2-15-2018

PII in Context: Video Privacy and a Factor-Based Test for Assessing Personal Information

Daniel L. Macioce Jr.

Follow this and additional works at: https://digitalcommons.pepperdine.edu/plr
Part of the Internet Law Commons, and the Privacy Law Commons

Recommended Citation
Available at: https://digitalcommons.pepperdine.edu/plr/vol45/iss2/2

This Comment is brought to you for free and open access by the School of Law at Pepperdine Digital Commons. It has been accepted for inclusion in Pepperdine Law Review by an authorized editor of Pepperdine Digital Commons. For more information, please contact josias.bartram@pepperdine.edu, anna.speth@pepperdine.edu.
PII in Context: Video Privacy and a Factor-Based Test for Assessing Personal Information

Abstract

As a central concept in American information privacy law, personally identifiable information (PII) plays a critical role in determining whether a privacy violation has occurred. Under the Video Privacy Protection Act of 1988 (VPPA), PII “includes information which identifies a person as having requested or obtained specific video materials or services.” Despite the clarity that these words may have when the Statute was enacted, the line separating PII from non-PII in the context of streaming video is not easily drawn, in part due to the prevalence of behavior tracking technologies and the emergence of “big data” analytics. The First Circuit, in Yershov v. Gannett Satellite Information Network, Inc., has held that PII is information that is “reasonably and foreseeably likely” to identify a person’s video viewing activities. By contrast, under the Third Circuit’s holding in In re Nickelodeon Consumer Privacy Litigation, PII is information that would enable an ordinary person to identify an individual. As applied to device identifiers, Internet “cookies,” and other behavior tracking information, the Third Circuit’s “ordinary person” test undermines an important privacy interest.

This Comment examines the meaning of PII under the VPPA, tracing the evolution of the concept from its origins through the Statute’s legislative history and modern jurisprudence. After arguing that the intent of the VPPA is best effectuated by a consideration of the context in which the information is disclosed, this Comment identifies the salient contextual factors and concludes by urging the adoption of a factor-based test for determining whether information constitutes PII.
TABLE OF CONTENTS

I. INTRODUCTION .......................................................................................................................... 333

II. BACKGROUND: INFORMATION PRIVACY AND THE CHALLENGES OF PII ......................................................... 336
   A. What Is Personally Identifiable Information? ................................................................. 342
   B. Drawing Inferences of Identity from Non-PII .............................................................. 345
      1. Linking PII and Non-PII ......................................................................................... 347
      2. Creating PII from Non-PII .................................................................................. 348
      3. Linking Non-PII Using a Common Identifier ...................................................... 349

III. THE VPPA: CURRENT STATE OF THE LAW AND ITS DEVELOPMENT ................................................................. 351
   A. Congressional Intent .................................................................................................... 353
      1. The 1988 Enactment ......................................................................................... 355
      2. The 2013 Amendment ...................................................................................... 359
   B. In re Hulu II and Its Progeny .................................................................................... 361
   C. Yershov v. Gannett Satellite Information Network, Inc. ........................................ 368
   D. In re Nickelodeon Consumer Privacy Litigation ....................................................... 370

IV. ANALYSIS .................................................................................................................................. 372
   A. Of Differing Standards and Unpredictable Results ................................................... 374
      1. The First Circuit’s Reasonable and foreseeable Likelihood Test ................................ 375
      2. The Third Circuit’s Ordinary Person Test .................................................................. 380
   B. Factors for Determining PII under the VPPA .............................................................. 387
      1. Capability to Link Information to an Identified Individual ....................................... 390
      2. Availability of Additional Information Identifying an Individual .............................. 391
      3. Uniqueness of the Information Disclosed ............................................................... 392
      4. Length of Time Information Will Be Stored ............................................................ 392
      5. Incentives to Identify an Individual ..................................................................... 393
      6. Likelihood That the Data Will Be Further Shared or Disclosed ............................... 394

V. IMPACT AND SIGNIFICANCE OF THE RECENT VPPA DECISIONS .............................................................. 394
   A. Recent Decisions Undermine Privacy Interests and Create Uncertainty ................. 395
   B. Recent Decisions Highlight the Need for Forward-Looking Privacy Regulations ........ 397
   C. Absent Congressional Action, Courts Should Adopt a
I. INTRODUCTION

A twelve-year-old boy—let’s call him William—uses his mobile phone to watch streaming videos, including superhero cartoons, comedy shorts, and action movies, on an Internet video website (video site).1 As he watches, advertisements are displayed at the bottom of the video.2 These advertisements are not served by the video site, but by a third-party advertising platform (ad platform), which has a somewhat ubiquitous presence on the Internet.3 In fact, most of the other websites William visits, as well as several of the mobile phone applications that he uses, all display advertisements served by this ad platform.4

Unbeknown to William or his parents, William’s use of the Internet has enabled the ad platform to collect information about William, including his name, Global Positioning System (GPS) coordinates of the locations where he has used his device, information that uniquely identifies his smartphone, the Internet “cookies”5 that have been placed on William’s phone by the ad platform, the Internet Protocol (IP) address that has been assigned to his device, and several characteristics about his device, operating system, and

---

1. This hypothetical fact pattern is drawn from the facts of In re Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 268–70 (3d Cir. 2016), cert. denied, 137 S. Ct. 624 (2017).
2. See id. at 269–70.
3. See id. at 268. The “ubiquitous presence” of the ad platform is significant because the ad platform is able to track user interactions across every website on which its advertisements are displayed. See id. at 269–70. The more pervasive the ad platform’s presence is on the Internet, the more information it is potentially able to collect about each person it tracks. See id.; see also discussion infra Section II.B.3.
4. See In re Nickelodeon, 827 F.3d at 268–70.
5. See id. at 268; see also Janice C. Sipior et al., Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons, 10 J. INTERNET COM. & L. 1 (2011) (providing a basic introduction on the use of cookies and other technologies to track user behavior on the Internet and related privacy concerns). An Internet cookie is a small file created by a website visited by the user and stored on the user’s device. Sipior et al., supra, at 2–3. While this file can contain any information a website chooses to store there, it is commonly used to assist a website to identify the user on subsequent visits, as well as to assist an advertising platform in tracking user activity across all the websites on which the advertising platform displays advertising. Id. at 2–3, 8–11; see also discussion infra Section II.B.3.
browser settings, which combine to form a browser “fingerprint.” The ad platform collects this information into a user profile, to which subsequent Internet activity may be linked. Collecting and analyzing information about user behavior is at the core of the ad platform’s behavior targeting technology, and the video site is aware of the ad platform’s use of this technology.

When William watches a video, the video site transmits information about the video and William’s interaction with the video site to the ad platform. This information includes the title of the video, the unique mobile device identifier of William’s phone, his phone’s IP address, and his browser’s fingerprint. Correlating this information with information the ad platform has already assembled in William’s profile, the ad platform links William’s video viewing activity to his profile. The ad platform then uses the behavioral information that it has amassed about William, including his video viewing activities, to target advertisements at him. Much to the chagrin of William’s parents, these advertisements promote fast food and e-cigarettes.

6. See In re Nickelodeon, 827 F.3d at 268–70. Browser fingerprints provide a highly accurate way for websites, marketing analytics services, and behavior targeting technologies to associate Internet activities of an individual with other information that has already been collected. See discussion infra notes 96–101 and accompanying text.

7. See In re Nickelodeon, 827 F.3d at 268–70. Subsequently collected information may be linked to a user profile through the use of a common identifier. See infra Section II.B.3.

8. See In re Nickelodeon, 827 F.3d at 268–70.

9. See id. at 269.

10. See id. at 268–70.

11. Unique mobile device identifiers, such as the “Android ID” or “Advertising ID,” uniquely identify smartphones and other mobile devices. See infra notes 119–21 and accompanying text. Courts have used the terms unique anonymous identifier, and information-anonymous identifier to refer broadly to information that—like unique mobile device identifiers—can be used, albeit indirectly, to identify a specific individual. See, e.g., In re Hula Privacy Litig. (In re Hula ID), No. C11-03764 JLB, 2014 WL 1724344, at *10–11 (N.D. Cal. Apr. 28, 2014) (using the term unique anonymous identifier to refer to any unique identifier that does not directly identify a specific person); Eichenberger v. ESPN, Inc., No. C14-463 TSZ, 2015 WL 7252985, at *4 (W.D. Wash. May 7, 2015) (using the term information-anonymous identifier to refer to “otherwise anonymous identification numbers or information”), aff’d, 876 F.3d 979 (9th Cir. 2017). However, these terms may be “unhelpful and possibly misleading,” in that they presume the underlying information is anonymous. Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 146 (D. Mass. 2015). Thus, this Comment adopts more descriptive, precise terms, such as unique mobile device identifier.

12. See In re Nickelodeon, 827 F.3d at 268–70.

13. See id.

14. See id.

15. See id. at 269 (“The purpose of all of this information gathering is to sell targeted advertising based on users’ web browsing,”); Dale S. Mantey et al., E-Cigarette Marketing Exposure Is Associated
The Video Privacy Protection Act of 1988 (VPPA), prohibits a "video tape service provider," from knowing or disclosing "personally identifiable information," (PII) about its customers. The statute defines PII to include [ ] information which identifies a person as having requested or obtained specifically, video materials or services. The video service provider's decision to link William's video viewing activity to his profile, which were unanticipated to apply the VPPA to factual circumstances not included within the First Circuit's holding in VPPA. By contrast, under the VPPA's holding in In re Nickelodeon, such information may constitute PII within the context of the statute. This Comment examines the meaning of PII within the context of the VPPA.
VPPA and argues for the adoption of a factor-based test for determining whether information constitutes PII.\textsuperscript{22} Part II discusses the development of privacy law in America, tracing the rise of PII as a fundamental concept of American privacy law and examining the challenges wrought by technological innovation.\textsuperscript{23} Part III reviews the current state of the law as it has developed from the VPPA’s enactment through recent circuit court decisions.\textsuperscript{24} Part IV analyzes the standards announced by the First and Third Circuits, and proposes a factor-based test.\textsuperscript{25} Part V discusses the impact and significance of the split in authority, and argues for the adoption of the proposed test.\textsuperscript{26} Finally, Part VI concludes.\textsuperscript{27}

II. BACKGROUND: INFORMATION PRIVACY AND THE CHALLENGES OF PII

There is no single, comprehensive definition of privacy.\textsuperscript{28} In their seminal article, \textit{The Right to Privacy}, Justices Warren and Brandeis defined the right to privacy as the “right of the individual to be let alone.”\textsuperscript{29} But courts subsequently expanded the concept to include protection of four distinct interests,\textsuperscript{30} including an interest in seclusion or solitude,\textsuperscript{31} an interest in information about

\textsuperscript{22} See infra Parts II–VI.
\textsuperscript{23} See infra Part II.
\textsuperscript{24} See infra Part III.
\textsuperscript{25} See infra Part IV.
\textsuperscript{26} See infra Part V.
\textsuperscript{27} See infra Part VI.
\textsuperscript{29} Samuel D. Warren & Louis D. Brandeis, \textit{The Right to Privacy}, 4 HARV. L. REV. 193, 206 (1890). Justices Warren and Brandeis were concerned primarily with protection from exposure of nonpublic personal information by “the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds.” \textit{Id.} at 206.
\textsuperscript{31} See id. at 389. Put another way, the interest in seclusion is “an interest in respite from observation and judgment.” Jane Yakowitz Bambauer, \textit{The New Intrusion}, 88 NOTRE DAME L. REV. 205, 230 (2012). This interest is not merely an interest in protecting against physical intrusions into one’s solitude or seclusion (e.g., when the intruder enters into one’s home), but it also involves concerns about nonphysical intrusion into private information (e.g., when the intruder uses a listening device to listen to a private telephone conversation). \textit{See Prosser, supra} note 30, at 390; \textit{see also} Bambauer, \textit{supra}, at 207–10 (arguing that the intrusion tort should be expanded further to provide a remedy for harm caused by “the observation of [personal] data” (emphasis in original)). Courts have held that
oneself, an interest in one’s reputation, and a proprietary interest in one’s name or likeness. The Supreme Court has also recognized that the right to privacy protects decision-making in personal matters. Thus, the concept of privacy is complex and involves several distinct, interrelated interests.

One interest that is central to nearly all conceptions of privacy is one’s ability to control information about oneself. Privacy scholars have identified

collection of a person’s video viewing activity does not constitute an intrusion, unless duplicitous tactics are used. See, e.g., In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 293-95 (3d Cir. 2016), cert. denied, 137 S. Ct. 624 (2017) (holding that the intrusion claim was adequately alleged against provider who employed deceptive tactics to collect information, but not against the third party who merely received the information disclosed by the provider). Note, also, that while the intrusion tort focuses on the observation of personal information, the VPPA protects against the disclosure of information. See infra notes 38-40, 42 and accompanying text.

32. See Prosser, supra note 30, at 392 (noting that one has an interest in not having private, embarrassing facts about oneself disclosed publicly). The interest protected here relates to disclosure of truthful information, which, if disclosed, would damage one’s reputation. Id. at 398. Importantly, this interest is narrower than the interest protected by the VPPA, which has no requirement that the disclosure be embarrassing or damaging to a person’s reputation. See 18 U.S.C. § 2710(b)(2) (2012). Indeed, the disclosure of a person’s video viewing activity may not reveal any unsavory activities, but it may nevertheless be objectionable because of the personal nature of the information revealed. See discussion infra Section III.A (discussing the VPPA’s pre-emption history).

33. Prosser, supra note 30, at 398. The interest protected here relates to the dissemination of false information that is damaging to the person’s reputation. Id. By contrast, the interests protected by the VPPA relate to truthful information about the videos a person has watched, without regard to the impact of the disclosure on the person’s reputation. See 18 U.S.C. § 2710(b)(2).

34. Prosser, supra note 30, at 406.

35. See Roe v. Wade, 410 U.S. 113, 152–53 (1973) (noting that the right to privacy extends to “activities relating to marriage, procreation, contraception, family relationships, and child rearing and education” (citations omitted), and that it is “broad enough to encompass a woman’s decision whether or not to terminate her pregnancy”).

36. See DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 37 (2008) (describing the task of finding a “common denominator” underlying the various conceptions of privacy as “onerous” and likely to be simultaneously overbroad and underinclusive). As a result of the difficulty in trying to conceptualize privacy, the right to privacy has been criticized extensively by theorists who hold that it has never been clearly defined. See, e.g., Judith Jarvis Thomson, The Right to Privacy, 4 PHIL. & PUB. AFF. 295, 295 (1975) (“Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is.”).

