commerce, Sci., & Transp.*, 112th Cong. (2011).

141. The Federal Trade Commission's initial regulations became effective on April 21, 2000. The Federal Trade Commission's amended rule took effect on July 1, 2013. *See Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (July 16, 2014), http://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

include "device serial number[s]" and "unique device identifier[s]."[142] Thus, an expanded interpretation of PII under the VPPA that includes unique device identifiers disclosed along with video titles would be consistent with recent administrative sentiments about consumer privacy.

Likewise, broadening the scope of PII would be consistent with Congress' intent for the VPPA to evolve over time. When Congress passed the VPPA, it was aware of how technology was revolutionizing the way people watched videos, and the need to protect the right to privacy "as we continue to move ahead."[143] Congress did not choose to define a video tape service provider as a brick-and-mortar video store.[144] Instead, by including the broad catch-all term "similar audio visual materials," Congress defined a video tape service provider in a way that would protect consumers' interactions with the brick-and-mortar video stores of the future.[145] Further, as discussed above, Senate Report 599 also mentions that the VPPA was designed to allow consumers "to maintain control over personal information divulged and generated in exchange for receiving services from video tape service providers."[146] As video tape service providers evolve and consumers divulge different forms of identification to video tape service providers, the notion of what qualifies as PII should similarly evolve.

Indeed, many commentators have noted that the definition of PII is changing as technology evolves.[147] While certain types of information may relate to an inanimate object itself (e.g., a smartphone or tablet) rather than an individual directly, some argue that information about a "device linked to a small number of individuals" qualifies as personal information.[148] Additionally, as part of a developing trend, many states now protect IP addresses of computing devices as PII.[149] This movement is driven in part by the idea that it is becoming harder and harder to "de-identify" data:

> The more information about a person that is known, the more likely it becomes that this information can be used to identify that person or de-

142. The regulation defines personal information as "individually identifiable information about an individual collected online, including . . . (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." 16 C.F.R. § 312.2 (2015).

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

144. *See* 18 U.S.C.A. § 2710(a)(4) (West 2015).

145. *Id.*

146. S. REP. NO. 100-599, at 8.

147. *See, e.g.*, Gratton, *supra* note 134, at 136–39.

148. *Id.*

149. Joshua J. McIntyre, Comment, *Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information*, 60 DEPAUL L. REV. 895, 918–19 (2011).

> termine further data about her. When aggregated, information has a way of producing more information, such that de-identification of data becomes more difficult.[150]

And even when data is de-identified, there are still ways to re-identify the data.[151] Thus, it is arguably necessary to increase the scope of PII in order to limit the number of data pieces available for aggregation and identification.

Finally, the potential benefits of broadening the scope of PII outweigh the potential burdens of doing so. If the scope of PII under the VPPA were to be broadened to include unique device identifiers disclosed in conjunction with video titles, it would be illegal for a video-streaming content provider to disclose viewing records that include specific video titles and unique device identifiers to third parties.[152] This would provide greater privacy to customers of such a video-streaming content provider. It would theoretically be more difficult for the customers' viewing histories to be correlated with their identities, since data-aggregation companies would no longer be able to use the customers' unique device identifiers for correlation and identification purposes.

On the other hand, for the video-streaming content provider, its customers' viewing records may potentially become less valuable. This could, in turn, result in a decrease in revenue for the video-streaming content provider, assuming third parties would not be willing to pay as much for viewing records that are not associated with unique device identifiers. However, there are several options still available for the video-streaming content provider to profit from its customers' viewing records. The VPPA allows the video-streaming content provider to disclose PII of any consumer with the informed, written consent of that consumer.[153] The VPPA also allows the video-streaming content provider to disclose solely the name and address of a consumer in conjunction with the subject matter of videos viewed by the consumer, provided that the consumer was given the opportunity to prohibit such disclosure and the "disclosure is for the exclusive use of marketing goods and services directly to the consumer."[154] Further, the VPPA presumably would allow the video-streaming content provider to disclose a unique device identifier of a consumer's device in conjunction

150. Schwartz & Solove, *supra* note 48, at 1843.
151. *Id.*
152. *See* 18 U.S.C.A. § 2710(b) (West 2015).
153. *See id.* § 2710(b)(2)(B).
154. *Id.* § 2710(b)(2)(D).

with a subject matter of videos viewed by the consumer, as long as the disclosure did not identify *particular* videos viewed by the consumer.[155]

On balance, the potential benefits to the video-streaming content provider's consumers appear to outweigh the burdens on the video-streaming content provider. Expanding the scope of PII under the VPPA to cover unique device identifiers linked to video titles could provide increased privacy to consumers that stream videos without completely barring video-streaming content providers from marketing their customers' viewing information. This analysis is in accord with the recent actions of several large players in the technology industry who have recognized the importance of protecting consumer privacy. For example, due to consumer privacy concerns, Apple Inc. began randomizing MAC addresses when iPhones scan for Wi-Fi signals, in an effort to prevent companies from tracking movement of individuals using the MAC addresses of their iPhones.[156] Similarly, Google Inc. switched from using its unique Android ID for advertising purposes in apps to using an anonymous identifier.[157] The new anonymous identifier is "a long, anonymous string of digits that will allow tracking and ad targeting without relying on an identifier uniquely married to the device" and can be reset by a user.[158]