37. See Whalen v. Roe, 429 U.S. 589, 598–600, 605 (1977) (recognizing that the right to privacy includes an individual’s interest in “avoiding disclosure of personal matters,” and expressing an awareness that “the accumulation of vast amounts of personal information” in massive databases creates a threat to privacy); W. A. Parent, Privacy: Morality and the Law, 12 PHIL. & PUB. AFF. 269, 269 (1983) (“Privacy is the condition of not having undocumented personal knowledge about one possessed by others.”); Adam D. Moore, Privacy: Its Meaning and Value, 40 AM. PHIL. Q. 215, 216 (2003) (“Privacy has to do with control over access to oneself and to information about oneself.”). But see SOLOVE, supra note 36, at 37-38 (arguing that any attempt to locate a common denominator for all of privacy law is a fruitless endeavor, likely to result in a conception of privacy that is both over- and
five ways in which personal information may be controlled or regulated, including observation, capture, processing, dissemination, and use.\textsuperscript{38} \textit{Observation} is the mere perceiving or viewing of the personal data by another.\textsuperscript{39} \textit{Capture} involves the collection and storage of personal data.\textsuperscript{40} \textit{Processing} refers to manipulation of information after it has been collected, and may include aggregation, anonymization, re-identification, and linking or merging it with information collected from other sources.\textsuperscript{41} \textit{Dissemination} means disclosure or distribution of the personal data.\textsuperscript{42} \textit{Use} involves the application of personal

\textsuperscript{38} See Bambauer, supra note 31, at 211 (suggesting that there are “four regulable stages” of personal information flow, including “observation, capture, dissemination, and use”). Bambauer does not include “processing” as a separate stage, but considers it to be part of the “capture” stage. See id. at 212–13 n.31–32 (comparing Bambauer’s categorization to the taxonomy of privacy harms suggested by Solove). However, the distinction between “capture” and information processing is important because each may implicate different privacy concerns and therefore be regulated separately. Compare infra note 40 (citing the Children’s Online Privacy Protection Act as an example of a restriction on the collection of information) with infra note 41 (citing the Privacy Act of 1974 as an example of a restriction on the aggregation of information). Solove’s taxonomy also categorizes information privacy harms into four categories, including “information collection,” “information processing,” “information dissemination,” and “invasion.” Daniel J. Solove, \textit{A Taxonomy of Privacy}, 154 U. Pa. L. Rev. 477, 489 (2006). Solove combines harms relating to “observation” and “information collection” into a single category, but there is value in considering these two categories separately in the context of defining what is regulable. Compare infra note 39 (citing case law and statutory examples imposing restrictions on access to information) with infra note 40 (citing Children’s Online Privacy Protection Act as an example of a restriction on the collection of information). Thus, because observation, capture, and processing represent distinct privacy interests and associated harms, there is value in characterizing these as distinct stages or categories. See Solove, supra, at 486–87 (“The goal is to define more precisely what the problem is in each context—how it is unique, how it differs from other problems, and how it is related to other types of privacy problems.”).

\textsuperscript{39} Bambauer, supra note 31, at 211; see, e.g., Kyllo v. United States, 533 U.S. 27, 39–40 (2001) (holding that use of a thermal imaging device to observe heat emanating from a home revealed “intimate” details and therefore violated defendant’s reasonable expectation of privacy); Cannedy v. Boardman, 16 F.3d 183, 188 (7th Cir. 1994) (holding that unnecessary observation of a male inmate’s naked body by female guards was a violation of the inmate’s reasonable expectation of privacy, for the protection of which he was entitled to reasonable accommodation); Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1330(a)(2)(A) (2012) (criminalizing the unauthorized access of financial information contained in the records of a financial institution or consumer reporting agency); see also Solove, supra note 38, at 491–99.

\textsuperscript{40} Bambauer, supra note 31, at 211; see, e.g., Children’s Online Privacy Protection Act, 15 U.S.C. §§ 6501–6502 (2012) (regulating the collection of personal information from children under thirteen years old); see also Solove, supra note 38, at 491–505.

\textsuperscript{41} Solove, supra note 38, at 505–06; see, e.g., Privacy Act of 1974, 5 U.S.C. § 552a (2012) (establishing restrictions on the joining and aggregation of PII between government agencies).

\textsuperscript{42} Bambauer, supra note 31, at 211; see, e.g., Video Privacy Protection Act of 1988, 18 U.S.C.
information in a manner that "directly affects an outcome or determination" about the data subject.\textsuperscript{43} These categories describe the ways in which a privacy regulation may restrict the handling of personal information.\textsuperscript{44} Such restrictions are aimed at providing individuals with a way to exert control over their personal information.\textsuperscript{45}

Advances in technology have driven much of privacy law's development,\textsuperscript{46} particularly with regard to information privacy.\textsuperscript{47} The computerization of government records in the 1960s ignited privacy concerns, prompting the government to take action to curb information privacy abuses.\textsuperscript{48} In 1973,
the Department of Health, Education, and Welfare (DHEW) proposed a set of fair information practices (FIPs) aimed at protecting a data subject’s right to participate in the control of personal information that had been collected and stored in an institution’s data systems. These principles recognized the difficulty in striking “an appropriate balance between the interest of the individual in controlling information about himself and all other interests—institutional and societal.” In attempting to strike that balance, DHEW distinguished between data in “personally identifiable form” (i.e., PII) and statistical data that could not be traced back to an individual, and its recommendation afforded protection only to the former.

Although the beginnings of our “Information-Based Society” can be traced back to the increased centralization of government resulting from the federal government’s involvement in social welfare programs, the increased availability and information processing capabilities of computers enabled government, institutions, and private enterprise to turn their desire for more information into action, thereby increasing the threat to information privacy. Miller, supra note 45, at 20–23.

49. U.S. DEP’T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 40–42 (1973) [hereinafter DHEW REPORT]. The FIPs included a prohibition on “secret” record systems, a provision affording an individual with the right to know what personal information had been collected, and a requirement that personal information be used only for the purpose for which it had been collected, along with several other principles. Id. at 41. These principles have had a long-lasting global impact on information privacy law, and although the FIPs have evolved over time, the original principles have been substantially retained. See Robert Gellman, Fair Information Practices: A Basic History 6–9 (Apr. 10, 2017), http://bobgellman.com/rg-docs/rg-FIPsistory.pdf[https://perma.cc/6AU3-4H34]. Underlying development of these principles is a “concept of mutuality,” which recognizes that a data subject’s right to control PII is a nonequitable right shared with the institution that possesses the information. DHEW REPORT, supra, at 40–41. As set forth by DHEW, this concept of mutuality provides that

[a]n individual’s personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record. A record containing information about an individual in identifiable form must, therefore, be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it. Any recording, disclosure, and use of identifiable personal information not governed by such procedures must be proscribed as an unfair information practice unless such recording, disclosure or use is specifically authorized by law.

Id.

50. DHEW REPORT, supra note 49, at 52.

51. See id. at 103 (“The protection should be limited to data identifiable with, or traceable to, specific individuals. When data are released in statistical form, reasonable precautions to protect against ‘statistical disclosure’ should be considered to fulfill the obligation not to disclose data that can be traced to specific individuals.”).
The Privacy Act of 1974\(^\text{52}\) (Privacy Act) embraced these FIPs,\(^\text{53}\) and together with the Fair Credit Reporting Act of 1970\(^\text{54}\) (FCRA) and Family Educational Rights and Privacy Act of 1974\(^\text{55}\) (FERPA), signaled a shift in privacy law from a tort-based approach focused on harm to a preventive approach focused on data.\(^\text{56}\) Since then, Congress enacted a "long line" of privacy protection statutes, and "[i]n each instance, Congress has expanded and given meaning to the right of privacy."\(^\text{57}\) The VPPA incorporates principles established in these earlier statutes.\(^\text{58}\) Specifically, it places limitations on how information about how a person's video transaction data can be used and disclosed, and provides a way for consumers to participate in decisions concerning the use of their PII via opt-in and opt-out consent provisions.\(^\text{59}\)

However, as technology has evolved, the question of what constitutes PII has become more complex.\(^\text{60}\) Prior conceptions of PII have proven to be inadequate.\(^\text{61}\) As a result, it has become increasingly difficult to determine


\(^{53}\) See Gellman, supra note 49, at 10; see also S. REP. NO. 93-1183, at 6 (1974) (noting that the report of the Department of Health, Education & Welfare report was "[p]articularly supportive of the principles and purposes" of the Privacy Act).


\(^{58}\) See id.


\(^{60}\) See Schwartz & Solove, supra note 56, at 1841 (noting that innovative techniques employed by computer scientists can be used to make inferences of identity from non-PII, thereby transforming it to PII).

\(^{61}\) See id. at 1842, 1854–55 (noting that the increase in availability of personal data online enables easier identification of individuals by combining pieces of non-PII, and that online advertisers are able to skirt PII restrictions by building profiles of individuals using only non-PII, for use in behavioral targeting); see also discussion infra Section II.B (discussing several ways in which PII may be created or inferred from non-PII). This is hardly a new concern, however, given that Congress was aware of such techniques at the time the Privacy Act was enacted. See S. REP. NO. 93-1183, at 42 ("The Committee was presented with circumstantial evidence in Volume II of the 1971 President's Commission on Federal Statistics which indicates that it is possible, through sophisticated computerized techniques to estimate with reasonable accuracy personal information relating to identifiable individuals using multiple sources of statistical and nonstatistical information published by Federal and State agencies.").

341
whether a privacy violation has occurred, and the protections afforded by privacy regulations may be so eroded as to be ineffective. This raises the question of whether the current PII approach to privacy protection is adequate in the face of advances in technology. Thus, because a privacy violation is triggered under the VPPA only when PII is disclosed, an understanding of the concept, including its historical roots and modern challenges, is essential, particularly when the Statute is applied in an Internet context.

A. What Is Personally Identifiable Information?

From the beginning, privacy protection statutes like the VPPA have taken the approach that only PII is entitled to protection. Concerns about information privacy arose out of Orwellian fears of “Big Brother,” stemming from the computerization of government records that had started a decade earlier at the dawn of the information age. Computers were no longer the slow, mas-

---

62. See Ohm, supra note 48, at 1704–06 (arguing that because of the high success rate associated with drawing inferences of identity from non-PII, the idea that privacy can be protected by protecting only PII must be re-examined).

63. See discussion infra Section II.B. Some scholars have argued that the PII approach should be retained in some form, and have advanced proposals for evolving the concept of PII to address the current challenges. See Schwartz & Solove, supra note 56. Other scholars have argued that the current approach to privacy regulation should be abandoned. See Ohm, supra note 48; Helen Nissenbaum, Privacy as Contextual Integrity, 79 WASH. L. REV. 119 (2004); see also Yuen Yi Chung, Goodbye PII: Contextual Regulations for Online Behavioral Targeting, 14 J. HIGH TECH. L. 413 (2014).

64. See discussion infra Sections II.A–B.

65. See Ohm, supra note 48, at 1733–35 (discussing the evolution of privacy law from its beginning in tort law to the advent of PII and statutory privacy harm prevention); Schwartz & Solove, supra note 56, at 1819–28 (discussing the development of PII from the enactment of the Fair Credit Reporting Act through the enactment of the Cable Communications Policy Act and its aftermath).

66. Privacy: The Collection, Use, and Computerization of Personal Data, Hearing on S. 3418, S. 3633, S. 3116, S. 2810, and S. 2542 Before the Ad Hoc Subcomm. on Privacy and Info. Sys. of the S. Comm. on Government Operations and the Subcomm. on Constitutional Rights of the S. Comm. on the Judiciary, 93d Cong. 7 (2d Sess. 1974) [hereinafter Privacy Act Hearings] (statement of Sen. Abraham Ribicoff, Member, S. Comm. on Gov’t Operations & Ad Hoc Subcomm. on Privacy and Info. Sys. and Privacy) (“[I]nvestigations have unearthed a situation where we find computerized data on practically every person in this country. It is clear that effective legislative action is needed if we are to avoid having Big Brother watching over all of us.”). But see Comm. on Gov’t Operations, 93d Cong., LEGIS. HISTORY OF THE PRIVACY ACT OF 1974; S. 3418 (PUBL. L. 93-579) 843 (J. Comm. Print 1976) [hereinafter LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974] (statement of Sen. Walter D. Huddleston, Member, Comm. on Gov’t Operations) (noting that not all uses of personal information are “sinister,” and emphasizing a need to balance the individual’s privacy interest in per-
sive machines that consumed entire rooms, but had become relatively compact, affordable, and sophisticated.\textsuperscript{57} They were becoming more prevalent, not only in government but also in private industry.\textsuperscript{58} Additionally, computers were being networked together, presenting enormous possibilities for combining data from different sources.\textsuperscript{69} Against this backdrop, Senator Erwin stated in his opening remarks to the Ad Hoc Subcommittee on Privacy and Information Systems:

\begin{quote}
[As] each new data bank is created and each additional bit of personal information is recorded, that precious sphere of privacy on which an individual can do as [that individual] pleases without outside interference is slowly but surely whittled away. . . . [T]echnological advances have made it possible for more institutions to gather, store, and use more information about all of us.
\end{quote}

\ldots

. . . Once collected and computerized, personal data about an individual is virtually out of that individual’s control. The data takes on a life of its own as a part of a file, a dossier, a data bank, or an information system.\textsuperscript{70}

Indeed, the primary purpose of the Privacy Act was to provide the individual data subject with greater control over personal data held in the govern-
ment’s databases by imposing conditions on disclosure of and access to records containing personal information.\textsuperscript{71} The Privacy Act’s definition of the records to be protected combined two distinct elements: the type of information to be protected and the identifying characteristics of the individual.\textsuperscript{72} Importantly, the Privacy Act distinguished between records containing PII and “statistical records,” which it defined as records that are used for “statistical research or reporting purposes only.”\textsuperscript{73} This distinction represents a practical compromise between individuals’ rights to control their personal information and the government’s interest in analyzing the data it has collected.\textsuperscript{74}

Subsequent privacy protection statutes set forth provisions specific to particular government agencies\textsuperscript{75} and non-government entities.\textsuperscript{76} With each new privacy protection provision, the protected personal information was tailored to the specific context.\textsuperscript{77} The Tax Reform Act of 1976, for example, defined “taxpayer identity” as consisting of “the name of a person with respect to whom a return is filed, his mailing address, his taxpayer identifying number . . . , or a combination thereof.”\textsuperscript{78} The VPPA defined PII to include “information which identifies a person as having requested or obtained specific video materials.”\textsuperscript{79} The Children’s Online Privacy Protection Act (COPPA) included in its definition of PII not only identifying elements such as name

\textsuperscript{71} See Privacy Act § 552a (b)-(d).
\textsuperscript{72} See id. § 552a(a)(4) (“The term ‘record’ means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.”).
\textsuperscript{73} Id. § 552a(a)(6).
\textsuperscript{74} See Privacy Act Hearings, supra note 66, at 124–25 (statement of Mr. Philip W. Buchen, Executive Director, Domestic Council Comm. on the Right to Privacy) (arguing that regulation of information in federal government databases should treat statistical records differently from records containing personal information, citing differences in the “degrees of data sensitivity” and “risks of possible abuse,” as well as fears of “becom[ing] bogged down in an administrative morass”).
\textsuperscript{77} See, e.g., Paul M. Schwartz & Daniel J. Solove, Reconciling Personal Information in the United States and European Union, 102 CAL. L. REV. 877, 887–88 (2014) (criticizing the lack of coherence and consistency in United States privacy law, both because the terminology used is inconsistent and because the scope of identifiable information is unique to each statute).
\textsuperscript{78} 26 U.S.C. § 6103(b)(6).
and e-mail address but also "any other identifier that the [Federal Trade] Commission [(FTC)] determines permits the physical or online contacting of a specific individual."  

The FTC's regulation included in its definition of PII:

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. 

Thus, what constitutes PII in one context may not be considered PII in a different context. 