B. Arguments Against Broadening the Scope of Personally Identifiable Information to Include Unique Device Identifiers

Perhaps the primary concern with broadening the scope of PII in the manner proposed herein is that unique device identifiers are assigned to inanimate objects (namely, computers, mobile devices, televisions, etc.) rather than to particular individuals, and therefore, unique device identifiers serve to identify objects rather than individuals. Because of this concern,

155. *See In re* Hulu Privacy Litig., No. C 11-03764, 2014 WL 1724344, at *8 (N.D. Cal. Apr. 28, 2014).

156. *See, e.g.*, Aaron Mamiit, *Apple Implements Random MAC Address on iOS 8. Goodbye, Marketers*, TECH TIMES (June 12, 2014, 3:46 AM), http://www.techtimes.com/articles/8233/20140612/apple-implements-random-mac-address-on-ios-8-goodbye-marketers.htm. Unfortunately, the feature seems to work only in limited scenarios (when location tracking is off, the iPhone is in sleep mode, and the iPhone is not connected to a Wi-Fi network). *See* Jim Edwards, *Apple's New Anti-Tracking System for iPhones Doesn't Work, Researcher Claims*, BUS. INSIDER (Oct. 1, 2014, 6:18 AM), http://www.businessinsider.com/ios-8-mac-randomization-wifi-iphone-doesnt-work-2014-10.

157. *See, e.g.*, Greg Sterling, *Google Replacing "Android ID" with "Advertising ID" Similar to Apple's IFDA*, MARKETING LAND (Oct. 31, 2013, 2:18 PM), http://marketingland.com/google-replacing-android-id-with-advertising-id-similar-to-apples-idfa-63636.

158. *Id.*

courts have been reluctant to grant protection under the VPPA to information about an individual's device(s).[159]

This criticism is flawed for at least two reasons. Initially, as outlined above, such a narrow interpretation of PII under the VPPA is improper in light of the text, purpose, and legislative history of the VPPA.[160] Furthermore, the concern about information identifying a device instead of a person fails to appreciate the changing nature of personal information; many people now use computing devices on a daily basis, and those computing devices can be traced back to particular individuals. Interestingly, as discussed above, the amended text of the Children's Online Privacy Protection Rule now unequivocally suggests that a unique device identifier of an individual's device *does qualify* as PII about that individual.[161] Likewise, legislators are shifting towards protecting information about computing devices, such as IP addresses, as PII.[162] Moreover, many statutes consistently protect data that does not necessarily identify an individual, such as a home address or telephone number.[163] Like a home address or telephone number, a unique device identifier may certainly be tied to a particular individual, and thus, merit similar protection. In the not-so-distant future, the trend to extend protection to information about individuals' devices is likely to continue, rather than regress.

Another related concern about broadening the scope of PII in the manner proposed herein is that considering information that identifies a device (rather than an individual) to be PII may be problematic if multiple people use the same device. As the argument goes, multiple individuals may share the same device, and consequently, information that identifies that device identifies multiple individuals rather than just one specific individual.[164] This criticism is also without merit, as many types of PII do not necessarily identify a single person either. For instance, "multiple people may have the same name, multiple residents may share the same home address and telephone number, and multiple users may log in to the same e-mail address."[165] In other words, unique device identifiers are actually quite similar to other forms of potentially ambiguous personal information.

159. *See, e.g.*, *In re* Nickelodeon Consumer Privacy Litig., MDL No. 2443(SRC), 2014 WL 3012873, at *10 (D.N.J. July 2, 2014).

160. *See supra* Part II(B).

161. 16 C.F.R. § 312.2 (West 2015).

162. *See* McIntyre, *supra* note 149, at 918–19.

163. *See id.* at 934–35.

164. *See, e.g.*, *In re* Hulu Privacy Litig., No. C 11-03764, 2014 WL 1724344, at *14 (N.D. Cal. Apr. 28, 2014).

165. McIntyre, *supra* note 149, at 906.

CONCLUSION

The VPPA prohibits a video tape service provider from knowingly disclosing PII concerning any of its consumers to third parties. This Note has argued that a disclosure that includes a unique device identifier of a user's device and the title of a video should qualify as PII under the VPPA.

Reviewing the legislative history surrounding the VPPA and recent case law reveals that the interpretation of PII adopted by several courts is too rigid. Rather than only including information that links an actual person to actual video materials *without more*, the scope of PII should simply encompass information that links an actual person to actual video materials. Broadening the scope of PII in this manner is merited given Congress' motivation for enacting the VPPA, technological changes in the way consumers view video content today, and the ease with which unique device identifiers can be correlated with particular individuals. By the same token, broadening the scope of PII would address growing concerns regarding consumer privacy and be consistent with the changing notion of what qualifies as PII.

Thus, unique device identifiers of devices that are disclosed with video titles viewed on those devices should be protected as PII under the VPPA.