B. Drawing Inferences of Identity from Non-PII

In the early 1970s, Congress acknowledged the possibility that personal information could be obtained "with reasonable accuracy" by combining non-PII from multiple sources using "sophisticated computerized techniques." Advances in technology and the development and growth of the Internet have contributed to a substantial increase in the ability of government and private parties to amass and access data about individuals. Through the emergence of "big data" analytics, which has been driven by a desire to gain timely insights from large scale databases, the ability to draw inferences of identity from non-PII has increased to such an extent as to disrupt much of existing

---

82. See Schwartz & Solove, supra note 77, at 888 ("The moment at which information becomes identifiable enough to fall within the scope of a particular law relies on how each information privacy statute specifically defines its particular concept of personal information.").
84. See Schwartz & Solove, supra note 56, at 1842 (noting that the widespread availability of large amounts of non-PII creates an increased ability to transform non-PII into PII).
85. See Next Generation Computing and Big Data Analytics: Hearing Before the Subcomm. on Research and the Subcomm. on Tech. of the H. Comm. on Sci., Space, and Tech., 113th Cong. 41 (2013) (statement of Dr. Farnam Jahanian, Assistant Director for the Computer and Information Science and Engineering Directorate, National Science Foundation) ("Insights and more accurate predictions from large and complex collections of data have important implications for the economy. Access to information is transforming traditional businesses and is creating opportunities in new markets. Further, Big Data is driving the creation of new IT products and services based on business intelligence and data analytics, and is boosting the productivity of firms that use it to make better decisions and identify new business trends.").
privacy law. Even without disclosure of what is traditionally recognized as PII, data scientists are often able to infer a data subject’s identity or use non-PII to construct complex profiles of individuals, including behavioral and predictive information about the data subject, from patterns occurring in non-PII.

The techniques for converting non-PII into PII generally fall into three categories, based on the type of analysis that is performed. First, non-PII in one dataset can be linked or merged with PII contained in another dataset, enabling an inference of the data subject’s identity. Second, non-PII alone can be used to learn the identity of the data subject. Third, non-PII from different sources can be combined and linked together using a common identifier, creating a highly detailed personal profile from which a data subject’s identity may be inferred.

86. See Ohm, supra note 48, at 1703, 1716 (noting that the growth of re-identification science over the past two decades has undermined the reliance on removal of PII to protect privacy).

87. See Kate Crawford & Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, 55 B.C. L. REV. 93, 94–95 (2014) (arguing that disclosure of predictive personal information drawn from non-PII may constitute a privacy violation). Retailers and marketers often employ predictive algorithms to suggest products or services that the data subject is likely to be interested in. See, e.g., Avi Goldfarb & Catherine E. Tucker, Economic and Business Dimensions: Online Advertising, Behavioral Targeting, and Privacy, COMM. ACM, May 2011, at 25, 26. Target, for instance, has employed an algorithm to predict from a customer’s individual purchases whether the customer is pregnant, and then uses this information in its marketing campaigns. Charles Duhigg, How Companies Learn Your Secrets, N.Y. TIMES MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/16/magazine/shopping-habits.html.

88. See Chung, supra note 63, at 428–29 (citing FED. TRADE COMM’N, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 22–23 (2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/085400behavadrreport.pdf) (hereinafter SELF-REGULATORY PRINCIPLES). The FTC has also suggested disclosure of non-PII may nevertheless reveal private information in situations involving use of one person’s computer by another person in the same household; however, that scenario is not within the purview of this Comment. See SELF-REGULATORY PRINCIPLES, supra, at 23. For an example of this scenario in the context of the VPPA, see Mollet v. Netflix, Inc., 795 F.3d 1062 (9th Cir. 2015) (holding that display of recently watched videos to third parties did not constitute a disclosure within the meaning of the VPPA, where those third parties—the subscriber’s friends, family, and guests—accessed Netflix on subscriber’s device with subscriber’s permission).

89. SELF-REGULATORY PRINCIPLES, supra note 88, at 22; see infra Part II.B.1.

90. SELF-REGULATORY PRINCIPLES, supra note 88, at 22; see infra Part II.B.2.

91. SELF-REGULATORY PRINCIPLES, supra note 88, at 22; see infra Part II.B.3.
1. Linking PII and Non-PII

Researchers have found that combinations of non-PII are often unique. These unique combinations of non-PII can be used to infer the identity of a data subject in anonymized data. For example, a voter registration list, which contains the name, address, ZIP code, birth date, and gender of each voter, can be used to identify patients in hospital-level data from which the patient names and addresses have been removed. A study of the characteristics of demographic information found that the combination of ZIP code, birth date, and gender was sufficient to uniquely identify 87% of the population in the United States.

Similarly, the characteristics of a web browser, such as the browser version, installed fonts and plugins, and operating system, can be used to uniquely identify a user and track the user’s activities across multiple websites. These browser fingerprints can be used to uniquely identify approximately 83.6% of users. Unlike cookies, which may be deleted or disabled by user preference settings, the uniqueness of a browser fingerprint is less easily managed. Even where changes in the user’s computing environment cause changes in the browser fingerprint, in most cases the new fingerprint

---


93. See Sweeney, supra note 92, at 2.

94. Id.

95. Id.

96. See Eckersley, supra note 92, at 2–4; Erik Larkin, Browser Fingerprints: A Big Privacy Threat, PC WORLD (Mar. 26, 2010, 6:00 PM), http://www.pcworld.com/article/192648/browser_fingerprints.html [https://perma.cc/ZYCS-KSRC]; see also Nick Nikiforakis & Güneş Acar, Browser Fingerprinting and the Online-Tracking Arms Race, IEEE SPECTRUM (Jul. 25 2014, 15:00 GMT), http://spectrum.ieee.org/computing/software/browser-fingerprinting-and-the-online-tracking-arms-race [https://perma.cc/4ESX-KXDE] (noting that since Eckersley’s study, supra note 92, significant advancements in browser fingerprinting have been made).

97. Eckersley, supra note 92, at 2, 8–9.

98. See Nikiforakis & Acar, supra note 96 (noting that although tools purporting to disguise a browser’s fingerprints are available, such tools provide no real ability to protect against even a “mildly accomplished fingerprinter” because of the numerous idiosyncrasies that inher in web browsers).
can be linked back to the correct user. Thus, ubiquitous online advertising networks are able to use browser fingerprints in the same manner they use cookies—to track user behavior over any sites in which their content is embedded. If the user has registered at one of those websites, then the browser fingerprint can be used to associate the user’s identifying information with collected behavioral tracking data.

2. Creating PII from Non-PII

Information that has not traditionally been considered PII may be combined to create PII or to infer a data subject’s identity. For example, when America Online (AOL) inadvertently released three months of user search query data in 2006, the identities of some AOL members who had performed the searches could be inferred, even though the member names and AOL account information had been removed to protect the searchers’ identities. The search queries themselves, however, were left intact. The released data included 21 million search queries by more than 650,000 AOL members. The New York Times pieced together the search queries of one of the data subjects and ultimately determined her identity and some intimate details of about her life.

99. See Eckersley, supra note 92, at 12 (noting that a simple algorithm correctly linked a changed fingerprint to the original fingerprint in sixty-five percent of the cases).
100. See Nikiforakis & Acar, supra note 96; see also infra Section II.B.3.
101. See infra text accompanying notes 103–10.
102. See infra notes 103–11 and accompanying text; see also Arvind Narayanan & Vitaly Shmatikov, Robust De-anonymization of Large Sparse Datasets, in PROC. IEEE SYMP. ON SECURITY & PRIVACY 111, 118, 122–23 (2008). Researchers conducted an analysis of the movie ratings provided by approximately 500,000 Netflix customers contained in a dataset that Netflix released to the public. Id. at 118. Although Netflix had removed its customers’ PII, researchers were able to correlate movie ratings in the Netflix dataset with the movie ratings on publicly available websites, including the Internet Movie Database. Id. at 122–23. Thus, the identity of two customers was inferred entirely from non-PII. Id. Moreover, this data enabled researchers to draw inferences about the likely religious and political beliefs of one of the customers. Id. at 123.
104. Id.
106. Barbaro & Zeller Jr., supra note 103; see also McCullagh, supra note 105 (compiling profiles
[S]earch by search, click by click, the identity of AOL user No. 4417749 became easier to discern. . . . It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends’ medical ailments[,] and loves her three dogs.\textsuperscript{107}

As the AOL search data demonstrate, a single Web search query viewed in isolation may not constitute PII, but when queries performed over the course of weeks or months are considered in the aggregate, a detailed profile of the data subject emerges.\textsuperscript{108} The issue presented by the aggregation of non-PII over time is akin to the “mosaic” theory about which the concurring justices in \textit{United States v. Jones} expressed support.\textsuperscript{109} There, Justice Sotomayor suggested that a person’s public movements, “recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on,” would violate a reasonable expectation of privacy.\textsuperscript{110} Thus, PII may be created from non-PII data sources, and a violation of privacy may result when such data are disclosed.\textsuperscript{111}

3. Linking Non-PII Using a Common Identifier

Identifiers that are common to two sets of data can be used to link the non-PII contained in one dataset to the PII contained in a second dataset, thereby revealing the identity of the data subject in a dataset containing only non-PII.\textsuperscript{112} Websites commonly employ Internet cookies to remember details about the current browsing session.\textsuperscript{113} These cookies contain identifiers that have been generated by the website for the purpose of associating multiple requests to the same user.\textsuperscript{114}

Because third-party advertising networks, social media websites, and website analytics services serve content to a host of first-party websites, third-party cookies can be used by such services to track user behavior, including...
page views, clicks, and other actions, across multiple websites.\footnote{See Andreas Kuehn, Cookies Versus Clams: Clashing Tracking Technologies and Online Privacy, 15 INFO, no. 6, 2013, at 21–22 (noting that third-party cookies, such as those used by Google, Facebook, and advertising networks, can be used to track user behavior across multiple websites).} Such tracking can be performed even if the user does not interact with the elements served by the advertising network, social media websites, or website analytics services.\footnote{See In re Facebook Internet Tracking Litig., 140 F. Supp. 3d 922, 926–27 (N.D. Cal. 2015) (describing the behavior of Facebook’s tracking cookies).} For example, a Facebook “like” button on news stories and other content on other websites enabled Facebook, as a third party, to gather information about the browsing habits of Facebook users, even when they were not actually logged in and using Facebook.\footnote{Id. at 928.} Facebook linked this behavioral information—not traditionally considered to be PII—to the user’s Facebook profile using identifiers stored in the cookies on the user’s computer.\footnote{See Kim-Mai Cutler, Amid Privacy Concerns, Apple Has Started Rejecting Apps That Access UDIDs, TECH CRUNCH (Mar. 24, 2012), https://techcrunch.com/2012/03/24/apple-udids/ [https://perma.cc/FRW8-CEHH]. Prior to March 2012, Apple devices allowed applications to access the unique device identifier (UDID), a unique identifier assigned to the device by the manufacturer that could not be changed or disabled by user preference. Id. In September 2012, Apple introduced a new identifier for advertisers (IDA), which gave users the ability to change the IDFA in the device’s privacy settings, while also providing advertisers with a way to track users. Jim Edwards, Apple Has Quietly Started Tracking iPhone Users Again, and It’s Tricky to Opt Out, BUSINESS INSIDER (Oct. 11, 2012, 9:00 AM), http://www.businessinsider.com/ifa-apples-iphone-tracking-in-ios-6-2012-10 [https://perma.cc/FP7B-726R]. In October 2013, Google announced a similar change to its Android operating system, whereby its “Android ID” (analogous to Apple’s UDID) would be replaced with a new “Advertising ID” (analogous to Apple’s IDFA). Greg Sterling, Google Replacing “Android ID” with “Advertising ID” Similar to Apple’s IDFA, MARKETING LAND (Oct. 31, 2013, 2:18 P.M.), http://marketingland.com/google-replacing-android-id-with-advertising-id-similar-to-apples-ida-63636 [https://perma.cc/M2NP-HWUH]. Although these changes represent attempts to balance consumer privacy interests against the economic value of consumer insights, the extent to which such measures enhance privacy may be limited by the ability to match these identifiers to PII using other non-PII. See supra Sections II.B.1–II.B.2.} Similarly, mobile device identifiers, which uniquely identify a mobile device, are commonly accessed and sent to websites via mobile applications installed on the mobile device.\footnote{See Kimberly Truong, Infographic: Users Weighed Down by Multiple Gadgets—Survey Reveals the Most Carried Devices, NAKED SECURITY (Mar. 14, 2013), https://nakedsecurity.sophos.com/2013/03/14/devices-wozniak-infographic/ [https://perma.cc/FJ6M-VEAR] (reporting that survey respondents carried an average 2.9 mobile devices around with them every day); see also PII in Context, PEPPERDINE LAW REVIEW.} Such identifiers are typically used to associate requests with a user, based on the assumption that a mobile device is primarily used by one person.\footnote{Id. at 928.} Thus, behavioral information collected by multiple
applications installed on the mobile device and sent to various third parties can be linked to the person’s profile by association with the device identifier, thereby creating “detailed dossiers.”

III. THE VPPA: CURRENT STATE OF THE LAW AND ITS DEVELOPMENT

The VPPA prohibits a “video tape service provider” from “knowingly disclosing . . . [PII] concerning any consumer of such provider,” unless one of six enumerated exceptions—including both an opt-in and an opt-out exception—applies. “[PII] includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.” Courts have construed this definition to require three elements: 1) information that identifies a person; 2) information that identifies “specific video materials;” and 3) a nexus between these two pieces of information. Applying these requirements to digital identifiers and other potentially identifying information in an Internet video context, courts have recognized that the VPPA’s definition is, at least, “amenable” to


123. See id. § 2710(b)(2). A full discussion of disclosures permitted by the VPPA is beyond the scope of this Comment. However, two exceptions are worth noting, because they have been used by courts to interpret the scope of PII. See, e.g., In re Vizio, Inc., Consumer Privacy Litig., 238 F. Supp. 3d 1204, 1224 (C.D. Cal. 2017). First, Subdivision 2710(b)(2)(B) states that a provider may disclose any PII, so long as the consumer has provided informed consent in advance (“opt in”). § 2710(b)(2)(B). By contrast, Subdivision 2710(b)(2)(D) allows a provider to disclose a consumer’s name and address (with no identification of video materials), but only if the consumer has not opted out of such a disclosure (“opt out”). Id. § 2710(b)(2)(D).

124. Id. § 2710(a)(3) (emphasis added).

a broad interpretation.\textsuperscript{126} However, courts disagree with respect to the meaning of the first element, concerning information that identifies a person.\textsuperscript{127}

At least four distinct interpretations of the definition's personal identification requirement have emerged since 2014, when the \textit{In re Hulu II} court first confronted the issue.\textsuperscript{128} In \textit{In re Hulu II}, the court held that an "anonymous" identifier, without more, does not identify a person.\textsuperscript{129} Drawing support from \textit{In re Hulu II}, the \textit{Ellis} court held that information identifies a person only if the person's identity can be ascertained from the disclosure itself, without any "further steps" being taken.\textsuperscript{130} Taking a broader view, however, the First Circuit in \textit{Yershov} held that the VPPA requires only that the information be "reasonably and foreseeably likely" to identify a person.\textsuperscript{131} Finally, the Third Circuit in \textit{In re Nickelodeon} held that information identifies a person only if the information would permit an "ordinary person" to make the identification.\textsuperscript{132} Underlying these differences of interpretation is a dispute concerning the extent to which context is relevant to the inquiry.\textsuperscript{133}

This dispute evolved from the VPPA's application to factual circumstances unanticipated at the time of its enactment,\textsuperscript{134} and it is most clearly exemplified in \textit{Yershov} and \textit{In re Nickelodeon}.\textsuperscript{135} Nevertheless, an examination of \textit{In re Hulu II} and its progeny, in addition to these circuit court decisions, is necessary for a full understanding of the interpretive range of the term PII.\textsuperscript{136}

\begin{thebibliography}{9}
\bibitem{126} See, e.g., \textit{In re Nickelodeon}, 827 F.3d at 285.
\bibitem{127} See infra notes 129–32 and accompanying text.
\bibitem{128} See discussion infra Sections III.B–D.
\bibitem{131} Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 486 (1st Cir. 2015).
\bibitem{132} \textit{In re Nickelodeon Consumer Privacy Litig.}, 827 F.3d 262, 290 (3d Cir. 2016), \textit{cert. denied}, 137 S. Ct. 624 (2017).
\bibitem{133} See infra notes 230–35 and accompanying text; infra Section IV.A.
\bibitem{134} See infra Section III.B; see also \textit{The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century; Hearing Before the Subcomm. on Privacy, Technology, and the Law of the S. Comm. on the Judiciary, 112th Cong. 15 (2012) [hereinafter VPPA 2012 Amendment Hearing] (statement of Mr. Christopher Wolf, Director, Privacy and Information Management Group, Hogan Lovells LLP) (“In 1988, when the VPPA was enacted, no one dreamed of streaming video and social sharing.”). Even as late as 1995, home entertainment commentators did not anticipate the extent to which the Internet would enable video-on-demand services to shake up an entire industry. See Nicole Winfield, \textit{Looking Beyond Blockbuster's Decade of Growth}, \textit{L.A. TIMES} (Dec. 5, 1995), http://articles.latimes.com/1995-12-05/business/fo-105911_1_blockbuster-video [https://perma.cc/T88Z-EUYE].
\bibitem{135} See infra Sections III.C–D.
\end{thebibliography}
Because a majority of courts have rested their interpretations on grounds of legislative intent, Section III.A begins with an examination of the VPPA's enactment in 1988 and amendment in 2013. 137 Section III.B traces the current state of the law through *In re Hulu II* and its progeny. 138 Sections III.C and III.D examine the decisions of the circuit courts in *Yershov* and *In re Nickelodeon*, respectively. 139

A. Congressional Intent

The VPPA was enacted in response to the publication in a weekly Washington, D.C. tabloid, of information about films that Judge Robert Bork had rented from a local video store. 140 This public disclosure occurred amid a heated debate in the United States Senate over Judge Bork's nomination to the Supreme Court. 141 The video store disclosed the list of 146 films in response to reporter Michael Dolan's request. 142 Although the list was innocuous—consisting of British costume dramas, Alfred Hitchcock films, mysteries, and the like—the disclosure was met with widespread condemnation. 143

---

137. See infra Section III.A.
138. See infra Section III.B.
139. See infra Sections III.C-D.
140. S. REP. NO. 100-599, at 5 (1988); see Michael Dolan, *The Bork Tapes*, WASH. CITY PAPER, Sept. 25–Oct. 1, 1987, at 1, 16 (describing Judge Bork's film preferences, including mysteries and a "preference for British costume dramas"). Although the disclosure of Judge Bork's videotapes was widely discussed due to Judge Bork's high profile and the story's coincidence with the Senate hearings on his nomination to the Supreme Court, it was not the only instance of such an intrusion. See S. REP. NO. 100-599, at 6. There were also reports of at least two instances involving attempts by government agencies to obtain the video rental records of consumers, and an attempt by a private party for use in divorce proceedings. *Video Privacy Protection Act of 1988: J. Hearing on H.R. 4947 and S. 2361 Before the S. Judiciary Subcomm. on Technology and the Law and the H. Judiciary Subcomm. on Courts, Civil Liberties, and the Administration of Justice*, 100th Cong. 77 (1988) [hereinafter Joint Hearing on H.R. 4947 and S. 2361] (statement of Vans Stevenson, Director of Public Relations, Erol's Inc.).
141. S. REP. NO. 100-599, at 5.
142. Dolan, supra note 140, at 14.
143. See, e.g., Joint Hearing on H.R. 4947 and S. 2361, supra note 140, at 10 (statement of Rep. Alfred McCandless) ("Books and films are the intellectual vitamins that fuel the growth of individual thought... This intimate process should be protected from the disruptive intrusion of a roving public eye."); Dolan, supra note 140, at 14, 16.
The legislative history of the VPPA indicates that there was a broad concern about the impact that disclosures of First Amendment materials could have on intellectual freedom and growth. Additionally, there is some indication that Congress was concerned about disclosure of video viewing activities extending beyond video clerks leaking information about customer rentals to the press, including concerns about how disclosure of such information might be accumulated and used by direct marketers in ways that could not necessarily be anticipated. Moreover, the VPPA’s definition of PII suggests an intent to provide broad protection of personal information in connection with a person’s video selections. The definition used the word includes, suggesting that Congress intended PII to mean more than simply a name. Finally, the Statute incorporates some of the same foundational principles established by the Privacy Act, including the concept of PII and the directive that “information collected for one purpose may not be used for a different purpose without the individual’s consent.” Thus, “Congress’s intent . . . evinces the principle that protection is merited when the consumer lacks control over the dissemination of the information at issue.”

144. See S. REP. NO. 100-599, at 4 (“Protecting an individual’s choice of books and films is a second pillar of intellectual freedom under the first amendment.”).
145. See, e.g., Joint Hearing on H.R. 4947 and S. 2361, supra note 140, at 115–16 (statement of Sen. Patrick J. Leahy, Chairman, Subcomm. on Technology and the Law of the S. Comm. on the Judiciary) (“I have this vision of big brother, where somebody sits at a massive computer—somebody whom I have never seen, never will meet in my life—but that person can kind of figure out that Patrick Leahy is this sort of person based on . . . what he views and, therefore, he gets pegged a certain way and we are now going to bring whatever the marketing tools are available against him.”).
146. See infra notes 147–48 and accompanying text. Notwithstanding the VPPA’s open-ended definition, courts have interpreted the definition of PII narrowly, often defining it as information “without more” that identifies a person as having accessed a video. See infra Section III.B.
147. Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(a)(3) (2012); see S. REP. NO. 100-599, at 12 (“Unlike the other definitions in this subsection, paragraph (a)(3) uses the word ‘includes’ to establish a minimum, but not exclusive, definition of personally identifiable information.”).
148. See S. REP. NO. 100-599, at 2–4, 8 (recounting the history of privacy protection laws, and placing the VPPA within that context); Joint Hearing on H.R. 4947 and S. 2361, supra note 140, at 54 (statement of Ms. Janlori Goldman, Staff Attorney, Project on Privacy and Technology, American Civil Liberties Union); see also notes 46–56 and accompanying text (discussing the evolution of the FIPs).
1. The 1988 Enactment

Following the publication of Judge Bork’s video list, three bills—H.R. 3523, H.R. 4947, and S. 2361—were introduced in Congress with the stated purpose of preserving personal privacy with respect to video materials.\(^ {150} \) Although both H.R. 3523 and H.R. 4947 ultimately failed, a brief examination of these bills in relation to the enacted legislation may provide an indication of the intended scope of the Act’s definition of PII.\(^ {151} \) Notably, the bills differ with respect to the scope of personal information to be protected.\(^ {152} \)

The earliest of these bills, H.R. 3523, would have provided the least protection of consumers’ video rental and purchase information.\(^ {153} \) Representative McCandless introduced H.R. 3523 on October 21, 1987, less than a month after the publication of Judge Bork’s video list,\(^ {154} \) and the language of the bill is closely aligned with the circumstances of that disclosure.\(^ {155} \) Significantly, the bill does not use the term PII, but instead prohibits wrongful disclosure of “the identity of the [video] tapes [rented or sold] to individuals for home use” along with the identity of the individual who rented or purchased those

\(^{150}\) See H.R. 4947, 100th Cong. (2d Sess. 1988); S. 2361, 100th Cong. (2d Sess. 1988) (enacted); H.R. 3523, 100th Cong. (1st Sess. 1987). Both H.R. 4947 and S. 2361, as introduced, would have prohibited libraries from disclosing their patron’s PII, including the titles of books requested or borrowed. See S. 2361 (as introduced in the Senate, May 10, 1988); H.R. 4947 (as introduced in the House, June 29, 1988). However, the library provision was removed from S. 2361 prior to its enactment, due to unresolved questions concerning its applicability to law enforcement. S. REP. NO. 100-599, at 8.

\(^{151}\) See United States v. Enmons, 410 U.S. 396, 404 n.14 (1973) (noting that an unenacted bill’s legislative history is “wholly relevant to an understanding of” a subsequently enacted statute that contains the same operative language); United States v. Johnson, 632 F.3d 912, 925 n.71 (5th Cir. 2011) (“Unenacted bills have limited persuasive value, but they do provide an insight into the evolution of the language that became the final statute.”). But see United States v. Laton, 352 F.3d 286, 314 (6th Cir. 2003) (“The Supreme Court has frequently rejected arguments based on unenacted legislation, noting the difficulty of determining whether a prior bill prompted objections because it went too far or not far enough.”) (citing Mead Corp. v. Tilley, 490 U.S. 714, 723 (1989)).

\(^{152}\) See infra notes 153–69 and accompanying text. Additional substantial differences among the proposed bills, including what constitutes a “wrongful disclosure,” the enumeration of circumstances in which disclosure would be permissible, and the availability of any civil remedy, may inform a discussion of Congress’s recognition of countervailing interests. See H.R. 4947; S. 2361; H.R. 3523; infra notes 163, 174. However, a full discussion of these differences is beyond the scope of this Comment.

\(^{153}\) See infra notes 155–58 and accompanying text (discussing the scope of personal information protected).

\(^{154}\) See 133 Cong. Rec. 28,619 (introducing H.R. 3523); Dolan, supra note 140, at 1.

\(^{155}\) See H.R. 3523 § 2(a)(2); infra text accompanying note 156; see also 133 Cong. Rec. 35,649 (statement of Rep. McCandless) (urging support for H.R. 3523 and suggesting that it would prohibit disclosures in circumstances similar to the disclosure of Judge Bork’s “video list”).
tapes.” 156 Thus, H.R. 3523 would have preserved a privacy interest in a very narrow band of information: the consumer’s actual identity (i.e., a name) and the identity (i.e., the titles) of the videos purchased or rented. 157 In other words, H.R. 3523 likely would not have prohibited the disclosure of information that indirectly identified a person and the person’s video tape transactions. 158

By contrast, H.R. 4947 would have provided much broader protection of consumer privacy. 159 H.R. 4947 was introduced by Representative Kastenmeier on behalf of himself and Representative McCandless, on June 29, 1988. 160 As introduced, H.R. 4947 would have prohibited “a video service provider or library knowingly . . . to disclose to any other person or entity any

156. H.R. 3523 § 2(a)(2) (emphasis added). H.R. 3523 defined wrongful disclosure as including “a disclosure that occurs in circumstances in which the individual who rented or purchased the video tapes involved has a reasonable expectation of privacy.” Id. (emphasis added). Interestingly, H.R. 3523 is the only one of the three bills to frame the prohibited conduct in terms of a reasonable expectation of privacy, and neither H.R. 4947 nor S. 2361 contemplates the circumstances of the disclosure. See H.R. 4947; S. 2361. Thus, if the disclosure of Judge Bork’s video list had been disclosed to law enforcement, then a court applying H.R. 3523’s provisions would likely have held that Judge Bork had no reasonable expectation of privacy: the video store clerk knew which videos Judge Bork rented, and Judge Bork, therefore, assumed the risk that the clerk might reveal this information to the government. See, e.g., Smith v. Maryland, 442 U.S. 735 (1979) (holding that there is no reasonable expectation of privacy in the phone numbers dialed on a telephone, given the phone company’s knowledge of that information, which it used to route the call). As enacted, however, the VPPA imposes a higher standard. See Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(b)(2)(C) (2012) (setting forth an exception to the general prohibition on disclosure of PII, for the disclosure “to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order”); Dirkes v. Borough of Rumene, 936 F. Supp. 235 (D.N.J. 1996) (finding that a video store violated the VPPA when it disclosed a customer’s video rental transactions to a law enforcement officer who had obtained neither a warrant, a subpoena, nor a court order).

157. See H.R. 3523 § 2(a)(2).

158. See id. Despite Congress’s apparent rejection of such a narrowly prescribed protection of an individual’s video transaction information, several courts have interpreted the VPPA’s definition of PII to require something akin to an individual’s identity. See, e.g., Ellis v. Cartoon Network, Inc., No. 1:14-CV-484-JWT, 2014 WL 5023535, at *3 (N.D. Ga. Oct. 8, 2014) (holding that information requiring a third party to take “extra steps” to identify an individual is not PII within the meaning of the VPPA), aff’d on other grounds, 803 F.3d 1251 (11th Cir. 2015); see also discussion infra Section III.B.

159. See infra notes 161–65 and accompanying text.

[PII] about any user of covered services."\(^{161}\) Although the bill did not define the term PII, the use of the word any suggests that PII included much more than an individual’s name.\(^{162}\) H.R. 4947’s opt-out provision, which severely limited the type of information that providers would be permitted to disclose, provides additional confirmation of an intention to provide broad protection of information about an individual.\(^{163}\) Moreover, as introduced, H.R. 4947 contained no express requirement that the information be disclosed in combination with specific personal information.\(^{164}\) Thus, at least for H.R. 4947, the meaning of PII was broad enough to encompass any information capable of identifying a consumer.\(^{165}\)

With respect to its definition of PII, S. 2361 may be seen as occupying the middle ground between the approaches taken in H.R. 3523 and H.R. 4947.\(^{166}\) Similar to H.R. 3523, the Senate bill’s prohibition on disclosure was expressly limited to the combination of information identifying both the individual and the videos ‘requested or obtained.’\(^{167}\) Like H.R. 4947, however, S. 2361 used the term PII, which it defined as a minimum, nonexclusive standard.\(^{168}\) Exactly how broadly the definition was intended to be applied, however, is unclear.\(^{169}\)


163. See H.R. 4947 § 2(a)(2). H.R. 4947’s opt-out provision made it permissible for a provider to disclose information “limited to the name and address of the user, that does not, directly or indirectly, reveal the category of service, or the title, description, or subject matter of service used.” Id. The Senate bill, S. 2361, included identical language when that bill was introduced, but the restrictions were significantly loosened in committee. See infra note 174 and accompanying text.

164. See H.R. 4947 § 2(a)(2).

165. See supra notes 160–64 and accompanying text.

166. See infra notes 167–69 and accompanying text.

167. See S. 2361 § 2(a)(2) (as introduced in the Senate, May 10, 1988) (“[T]he term [PII] includes information which identifies a person as having requested or obtained specific materials or services from a video tape service provider or library.”); S. REP NO. 100-599, at 12 (“This definition makes clear that 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.”). Apart from the removal of the reference to library materials or services, there was no change to this definition at its enactment. See Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(a)(3) (2012).

168. See S. 2361 § 2(a)(2); S. REP. NO. 100-599, at 12 (“[P]aragraph (a)(3) uses the word ‘includes’ to establish a minimum, but not exclusive, definition of personally identifiable information.”).

169. See discussion infra Sections III.B–D.
Nevertheless, the legislative history of S. 2361 suggests an intention to protect consumer video privacy in circumstances extending well beyond those involved in the disclosure of Judge Bork’s video rental history.\textsuperscript{170} For example, Representative McCandless suggested that the Act’s privacy protections would extend to “any distribution” of video materials.\textsuperscript{171} Similarly, Senator Leahy, the bill’s author, expressed concerns about the accumulation of personal information, including the subject matter and titles of videos a person has watched, in the hands of marketers and advertisers.\textsuperscript{172} At the same time, however, the legislative history also shows a willingness to accommodate commercial interests to the extent consistent with the statute’s purpose.\textsuperscript{173} For example, the bill’s opt-out provision underwent substantial amendment in committee, with the result being that video service providers were allowed to disclose more information unless a consumer had opted out of such a disclosure.\textsuperscript{174} Thus, although the disclosure of Judge Bork’s video list may have provided the impetus for the enactment of the VPPA, the statute represents Congress’s measured response to what it perceived as a serious, growing threat to freedoms protected by the First Amendment.\textsuperscript{175}

\textsuperscript{170} See infra notes 171–75 and accompanying text. Indeed, had Congress intended to limit the Act to disclosure of customer names and video titles only, it could have crafted a definition that more closely resembled the language of H.R. 3523. See supra notes 153–58 and accompanying text.

\textsuperscript{171} See Joint Hearing on H.R. 4947 and S. 2361, supra note 140, at 31 (statement of Rep. McCandless).

\textsuperscript{172} See id. at 115–16 (statement of Sen. Leahy, Member, Comm. on the Judiciary).

\textsuperscript{173} S. Rep. No. 100-599, at 12–15 (analyzing the provisions of S. 2361 permitting disclosure of PI, with reference to the practices and concerns of video service providers).

\textsuperscript{174} Compare S. 2361 (as introduced in the Senate, May 10, 1988) with S. 2361 (as reported by S. Comm. on the Judiciary, Oct. 21, 1988). At S. 2361’s introduction, Section 2710(b)(2)(D)(ii) restricted the information that a provider could disclose pursuant to the opt-out provision, prohibiting such a disclosure that would “reveal, directly or indirectly, the title, description, or subject matter of any video tapes or other audio visual material.” S. 2361 (as introduced in the Senate, May 10, 1988) (emphasis added). However, the committee amended the bill to allow video providers to disclose more information unless the consumer opted out of such disclosure. See S. 2361 (as reported by S. Comm. on the Judiciary, Oct. 21, 1988). Specifically, the amended version restricted disclosures pursuant to the opt-out provision, prohibiting only such a disclosure that “identifies [the] title, description, or subject matter of any video tapes or other audio visual material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer.” See id. (emphasis added).

\textsuperscript{175} See supra notes 170–73 and accompanying text.
2. The 2013 Amendment

Recognizing a need to "modernize" the VPPA "to keep up with today's technology and the consumer marketplace,"176 Congress amended the Act in 2013.177 Despite widespread changes in technology, including the advent of Internet video streaming technology, the actual amendment was "narrowly crafted" to update only the VPPA's opt-in provision.178 The amendment made it permissible for a video provider to obtain—via the Internet—a consumer's informed consent to the disclosure of PII.179 Given the disparity between the widespread changes in technology and the narrowly-tailored amendment, some courts have interpreted Congress's decision to leave the definition of PII untouched as a clue to understanding the term's application in the Internet context.180

177. Video Privacy Protection Act Amendments Act of 2012, H.R. 6671, 112th Cong. (2d Sess. 2012). Two bills—H.R. 2471 and H.R. 6671—were introduced in the House of Representatives during the enactment process. H.R. 2471, introduced July 8, 2011, was passed in the House by a two-thirds vote over the objections of Representative Melvin Watt, who objected to passage of the bill in the absence of hearings and without full debate. See 157 Cong. Rec. H8161–65, H8169 (2011) (statement of Rep. Melvin Watt) (urging defeat of the bill on suspension). The bill subsequently failed in the Senate, after Senator Leahy included an amendment to the Electronic Communications Privacy Act (ECPA). See S. Rep. No. 112-556, at 6–8 (summarizing the changes to H.R. 2471 in the Senate Committee on the Judiciary). Ultimately, the ECPA provisions were dropped, and the VPPA amendment was reintroduced as H.R. 6671. See H.R. 6671 (enacted). This bill was passed by both chambers in the latter part of December 2012 and signed into law by President Obama on January 10, 2013. Id.
178. See H.R. 6671 (enacted); 158 Cong. Rec. H6850 (Dec. 18, 2012) (statement of Rep. Goodlatte) ("[H.R. 6671] is narrowly crafted to preserve the VPPA’s protections for consumers' privacy, while modernizing the law to empower consumers to do more with their video consumption preferences, including sharing names of new or favorite TV shows or movies on social media in a simpler way."). From its initial introduction, the amendment was simply a wholesale replacement of subsection (b)(2)(B), the Statute's informed consent (opt-in) provision, with no other changes to the Statute. See H.R. 6671; H.R. 2471.
The initial effort to amend the VPPA began in July 2011. But neither at that time, nor at any time prior to President Obama’s approval of the amendment in 2013, had any court applied the VPPA in an Internet streaming video context. As a result, Congress could be seen as neither acting to correct a misapplication of the law, nor ratifying an interpretation with which it agreed. Moreover, despite calls to strengthen the VPPA’s privacy protections, Congress’s decision to update only the Act’s opt-in provision does not signal an intent to restrain the scope of its protections or of the term PII. To the contrary, the amendment reflects Congress’s continuing intent for the

181. See supra note 177.

182. See infra Section III.B. Although several VPPA issues were decided in In re Hulu I in 2012, the court did not examine the PII issue until April 2014, over a year after the VPPA had been amended. See In re Hulu II, No. C 11-03764 LB, 2014 WL 1724344, at *7–9 (N.D. Cal. Apr. 28, 2014); In re Hulu I, No. C 11-03764 LB, 2012 WL 3282960, at *4–8 (N.D. Cal. Aug. 10, 2012).

183. Cf. Apex Hosiery Co. v. Leader, 310 U.S. 469, 486 (1940) (“The long time failure of Congress to alter the [law] after it had been judicially construed, and the enactment by Congress of legislation which implicitly recognizes the judicial construction as effective, is persuasive of legislative recognition that the judicial construction is the correct one.”). But cf. Jones v. Liberty Glass Co., 332 U.S. 524, 534 (1947) (“We do not expect Congress to make an affirmative move every time a lower court indulges in an erroneous interpretation. In short, the original legislative language speaks louder than such judicial action.”).

184. See, e.g., VPPA 2012 Amendment Hearing, supra note 134, at 3 (statement of Sen. Al Franken, Chairman, Subcomm. on Privacy, Technology, and the Law) (expressing concern about the “real risk” that a judge might interpret the VPPA to apply to video tapes and DVDs, but not to movies streamed over the Internet, and calling for a “fair and comprehensive update of the entirety of this law”). See VPPA 2012 Amendment Hearing, supra note 134, at 19 (statement of Mr. Marc Rothenberg, Executive Director, Electronic Information Privacy Center) (suggesting that the law needed be strengthened in light of the increased amount of data collection associated with Internet video streaming). Mr. Rothenberg’s prepared statement proposed an amendment to the definition of PII, to make clear that it included, but was not limited to, “Internet Protocol (IP) addresses and account identifiers.” Id. at 60. Congress took no action with regard to Mr. Rothenberg’s proposal. See generally VPPA 2012 Amendment Hearing, supra note 134.

185. See supra note 184; cf. Fox v. Standard Oil Co. of N.J., 294 U.S. 87, 96–97 (1935) (holding that rejection of a proposed amendment to a bill is not conclusive of Congressional intent, but “a circumstance to be weighed along with others when choice is nicely balanced”). In Fox, the Supreme Court considered the effect of a rejected amendment to a bill prior to its enactment, which would have limited the definition of the term store to exclude “filling stations.” Fox, 294 U.S. at 95–96. In holding that Congress intended not to exclude “filling stations” from the definition, however, the Court stressed the importance of extrinsic tokens in addition to the rejected amendment. Id. at 96. By contrast to Fox, where a proposed amendment to a bill had been put to a vote and rejected, id., here, Congress never put Mr. Rothenberg’s proposed amendment to a vote, supra note 184. Moreover, unlike Fox, where contemporaneous interpretation by the state tax commissioner was also a factor, Fox, 294 U.S. at 96–97, here, there had been no interpretation of PII in the context of Internet streaming video, see supra note 182.
VPRA to be “a protection for consumers, not a punishment on the industry.” 186 There is evidence, for example, that the law had impeded the innovation of video service providers, particularly with respect to integrating their services with social networking websites. 187 As the “main proponent” of the amendment, Netflix, Inc. (Netflix) engaged in a public campaign to bring about its enactment. 188 Netflix’s chief complaint with the law was that its written consent (opt-in) provision precluded companies like Netflix from offering their customers the ability to share information about the movies they watched with their friends on Facebook. 189 The amendment specifically addressed these concerns by clarifying that a consumer’s consent to the disclosure of PII may be given via the Internet, rather than “in writing.” 190 Thus, given the narrow scope of the amendment in combination with the absence of an affirmative action relating to the VPRA’s definition of PII, the amendment’s legislative history is unhelpful to an inquiry into the limits of that term. 191

B. In re Hulu II and Its Progeny

In re Hulu II marks the first time a district court applied the VPRA to the Internet streaming video context involving disclosure of a viewer’s unique

---


189. See supra note 187.


191. See Alexander v. Sandowal, 532 U.S. 275, 292 (2001) (“[W]hen . . . Congress has not comprehensively revised a statutory scheme but has made only isolated amendments ‘it is impossible to assert with any degree of assurance that congressional failure to act represents’ affirmative congressional approval of the Court’s statutory interpretation.” (quoting Patterson v. McLean Credit Union, 491 U.S. 164, 175 n.1 (1989)).
digital identifiers. There, viewers of Hulu’s online video content brought a putative class action, alleging that Hulu acted in violation of the VPPA when it disclosed information about the videos they had watched to third parties—comScore, an online marketing analytics company, and Facebook, a popular social media website. At issue were three different pieces of information—the browser fingerprint that comScore used to track behavior of unidentified individuals (“comScore User ID”), the unique identifier Hulu generated and used to identify its own registered users (“Hulu User ID”), and the unique identifier that Facebook stored in a cookie to track its own users (“Facebook User ID”)—which Hulu transmitted along with the titles of videos its users watched.

The court interpreted the VPPA’s text and legislative history to mean that PII “identifies a specific person and ties that person to particular videos that

192. See In re Hulu II, No. C 11–03764 LB, 2014 WL 1724344, at *9 (N.D. Cal. Apr. 28, 2014) (“No case has addressed directly the issues raised by Plaintiffs: the disclosure of their unique identifiers and the videos they are watching.”). In an earlier opinion in the same case, the court also interpreted the VPPA’s definitions of consumer and video tape service provider. See In re Hulu I, No. C 11–03764 LB, 2012 WL 3282960, at *4–6, 7–8 (N.D. Cal. Aug. 10, 2012). The court subsequently interpreted the VPPA’s prohibition on disclosure to require that a video service provider have actual knowledge that it was disclosing PII. See In re Hulu III, 86 F. Supp. 3d 1090 (2015). The court’s opinions in this case have had a profound impact on virtually every aspect of the privacy protections afforded to consumers’ online video viewing activities under the VPPA, but full discussion of this impact is beyond the scope of this Comment. For a brief overview of the issues addressed in the In re Hulu I–III decisions, see Chris King, Case Summaries, Three Years of Change: Recent Court Cases Under the Video Privacy Protection Act, 26 DEPAUL J. ART TECH. & INTELL. PROP. L. 135 (2016).


194. See id. at *4 (“The comScore UID . . . identifies the specific copy of the web browser.”); see also notes 96–101 and accompanying text (discussing the characteristics of browser fingerprints). That comScore did not know the identities of the users it tracked is suggested by the allegation that it was able to learn the identities of those users through an association with the Hulu User ID. See In re Hulu II, 2014 WL 1724344, at *4; infra note 195. Thus, although comScore’s practice was to track users across multiple websites, there was apparently no allegation that it possessed information that would have enabled it to identify the tracked users without additional information supplied by Hulu. See In re Hulu II, 2014 WL 1724344, at *4.

195. In re Hulu II, 2014 WL 1724344, at *2. “Hulu assigned each new registered Hulu user a ‘User ID,’ which is a unique numerical identifier of at least seven digits.” Id.

196. Id. at *5. The Facebook cookies contained two values that Facebook could use to identify its users, whether or not the user was currently logged in to Facebook. Id. Specifically, the “lu” (last user) cookie identifies the Facebook user who last logged into Facebook using the browser, and the “c user” (current user) cookie identifies the Facebook user who is currently logged in to Facebook. Id.

197. Id. at *3–5.
the person watched.”

First, the court recognized that “unique anonymous [identifiers] do not necessarily identify people.” Second, the court observed that “[PII] requires more than a unique anonymous [identifier].” Finally, the court distinguished situations involving disclosure of unique identifiers “without more” from such a disclosure “to a person who could understand it.” Importantly,

198. Id. at *8. In In re Hulu III, the court reformulated this definition, stating it as comprising three distinct elements: “1) a consumer’s identity; 2) the identity of ‘specific video materials; and 3) the fact that the person identified ‘requested or obtained’ these materials.” In re Hulu III, 86 F. Supp. 3d 1090, 1095 (N.D. Cal. 2015); see supra note 125.

199. See In re Hulu II, 2014 WL 1724344, at *9–11. Throughout its opinion, the court uses the term “anonymous identifier” to refer to unique digital identifiers such as mobile device identifiers, user identification numbers, and other types of digital information. See id. However, as the district court in Yershov noted, “relying on these identifiers as ‘anonymous identifiers’ . . . is unhelpful and possibly misleading.” Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 146 (D. Mass. 2015), rev’d on other grounds, 820 F.3d 482 (1st Cir. 2016). For example, a social security number, standing alone, is anonymous, but “it would be absurd to conclude that a social security number is not PII.” Id.

200. In re Hulu II, 2014 WL 1724344, at *9–10 (citing Viacom Int’l, Inc. v. YouTube Inc., 253 F.R.D. 256 (S.D.N.Y. 2008)). In Viacom, a copyright infringement action, the court granted the plaintiff’s motion to compel YouTube to produce all data from its logging database relating to the viewing of videos by its users. YouTube, 253 F.R.D. at 262. The issue was whether there was a sufficient privacy interest in the YouTube login identifiers (Login IDs) contained in the logging database to bar discovery. Id. Importantly, the court found, based on agreement between the parties, that the “login ID is an anonymous pseudonym that users create for themselves when they sign up with YouTube which without more cannot identify specific individuals.” Id.

201. In re Hulu II, 2014 WL 1724344, at *10 (examining Lahr v. NTSB, 453 F. Supp. 2d 1153 (C.D. Cal. 2006), rev’d in part on other grounds, 569 F.3d 964 (9th Cir. 2009)). Lahr was a Freedom of Information Act case, in which plaintiffs sought information that the government had withheld concerning its investigation into the explosion of a commercial aircraft. Lahr, 453 F. Supp. 2d at 1161–63. Specifically, the plaintiffs sought eyewitness identification numbers that had been redacted. Id. at 1182. In holding that the defendants lacked a sufficient privacy interest in the eyewitness identification numbers, the court stressed that defendants could not demonstrate how these numbers by themselves “could provide access to [the witnesses] or any personally identifying information about them.” Id. at 1183.

202. In re Hulu II, 2014 WL 1724344, at *11 (examining Pruitt v. Comcast Cable Holdings, 100 F. App’x 713 (10th Cir. 2004)). Other courts have also relied in part on Pruitt in holding that digital identifiers were not PII. See Robinson v. Disney Online, 152 F. Supp. 3d 176, 183 (S.D.N.Y. 2015); Eichenberger v. ESPN, Inc., No. C14–463 TSZ, 2015 WL 7252985, at *3 (W.D. Wash. May 7, 2015), aff’d, 876 F.3d 979 (9th Cir. 2017); Ellis v. Cartoon Network, Inc., No. 1:14–CV–484–TWT, 2014 WL 5023535, at *3 n.39 (N.D. Ga. Oct. 8, 2014), aff’d on other grounds, 803 F.3d 1251 (11th Cir. 2015). In Pruitt, the Tenth Circuit held that pay-per-view purchase history information stored in a set-top cable box did not constitute PII within the meaning of the Cable Communications Policy Act (Cable Act). 100 F. App’x at 717. Under the Cable Act, PII was defined to exclude information.
the court noted that whereas the latter might constitute PII, the former would not. In other words, the Statute required “something akin to [a name].”

Applying these principles, the court found no indication that the comScore User ID revealed the identity of the person who watched a video. Although the court acknowledged that comScore used this identifier to amass “as much evidence as it [could] about what webpages Hulu users visit,” it was significant that comScore did so without knowing the identity of the users it tracked. Thus, the court held that because the comScore User ID did not reveal the identities of the Hulu users it tracked, it did not fall within the meaning of PII under the Statute.

Similarly, the court found that Hulu did not disclose PII when it transmitted the Hulu User ID in combination with a person’s video viewing activities. Unlike the comScore User IDs, which comScore used to track unidentified users, the Hulu User IDs identified registered Hulu users. Anyone in possession of a person’s Hulu User ID was able to access the person’s profile

“which does not identify particular persons.” 47 U.S.C. § 551(a)(2)(A) (2012). The issue was whether the cable company retained PII longer than permitted by failing to delete the information when the set-top-boxes were redistributed to other customers. Pruitt, 100 F. App’x at 716; see 47 U.S.C. § 551(e). Importantly, identifying a consumer based on the codes contained in the set-top-box was not possible without access to information in the company’s billing system (i.e., “without more”), because the codes by themselves “provide(d) nothing but a series of numbers.” Pruitt, 100 F. App’x at 716. Thus, in the absence of any allegation that the company retained records in its billing system longer than required, the court concluded that the cable company had not illegally retained PII. Id. at 717.


204. Id. at *14. Courts have interpreted “something akin to a name” to mean information that directly identifies an individual, on the basis of distinctions made between the three types of information considered in In re Hulu II. See discussion infra notes 205–17 and accompanying text. Even where the recipient is already in possession of information that can be used to identify the person, courts have held that this requirement is not satisfied. See, e.g., Eichenberger, 2015 WL 7252985, at *1. *5 (finding that a device identifier was not “akin to a name,” even though the third party “automatically correlated [it] with existing user information” already in its possession to identify the plaintiff).


206. Id. The court’s focus on knowledge of a person’s “identity” ignores the reality that an individual becomes less “anonymous” as the amount of information collected about that individual increases, in addition to the context in which that information is viewed. See Jeffrey M. Skopec, Anonymity, the Production of Goods, and Institutional Design, 82 FORDHAM L. REV. 1751, 1758–59 (2014) (“[T]he degree to which something is anonymous can depend on context, including the knowledge of the person seeing it. . . . [T]he quantity of identifying information associated with something that is anonymous is rarely fixed, in that more information will often be available at some additional cost or effort.”); see also discussion supra Section II.B.


208. Id.

209. Id. at *3.
page on the Hulu website, which contained the person’s first and last name.\textsuperscript{210} Significantly, however, the court found that there was no evidence to suggest that comScore had actually used that information to learn the identities of the users it tracked.\textsuperscript{211} Furthermore, comScore’s interest in gathering information relevant to the targeting of advertisements was not sufficient to “suggest any linking of a specific, identified person and his video habits.”\textsuperscript{212} Thus, the court concluded that the Hulu User ID was not PII.\textsuperscript{213}

By contrast, the court concluded that information disclosed to Facebook was sufficient to identify individual Facebook users.\textsuperscript{214} The court distinguished the Facebook User ID from the comScore User ID on the basis that it is “more than a unique, anonymous identifier,” because it “personally identifies a Facebook user.”\textsuperscript{215} Moreover, unlike the disclosure of the Hulu User ID, which required comScore to take steps to extract the user’s identity from a profile page, Facebook would have understood that the Facebook User ID identifier represented one of its users.\textsuperscript{216} Thus, the court found that Hulu had transmitted its users’ actual identities to Facebook.\textsuperscript{217}

Revisiting the issue in\textit{ In re Hulu III}, however, the court held that Hulu had not violated the VPPA because it did not\textit{ knowingly} disclose PII.\textsuperscript{218} The court focused on evidence that the Facebook ID and video viewing information were sent to Facebook in separate, albeit simultaneous, transmissions.\textsuperscript{219} Absent evidence that Facebook actually joined these two pieces of

\begin{enumerate}
\item \textit{Id.} at *3, *9. Although the Hulu User ID could not be used to locate a user profile using a search function on the Hulu website, the profile page could be accessed by manipulating the profile page URL. \textit{Id.} at *3. Specifically, the profile page URL was constructed as “http://www.hulu.com/profiles/u/[User ID],” where “[User ID]” is the Hulu User ID. \textit{Id.}
\item \textit{Id.} at *12.
\item \textit{Id.}
\item \textit{Id.} at *8, *12. \textit{In re Hulu II}’s requirement that the recipient of disclosed information actually attempt to identify an individual is at odds with the remedial character of the VPPA, particularly where, as here, the one disclosing the information has control, not only over the information it discloses directly but also over the additional information that is disclosed indirectly. \textit{See} Dirkes v. Borough of Runnemede, 936 F. Supp. 235, 241 (D.N.J 1996) (holding that as a remedial statute, the VPPA “should be construed broadly” to protect consumer privacy (citing Local 28 of Sheet Metal Workers v. E.E.O.C., 478 U.S. 421 (1986)).
\item \textit{In re Hulu II}, 2014 WL 1724344, at *14.
\item \textit{Id.}
\item \textit{Id.} at *12–13.
\item \textit{Id.} at *14; \textit{see supra} note 125 and accompanying text.
\item \textit{In re Hulu III}, 86 F. Supp. 3d 1090, 1105 (N.D. Cal. 2015).
\item \textit{See id.} at 1096.
\end{enumerate}
information, the court concluded that there could be no “disclosure.” 220 Additionally, there was no evidence that Hulu knew whether Facebook would link the information together to learn the video preferences of an identified Facebook user. 221 Thus, because Hulu had not “knowingly” disclosed PII, the court granted Hulu’s motion for summary judgment. 222

In In re Hulu II’s wake, the majority of courts that have applied the VPPA in an Internet video context have found support in In re Hulu II for a narrow construction of the Statute’s definition of PII. 223 The district court in In re Nickelodeon I, for example, drew support from In re Hulu II in holding that “PII is information which must, without more, itself link an actual person to actual video materials.” 224 Applying its rule to the information at issue in In re Nickelodeon I—including, among other things, anonymous usernames, IP addresses, and unique device identifiers—the court concluded that “[n]one of this information, either individually or aggregated together, could without more serve to identify an actual, identifiable Plaintiff ....” 225 Thus, even though the plaintiffs contended that Google could identify individuals based on disclosed information, the court held that the disclosed information was not PII because it did not itself identify a person. 226

Likewise, in Ellis, the court interpreted In re Hulu II as standing for the proposition that there is no VPPA violation where the recipient of information

220. Id.; see supra note 213.  But see Suzanne L. Riopel, Comment, The Price of Free Mobile Apps Under the Video Privacy Protection Act, 6 AM. U. BUS. L. REV. 115, 135 (2016) (“[T]he courts should consider whether the individual’s information and the video title or description [are] transmitted separately or together, and if separately, the length of time between the transmissions.”).
221. In re Hulu III, 86 F. Supp. 3d at 1097.
222. Id. at 1105.
225. Id. (emphasis added).
must take “further steps” to match the identifier to a specific person.\textsuperscript{227} The issue before the court was whether a mobile device identifier constituted PII when it was disclosed along with video viewing activities to an analytics company that allegedly combined that information with data already in its possession to identify the person.\textsuperscript{228} Relying on \textit{In re Hulu II} and \textit{In re Nickelodeon I}, the court concluded that because the recipient could not learn the identity of the person by looking \textit{only} at the disclosed information, there was no disclosure of PII.\textsuperscript{229}

Thus, \textit{In re Hulu II} has been interpreted to prohibit an examination of the context in which information is disclosed.\textsuperscript{230} But \textit{In re Hulu II} did not foreclose the importance of examining the context of information disclosure in determining whether it constitutes PII.\textsuperscript{231} To the contrary, the \textit{In re Hulu II}


\textsuperscript{228} Ellis, 2014 WL 5023535, at *1, *3.

\textsuperscript{229} Id. at *3 & nn.34 & 38 (citing \textit{In re Nickelodeon I}, 2014 WL 3012873, at *10; and then citing \textit{In re Hulu II}, 2014 WL 1724344, at *15–16).

\textsuperscript{230} See Perry v. Cable News Network, Inc., No. 1:14–CV–02926–ELR, 2016 WL 4373708, at *1, *4 (N.D. Ga. Apr. 20, 2016) (concluding that—despite allegations that a recipient used disclosed information to actually identify users and their private viewing habits—“an anonymous string of numbers . . . is insufficient to qualify as [PII]”), \textit{aff’d on other grounds}, 854 F.3d 1336 (11th Cir. 2017); \textit{In re Nickelodeon II}, 2015 WL 248334, at *3 (finding allegations of information already in possession of recipient were irrelevant to determining whether information disclosed was itself PII); Ellis, 2014 WL 5023535, at *3 (declining to consider information already in possession of the recipient of a disclosure in determining whether information constituted PII); supra notes 223–29 and accompanying text. But see Robinson v. Disney Online, 152 F. Supp. 3d 176, 182 (S.D.N.Y. 2015) (“Context may matter, for instance, to the extent other information disclosed by the provider permits a ‘mutual understanding that there has been a disclosure’ of PII.”) (quoting \textit{In re Hulu III}, 86 F. Supp. 3d 1090, 1097 (N.D. Cal. 2015)); Yeshov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 145 (D. Mass. 2015) (examining \textit{In re Hulu II} and concluding that “the inquiry is context-dependent”), \textit{rev’d on other grounds}, 820 F.3d 482 (1st Cir. 2016). Interestingly, despite acknowledging the relevance of context in the PII inquiry, the Robinson court excludes from its definition of context the capability of the recipient to identify the subject of the disclosure. Robinson, 152 F. Supp. 3d at 183.

As the court notes, recognizing that context matters—and that a third-party recipient needs to know the import or nature of the information it receives for that information to have meaning—is not the same as concluding that information which is not otherwise PII can somehow become PII because of the potential, however remote, of a third party to “reverse engineer” a disclosure using data gathered from other sources.

\textit{Id.}

\textsuperscript{231} See \textit{In re Hulu II}, 2014 WL 1724344, at *11 (“[T]he statute, the legislative history, and the case law do not require a name, instead require the identification of a specific person tied to a specific transaction, and support the conclusion that a unique anonymized ID alone is not PII but context could render it not anonymous and the equivalent of the identification of a specific person.”).
court suggested that unique identifiers, such as unique user identifiers or mobile device identifiers, may constitute PII in the proper context. The difference in interpretation results from an ambiguity in the words—oft repeated by In re Hulu II and its progeny—"without more." As noted above, some courts have interpreted this language to render context irrelevant, while those that do interpret these words to require an examination of context nevertheless disagree as to the permissible extent of the contextual inquiry.

C. **Yershov v. Gannett Satellite Information Network, Inc.**

In Yershov, the First Circuit articulated a new test for determining whether information constituted PII within the meaning of the VPPA, departing from the reasoning of In re Hulu II and its progeny. There, a user of the USA Today mobile application (the App) claimed that Gannett Satellite Information Network, Inc. (Gannett) disclosed information about user video viewing activities in violation of the VPPA. The user claimed that when he accessed video content on the App, his GPS coordinates, a unique mobile device identifier, and the titles of the videos viewed were disclosed to Adobe Systems, Inc. (Adobe).

Adobe is a third-party that provides its clients with online marketing services and analytics. In this capacity, Adobe collected information from

---

232. *Id.*

233. *Compare Ellis*, 2014 WL 5023535, at *3 ("[PII] is that which, in its own right, without more, links an actual person to actual video materials.") (quoting In re Nickelodeon I, 2014 WL 3012873, at *10), with In re Hulu II, 2014 WL 1724344, at *12 ("[I]t is whether a unique identifier—without more—violates the VPPA. It does not."). *In re Hulu II*’s formulation of the rule was based on an examination of Pint v. Comcast Cable Holdings, LLC, 100 F. App’x 713 (10th Cir. 2004), where the information required to link digital identifiers to an identifiable person was implicitly inaccessible to everyone outside of the cable company. *See supra* note 202.

234. *See* cases cited *supra* note 230.

235. *Compare Yershov*, 104 F. Supp. 3d at 145 (finding support in In re Hulu II for holding that context could render an Android ID PII, but noting that In re Hulu II was ambiguous with respect to whether that context included information already in the possession of the party to whom information was disclosed), with Robinson, 152 F. Supp. 3d at 183 (acknowledging the relevance of context, but holding that the relevant context does not include information the recipient of a disclosure had culled from other sources).


237. *Id.* at 484–85. Gannett published the newspaper USA *Today* in print form and provided access to its content online through its mobile application. *Id.* at 484.

238. *Id.* at 484–85.

239. *Id.* at 484. Specifically, Adobe helps its clients by enabling them to "personalize and improve
Gannett, including unique device identifiers, which allowed Adobe “to identify and track specific users across multiple electronic devices, applications and services.”240 With this information, Adobe was able to create a profile of the user from data collected from different sources.241 This profile allegedly included details such as the user’s name and age, as well as a history of online activities, and provided “an intimate look at the different types of materials consumed by the individual” for the purpose of behavior targeting of online advertisements.242

After noting that the definition of PII provided in the statute “adds little clarity beyond training [the court’s] focus on the question whether the information identifies the person who obtained the video,” the court recognized that “PII is not limited to information that explicitly names a person.”243 Like other courts to consider the definition, the First Circuit focused on the use of the word includes, which it found to suggest that “the proffered definition falls short of capturing the whole meaning.”244 Moreover, the court found support in the legislative history that “the drafters’ aim was ‘to establish a minimum, but not exclusive, definition of personally identifiable information.’”245

Reasoning by analogy—likening the user profile in Adobe’s system to a “game program” that would enable them to identify the user based on the information disclosed—the court concluded that the disclosure to Adobe was “reasonably and foreseeably likely” to reveal the identity of the plaintiff in connection with the videos that he watched.246 Thus, the First Circuit articulated a new test for PII, one that significantly departed from the majority of

240. Yershov, 820 F.3d at 484.
241. Id.
242. Id. at 484–85; see also Adobe Marketing Cloud Privacy, supra note 239.
243. Yershov, 820 F.3d at 486.
244. Id.
245. Id. (quoting S. Rep. No. 100-599, at 12).
246. Id. Interestingly, the First Circuit did not discuss the development of the law through In re Hulu II and its progeny. However, the district court reviewed the case law and concluded that the conclusions in In re Nickelodeon I and Ellis were flawed. See Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 145 (D. Mass. 2015) (“Nickelodeon’s conclusion that ‘PII is information which must, without more, itself link an actual person to actual video materials’ is flawed. That conclusion would seemingly preclude a finding that a home address or social security number is PII.”).
decisions by the district courts that had considered the issue.\textsuperscript{247}

D. \textit{In re Nickelodeon Consumer Privacy Litigation}

Shortly after \textit{Yershov}, the Third Circuit also confronted the issue of what constitutes PII within the meaning of the VPPA.\textsuperscript{248} In a lengthier opinion, which purported to be consistent with \textit{Yershov}, the Third Circuit articulated a new test that nevertheless departed substantially from the contextual approach of the First Circuit.\textsuperscript{249} In \textit{In re Nickelodeon}, a purported class of children under age thirteen (the Children) claimed that Viacom disclosed information about the videos they had watched on the Nick.com website to Google, who provides advertising on the website.\textsuperscript{250} According to the Children’s claim, at least eleven pieces of information were disclosed, but the court focused on three types of information in particular.\textsuperscript{251} These included the user’s IP address, the browser fingerprint,\textsuperscript{252} and the unique device identifiers\textsuperscript{253} of devices used to access the Nick.com website.\textsuperscript{254} The Children claimed that Google’s ubiquity would enable Google to accurately identify them and the videos they watched.\textsuperscript{255}

In its defense, Viacom argued that the disclosures protected by the VPPA

\textsuperscript{247} Surely, that cannot be correct. Therefore, because it relies on \textit{Nickelodeon} and \textit{Hulu}, the holding in \textit{Ellis} . . . is unpersuasive.", \textit{rev’d on other grounds}, 820 F.3d 482 (1st Cir. 2016). Further, the district court found ambiguity in \textit{In re Hulu II} regarding whether “context could render [an anonymous identifier] PII if the third party receiving the information had independent information that helped link the [identifier] with a specific person.” \textit{Id.} By articulating its new test, the First Circuit addresses these concerns, although the extent to which context factors into the analysis is unclear. \textit{See} discussion infra Section IV.A.1.

\textsuperscript{248} \textit{In re Nickelodeon}, 827 F.3d at 281–90.

\textsuperscript{249} \textit{Id.} at 289–90; \textit{discussion supra} Section III.C.

\textsuperscript{250} \textit{In re Nickelodeon}, 827 F.3d at 268–70. at 270.

\textsuperscript{251} \textit{Id.} at 281.

\textsuperscript{252} \textit{Id.} at 281–82. \textit{See} supra notes 119–21 and accompanying text.

\textsuperscript{253} \textit{In re Nickelodeon}, 827 F.3d at 282. \textit{See supra} notes 119–21 and accompanying text.

\textsuperscript{254} \textit{In re Nickelodeon}, 827 F.3d at 282. Importantly, browser fingerprints and device identifiers would each enable the accurate tracking of an individual online. \textit{See} supra notes 96–101, 119–21 and accompanying text.

\textsuperscript{255} \textit{In re Nickelodeon}, 827 F.3d at 282.
were limited to instances in which the information, standing alone, was sufficient to identify a particular individual. Further, the type of data disclosed was not of a type that legislators, who were concerned with “brick-and-mortar transactions,” would have had in mind when they enacted the law.

In analyzing the merits of the two positions, the court found that PII constitutes a spectrum, with the individual’s name at one end of the spectrum, and the type of static digital identifiers at issue here on the opposite end of the spectrum. The court suggested that a phone number, street address, and similar information typically in the public record would reside somewhere in the middle of the spectrum. Because such information may be readily found in public records, identification of the individual could readily be accomplished by consulting “a phone book or property records.” This contrasts with the information at issue here, the court noted, because “[t]o an average person, an IP address or a digital code in a cookie file would likely be of little help in trying to identify an actual person.”

The general rule that emerges from the court’s decision is that under the VPPA, PII means “the kind of information that would readily permit an ordinary person to identify a specific individual’s video-watching behavior.” Applying this rule, the court held that static digital identifiers, such as an IP address, unique device identifier, and browser fingerprints, were “simply too far afield from the circumstances that motivated the Act’s passage to trigger

---

256. Id.
257. Id.
258. Id. at 282–83. On the surface, the court’s analysis echoes recent privacy scholarship. See, e.g., Schwartz & Solove, supra note 56, at 1877 (proposing a new standard for PII that arranges information on a continuum based on the risk of identification). However, in its analysis, the court focuses on the kind of information rather than on the risk of identification, placing information that scholars deem to carry a high risk of identification at the opposite end of the spectrum. See In re Nickelodeon, 827 F.3d at 282–83; Schwartz & Solove, supra note 56, at 1878 (“Information that brings a substantial risk of identification of an individual should . . . be treated as referring to an identified person.”); see also discussion infra Section IV.A.2.
259. In re Nickelodeon, 827 F.3d at 282–83.
260. Id. at 283.
261. Id.
262. Id. at 290.
liability." In reaching this conclusion, the court expressed concern that recognizing such information as PII would be overinclusive.

IV. ANALYSIS

The split in authority that has emerged from the First and Third Circuits exemplifies a key problem relating to the definition of PII as applied in an Internet context. Because there has been no unifying conception of privacy, courts have had a tendency to reduce privacy to an amalgamation of separate and distinct concepts. As a result, privacy interests may not be weighed sufficiently or countervailing concerns may be overvalued. This is particularly true in instances where the privacy harm may not be readily apparent, such as in cases involving disclosure of PII under statutes that do not require

263. Id. at 279, 290. In reaching this conclusion, the court placed significant weight on the VPPA’s pre-enactment history, particularly the disclosure of Judge Bork’s video rental history. See id. at 279, 284–87; see also discussion supra Section III.A.

264. See In re Nickelodeon, 827 F.3d at 290 (“If an IP address were to count as [PII], either standing alone or coupled with similar data points, then the disclosure of an IP address to any Internet company with registered users might trigger liability under the [VPPA].”). The Ninth Circuit expressed similar concerns in Eichenberger when it affirmed the district court’s grant of a 12(b)(6) motion to dismiss. See Eichenberger v. ESPN, Inc., 876 F.3d 979 (9th Cir. 2017). There, the issue was whether disclosure to Adobe of a unique device identifier, in conjunction with the identity of videos watched, constituted PII under the VPPA’s definition. Id.; see also supra notes 239–42 and accompanying text (discussing similar allegations involving Adobe’s capabilities in Yeshivah). In adopting the Third Circuit’s ordinary person test, the Ninth Circuit reasoned that this test “better informs video service providers of their obligations under the VPPA” because “[i]t looks to what information a video service provider discloses, not to what the recipient of that information decides to do with it.” Eichenberger, 876 F.3d at 985.

265. See Schwartz & Solove, supra note 56, at 1836–39, 1841–49 (suggesting that the “key recent development” challenging PII is online behavioral marketing, which coincides with AOL’s search data release in 2006, Facebook’s introduction of its “Beacon online ad system” in 2007, and the increase in the prevalence of static IP addresses, which increase the traceability of users, in the same period).

266. See SOLOVE, supra note 36, at 37–38 (noting that due to the difficulty of conceptualizing privacy, efforts to define a “common denominator” that underlies the various interests included within “the rubric of ‘privacy’” has led many to see privacy as derivative of “more primary conceptions”) (emphasis added); see also Amy L. Peikoff, The Right to Privacy: Contemporary Reductionists and Their Critics, 13 VA. J. SOC. POL’Y & L. 474, 476–79 (2006) (describing Prosser’s effort to define privacy as four distinct torts as a primarily reductionist effort); Ruth Gavison, Privacy and the Limits of Law, 89 YALE L.J. 421, 460 (1980) (noting that those who seek to understand the right to privacy by starting with an examination of judicial decisions “tend to conclude with a reductionist account”).

267. Gavison, supra note 266, at 421–24 (suggesting that the lack of an “affirmative and explicit commitment to privacy” in the legal system leads to legal results that undervalue privacy in relation to other considerations).
proof of harm beyond the disclosure of PII itself.\textsuperscript{268}

Thus, because statutory protections of privacy are triggered only by the disclosure of PII, it is critical that courts adjudicating claims brought under such provisions have a clear conception of what constitutes PII, or—when it is not clear—a consistent standard for determining whether the information in question constitutes PII.\textsuperscript{269} Where, as here, the statute in question does not define the specific types of information that should be treated as PII, the burden rests more heavily on the court to effectuate the statute’s remedial purpose.\textsuperscript{270}

The VPPA defines PII as a standard, which permits courts to exercise broad discretion in determining how best to carry out the Statute’s underlying policy.\textsuperscript{271} Moreover, a broad interpretation of the Statute is appropriate, given its remedial purpose of protecting a privacy interest that implicates the First Amendment.\textsuperscript{272} A proper analysis of the holdings in \textit{In re Nickelodeon} and \textit{Yershov} must, therefore, examine the tests used by each court and consider the extent to which each test furthers that purpose.\textsuperscript{273} This analysis begins


\textsuperscript{269} See Schwartz & Solove, \textit{supra} note 56, at 1817 (noting that the reductionist conceptions of PII tend to view PII as “only that personal data that has been specifically associated with a specific person,” and as a result, much personal data that should be legally protected is not).

\textsuperscript{270} See, e.g., United States v. Drum, 368 U.S. 370, 375–76 (1962) (reversing a district court’s narrow interpretation of imprecise definitional language where a broader interpretation did not run contrary to the remedial purpose of a regulatory statute); Schwartz & Solove, \textit{supra} note 56, at 1828–36 (comparing three different approaches that privacy protection statutes have used to define PII, and noting that while the “tautological” approach taken by the VPPA has the advantage of being able to “evolve and remain flexible,” it suffers from being uninformative).

\textsuperscript{271} See Schwartz & Solove, \textit{supra} note 56, at 1870. This contrasts with the approach taken in other statutes which define PII to include specific types of information. See \textit{id}. at 1831.


\textsuperscript{273} See Schwartz & Solove, \textit{supra} note 56, at 1870.
with an examination of the reasoning employed by each court.\textsuperscript{274} Next, the pertinent factors underlying the standards applied by both courts are discussed in the context of advancing a factor-based test for classifying information as PII or non-PII in the context of the VPPA.\textsuperscript{275}

\textbf{A. Of Differing Standards and Unpredictable Results}

Although several district courts have considered the VPPA’s prohibition on the disclosure of PII,\textsuperscript{276} the First, Third, and Ninth Circuits are the only circuit courts to examine this issue to date.\textsuperscript{277} In \textit{Yershov}, the First Circuit departed from the rationale of \textit{In re Hulu II} and its progeny to make clear that context is relevant to determining whether information is PII, while avoiding a rigid focus on the kinds of information involved.\textsuperscript{278} In \textit{In re Nickelodeon}, the Third Circuit announced a new test that is less focused on the context than on the type of information involved.\textsuperscript{279} In \textit{Eichenberger}, the Ninth Circuit adopted the Third Circuit’s approach without modification, noting that the definition of \textit{PII} cannot depend on the recipient’s capabilities, because that “would make ‘[t]he lawfulness of [a] disclosure . . . depend on circumstances outside of [a video service provider’s] control’”\textsuperscript{280} Despite some overlap, in which the courts are likely to arrive at the same results, there is a significant

\begin{itemize}
  \item \textsuperscript{274} See discussion infra Section IV.A.
  \item \textsuperscript{275} See discussion infra Section IV.B.
  \item \textsuperscript{276} See cases cited supra notes 192, 223.
  \item \textsuperscript{277} See Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482 (1st Cir. 2016); In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262 (3d Cir. 2016), cert. denied, 137 S. Ct. 624 (2017). Although the Eleventh Circuit had an opportunity to examine the issue in Ellis v. Cartoon Network, Inc., the court declined to address the issue, affirming the district court’s dismissal of the case on the grounds that the plaintiff was not a “subscriber” within the meaning of the VPPA. 803 F.3d 1251, 1258 (11th Cir. 2015).
  \item \textsuperscript{278} See infra Section IV.A.1.
  \item \textsuperscript{279} See infra Section IV.A.2.
  \item \textsuperscript{280} Eichenberger v. ESPN, Inc., 876 F.3d 979 (9th Cir. 2017) (alterations and omission in original) (quoting Mollett v. Netflix, Inc., 795 F.3d 1062, 1066 (9th Cir. 2015)). This is arguably a mischaracterization of the First Circuit’s test, which requires that the recipient’s identification of the data subject be both reasonably and foreseeable likely. See discussion infra Section IV.A.1. In other words, the First Circuit’s inquiry asks not what the recipient actually does with the information after it has been disclosed, but whether the identification is foreseeable based on the video service provider’s knowledge of the recipient. See Yershov, 820 F.3d at 486 (“When Gannett makes . . . a disclosure to Adobe, it knows that Adobe has the ‘game program,’ so to speak, allowing it to link the the GPS address and device identifier information to a certain person by name, address, phone number, and more.” (emphasis added)).
\end{itemize}
divergence in the effect of the two tests, resulting in the inconsistent application of federal law.281

1. The First Circuit’s Reasonable and Foreseeable Likelihood Test

The First Circuit’s holding in *Yershov* represents a substantial departure from the majority of district courts to consider the scope of PII in the context of streaming video under the VPRA.282 By defining that scope to include information that is “reasonably and foreseeably likely” to identify a person’s video viewing activities, the court rejects the rule, adopted by most district courts to have considered the issue, that “PII is information which must, without more, itself link an actual person to actual video materials.”283 Importantly, the First Circuit acknowledges the relevance of contextual factors in determining whether information constitutes PII under the Statute.284 Although the court does not expressly identify them, several factors are implicated by the analogies that form the basis of the court’s holding.285

281. *See* discussion infra Sections IV.A.1–2. Although the tests adopted by the First Circuit (“reasonable and foreseeable likelihood”) and the Third Circuit (“ordinary person”) may have a substantial degree of overlap in which consistent results would be achieved, there are important differences. *See* discussion infra Sections IV.A.1–2. Both courts are likely to agree that GPS coordinates, physical addresses, or email addresses, if disclosed in connection with video viewing activities, would constitute PII within the meaning of the VPRA. *See* discussion infra Sections IV.A.1–2. On the other hand, the types of information that are typically used by behavior targeting technologies, including device identifiers, cookies, IP addresses, and browser fingerprints, may be included by the First Circuit’s test, but would be excluded by the Third Circuit’s test. *See* discussion infra Sections IV.A.1–2. To add to the confusion, when the district court interpretations are counted, there are at least four distinct interpretations of the meaning of PII under the VPRA. *See supra* notes 128–33 and accompanying text.

282. *See* discussion supra Section III.B.

283. *In re Nickelodeon I*, No. 12–07829, 2014 WL 3012873, at *10 (D.N.J. Jul. 2, 2014); *see also* Eichenberger v. ESPN, Inc., No. C14–463 TSZ, 2015 WL 7252985, at *6 (W.D. Wash. May 7, 2015) (holding that disclosure of information, which standing alone does not identify an individual, is not PII within the meaning of the VPRA, even if the recipient is already in possession of additional information that could be combined with the disclosed information to identify the plaintiff), *aff’d*, 876 F.3d 979 (9th Cir. 2017); Locklear v. Dow Jones & Co., 101 F. Supp. 3d 1312, 1318 (N.D. Ga. 2015) (holding that information disclosed by defendant was not PII within the meaning of the VPRA where the recipient was required “to take further steps” to match the disclosed information to the plaintiff); Ellis v. Cartoon Network, Inc., No. 1:14–CV–484–TWT, 2014 WL 5023535, at *3 (N.D. Ga. Oct. 8, 2014) (holding that disclosed information was not PII where “extra steps” were required by the recipient of the information in order to identify plaintiff), *aff’d on other grounds*, 803 F.3d 1251 (11th Cir. 2015); supra Section III.B (discussing the evolution of this rule in the district courts).

284. *See* infra notes 286–307 and accompanying text.

285. *See* infra notes 287–88, 295, 300–01, 306–07, 309 and accompanying text; *see also* discussion infra Section IV.B (discussing the factors implicated by the First Circuit’s holding).
In its first analogy, the court proposes that “[r]eviewing a person’s social security number to the government” identifies a person as easily as revealing the person’s name. From this, we may infer that whether information constitutes PII depends, at least in part, on the characteristics of the information disclosed and what the recipient is able to ascertain from that information. Importantly, social security numbers are unique, with each number representing one and only one person. However, unlike a person’s name, a social security number standing alone does not constitute an actual identification. Without access to a data source that would permit the recipient to match it to a name, a social security number does not actually reveal a person’s identity. Thus, it is important to the court’s analogy that the social security number is revealed “to the government." Implicitly, the government has access to records that link an individual’s social security number to a name, and the government has the capability to actually use that information for the purpose of identification. This does not mean, however, that a social security number revealed to an ordinary person is non-PII. Although the likelihood of identification may be at its highest when a person’s social security number is revealed to the government, disclosure of this information to others is nevertheless significant given the widespread use of the social security number in private enterprises. As the court’s example suggests, however,

287. See id.; infra text accompanying notes 288–92.
288. See, e.g., Bowen v. Roy, 476 U.S. 693, 710 (1986) (observing that social security numbers are “unique numerical identifiers” that are used “pervasively” by government programs to track individuals). Because social security numbers are unique, they are often used in government records to distinguish between individuals having the same name. Id.
289. [A] social security number . . ., in isolation, is anonymous”), rev’d on other grounds, 820 F.3d 482 (1st Cir. 2016).
290. See id.
291. See Yershov, 820 F.3d at 486; see also supra note 288.
292. See supra note 288.
293. See infra note 294 and accompanying text.
294. See Daniel J. Solove & Chris Jay Hoofnagle, A Model Regime of Privacy Protection, 2006 U. Ill. L. Rev. 357, 366–67 (2006) (suggesting that the Privacy Act’s failure to rein in the use of social security numbers in private sector entities has enabled data brokers and consumer reporting agencies to amass databases that may include social security numbers). In Nickelodeon, the Third Circuit similarly remarked that a social security number is not “easily matched” to a name without consulting another source. In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 282–83 (3d Cir. 2016), cert. denied, 137 S. Ct. 624 (2017). Nevertheless, a social security number is universally held to be
determining the likelihood of identification necessarily requires consideration of the nature of the information disclosed, the recipient’s ability to access additional required information, and the recipient’s capability to make an identification.295

The court’s second analogy functions to broaden the scope of PII through incorporation of additional factors.296 There, the court suggests that “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.”297 Similar to a social security number, a jersey number identifies a person to the extent that the recipient has access to additional information and the capability to use that information for the purposes of identification.298 However, unlike a social security number, a jersey number is, at most, unique only within the scope of the player’s team.299 Additional information about the context may be required for an identification to be likely.300 In other words, the ability of a spectator to identify “No. 12 on the offense” requires that the spectator know which team has possession of the ball, in addition to a listing of the team’s players and their jersey numbers.301 Thus, the court suggests that information may be PII, even if it must be combined with other information in order to

PII. See Yershov, 104 F. Supp. 3d at 141, 146 (noting that a social security number is “[w]ithout question” PII, and to conclude otherwise would be “absurd,” even in the absence of a publicly available source by which that number can be linked to a name). This suggests that the risk of identification, although sufficient, may not be necessary to constitute PII. See id. Other considerations may include risk of harm beyond that incurred as a result of identification, such as the risk of fraud and the resulting potential for financial and reputational harm. See Daniel J. Solove, Identity Theft, Privacy, and the Architecture of Vulnerability, 54 HASTINGS L.J. 1227, 1245 (2003) (“The identity thief not only pilfers victims’ personal information, but also pollutes their dossiers by adding false information, such as unpaid debts, traffic violations, parking tickets, and arrests.”). Importantly, some types of fraud, including synthetic identity theft, do not require the identity thief to know the name of the person whose social security number has been fraudulently used. Chris Jay Hoofnagle, Identity Theft: Making the Known Unknowns Known, 21 HARV. J.L. & TECH. 97, 101 (2007). In Yershov, the First Circuit is concerned exclusively with the risk of identification, insofar as a social security number “plainly identifies the person.” Yershov, 820 F.3d at 486.

295. See supra text accompanying notes 286–92.
296. See Yershov, 820 F.3d at 486; infra notes 297–301 and accompanying text.
297. Yershov, 820 F.3d at 486.
298. See id.
300. See supra notes 298–99 and accompanying text.
301. See Yershov, 820 F.3d at 486; supra notes 297–300 and accompanying text.
make an identification.302

Finally, in its examination of the ability to use GPS coordinates to identify a person, the court proposes a hypothetical fact pattern involving a disclosure that “a person viewed 146 videos on a single device at [two] sets of specified GPS coordinates.”303 Unlike social security and football jersey numbers, which uniquely identify individuals, GPS coordinates uniquely identify locations.304 Apparently in acknowledgment of this difference, the court’s hypothetical includes multiple locations (home and work) observed over an extended series of events (146 videos watched), with each observation associated to the other observations through some commonality (a single device).305 Through these hypothetical facts, the court suggests that although the likelihood of identifying an individual by a single set of GPS coordinates may be low, the likelihood of identification increases with the amount of data collected.306 Thus, the quantity of information disclosed and length of time that information is likely to be stored may be relevant in determining whether the information constitutes PII.307

The court draws support for including unique device identifiers and GPS coordinates within the scope of PII by analogizing its hypothetical to the VPPA’s pre-enactment history, suggesting a similarity between the disclosure of Judge Bork’s name and video list to a reporter, on the one hand, and the disclosure of GPS coordinates and unique device identifiers to a company

302. See Yershov, 820 F.3d at 486.
303. Id. Given that the disclosure of Judge Bork’s video rental list included 146 videos, the use of the same number here signals an attempt to tie this hypothetical to the VPPA’s pre-enactment history. See supra text accompanying notes 140–43.
304. See Yershov, 820 F.3d at 486. GPS coordinates reported by devices may refer to a variety of locations due to the mobility of such devices, and may not necessarily refer to a location at which the individual is likely to stay or to which she is likely to return. See PEW RESEARCH CENTER, supra note 120, at 37 (reporting that adults use their smartphones in a variety of locations outside of home and work, and such use is more prevalent among younger adults). On the other hand, a mobile device identifier refers to a single mobile device. See supra notes 119–21 and accompanying text. Thus, while a “game program” might identify the user of a mobile device based on disclosure of a single device identifier, identification of a specific person using GPS coordinates would potentially require the collection of multiple GPS coordinates collected over a sufficient period of time. See infra notes 305–07 and accompanying text.
305. See Yershov, 820 F.3d at 486. For a discussion of the use of a common identifier in the context of inferring an individual’s identity, see supra Section II.B.3.
306. See Yershov, 820 F.3d at 486.
307. See supra notes 303–06 and accompanying text.
holding a “game program,” on the other.308 Thus, when the person to whom
the information is disclosed has access to additional information and the ca-
phability of using that information to identify a person, it is “reasonably and
foreseeably likely” that such an identification will be made.309

Despite the apparent clarity this approach provides by casting highly tech-
nical concepts in commonplace terms, the court’s opinion is ambiguous with
respect to the kinds of information included within the scope of its holding.310
Although the court concluded that the unique device identifiers and GPS co-
dordinates constitute PII within the meaning of the VPPA to the extent that they
are reasonably and foreseeably likely to reveal an individual’s video watching
activities, it is unclear whether the court meant that each kind of information,
standing alone, is within the Statute’s meaning of PII, or whether the combi-
nation of both kinds of information is required.311 Moreover, it is ambiguous
whether the court intended its holding to be restricted to only unique device
identifiers and GPS coordinates, or whether other information, such as IP ad-
dresses and browser fingerprints, might fall within the scope of PII.312 This
lack of specificity makes the court’s holding susceptible to misinterpretation
by other courts to confront the issue.313 Nevertheless, it is reasonable to inter-
pret the First Circuit’s opinion to mean that any information, whether it is a

308. See Yershov, 820 F.3d at 486 (suggesting that when the recipient of a disclosure holds a “game
program” enabling it to identify the individual whose information has been disclosed, such information
may identify the person as easily as a name); supra Section III.A.

309. See Yershov, 820 F.3d at 486 (concluding that the disclosure of device identifiers, GPS co-
nordinates, and titles of videos watched by Yershov was “reasonably and foreseeably likely” to identify
Yershov and the videos he had watched).

310. See infra notes 311–13 and accompanying text.

311. See Yershov, 820 F.3d at 486. If the court views device identifiers as being similar to social
security numbers in terms of their ability to uniquely identify a particular person, then disclosure of a
device identifier to someone who has a “game program” would constitute PII under the court’s hold-
ing, even if no GPS coordinates were disclosed. See id.; supra notes 286–95 and accompanying text.
The court’s conclusion, however, specifically considers only the combination of both kinds of infor-
mation. See Yershov, 820 F.3d at 486 (“[W]hen Gannett makes . . . a disclosure to Adobe, it knows
that Adobe has the ‘game program,’ so to speak, allowing it to link the GPS address and device iden-
tifier information to a certain person by name, address, phone number, and more.”).

312. See Yershov, 820 F.3d at 486. Although the court does not specifically discuss other types of
information, the court does acknowledge that “[m]any types of information other than a name can
easily identify a person.” Id.

313. See, e.g., Eichenberger v. ESPN, Inc., 876 F.3d 979, 986 (9th Cir. 2017) (noting that its deci-
sion, based on the Third Circuit’s test, “does not necessarily conflict with Yershov,” which “relies, in
part, on the nature of GPS location data”); In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262,
mobile device identifier, a set of GPS coordinates, or a combination of these, would constitute PII within the meaning of the VPPA, so long as it is "reasonably and foreseeably likely" that such information identifies an individual.314

Beyond its analogies, however, the court provides little guidance for determining whether it is reasonably and foreseeably likely that the recipient of disclosed information would be able to match video viewing activities to an identifiable individual.315 Although the court does acknowledge that "there is certainly a point at which the linkage of information to identity becomes too uncertain, or too dependent on too much yet-to-be-done, or unforeseeable detective work,"316 it is unclear where that point is or how it should be determined.317

2. The Third Circuit’s Ordinary Person Test

The Third Circuit interprets the VPPA’s definition of PII narrowly, construing it to mean “the kind of information that would readily permit an ordinary person to identify a specific individual’s video-watching behavior."318 Although the court acknowledges that Congress was concerned about the impact of advancements in technology on the legitimate privacy interests of consumers, the court’s “ordinary person” test reflects an effort to limit the application of the VPPA to cases that do not stray too far from the paradigmatic

289 (3d Cir. 2016) (interpreting the First Circuit’s holding in Yershov to be based solely on the presence of GPS coordinates in the information disclosed), cert. denied, 137 S. Ct. 624 (2017). The First Circuit’s failure to address the disclosure of each piece of information disclosed, as well as the totality of the disclosure, in a disciplined manner not only adds to the confusion, but may also undermine important privacy interests. See discussion infra Section V.A.

314. See Yershov, 820 F.3d at 486 (concluding that the information disclosed was “reasonably and foreseeably likely” to reveal which videos Yershov had obtained). The court’s conclusion is significant in that it is not based on the type of information disclosed, but on a determination of the risk of identification, which, as discussed, involves an examination of contextual factors, including access to additional information and the likelihood that an identification would be made. See supra notes 286–307 and accompanying text; see also discussion infra Section IV.B. This approach differs significantly from the Third Circuit’s approach, which is more focused on the kind of information disclosed. See In re Nickelodeon, 827 F.3d at 282–83 (holding that IP addresses, unique device identifiers, and browser fingerprints were not the kind of information encompassed by the VPPA’s definition of PII); discussion infra Section IV.A.2.

315. See Yershov, 820 F.3d at 486.

316. Id.

317. See id.; see also discussion infra Section IV.B (discussing factors).

318. In re Nickelodeon, 827 F.3d at 267 (emphasis added).
example of “a video clerk leaking an individual customer’s video rental history.”\textsuperscript{319} Clearly, the court was concerned that recognizing digital information, such as IP addresses, browser fingerprints, and unique device identifiers, would result in an interpretation of the VPPA that “lack[ed] a limiting principle.”\textsuperscript{320} Thus, the ordinary person test aims to balance the privacy concerns of individuals against the legitimate interests of Internet commerce, which could be unduly burdened if too broad a rule were to be adopted by the court.\textsuperscript{321}

Under the ordinary person test, a court must consider whether an average person would be able to use disclosed information to determine an individual’s identity.\textsuperscript{322} The court’s holding is in accord with Yershov with respect to GPS coordinates, “[g]iven how easy it is to locate a GPS coordinate on a street map.”\textsuperscript{323} But the Third Circuit declined to include IP addresses, device identifiers, and browser fingerprints in the class of information that an average person would be able to link to a specific individual.\textsuperscript{324} The court’s focus on what inferences an ordinary person would be able to draw from such information minimizes the unique risks implicated by the factual circumstances at

\textsuperscript{319} Id. at 290.
\textsuperscript{320} Id.
\textsuperscript{321} See id. at 289–90 (“If an IP address were to count as [PII], either standing alone or coupled with similar data points, then the disclosure of an IP address to any Internet company with registered users might trigger liability under the Act. Indeed, the import of the plaintiffs’ position seems to be that the use of third-party cookies on any website that streams video content is presumptively illegal. We do not think the [VPPA] sweeps quite so broadly.”). The VPPA’s pre-enactment history suggests that Congress was aware of the potential to overburden industry and made choices that aligned with industry practices. See supra Section III.A.1.
\textsuperscript{322} See In re Nickelodeon, 827 F.3d at 282–83 (differentiating between the kinds of information that would permit an ordinary person to identify an individual as having watched certain videos and the kinds of information at issue here, which “[t]o an average person . . . would likely be of little help in trying to identify an actual person”).
\textsuperscript{323} Id. at 289 (alteration in original) (quoting Yershov v. Gannett Satellite Network, Inc., 820 F.3d 482, 486 (1st Cir. 2016)).
\textsuperscript{324} Id. at 283, 289. Notably, the court groups these different kinds of information into the same general category, without regard to the characteristics of each type. See id. For instance, browser fingerprints, although an arguably unique characteristic of individual web browsers, are not guaranteed to be unique. See supra notes 96–101 and accompanying text (discussing the characteristics of browser fingerprints). By contrast, unique mobile device identifiers are unique to the specific device used. See supra notes 119–21 and accompanying text (discussing the characteristics of unique mobile device identifiers). Ironically, therefore, recipients of disclosures containing both a unique device identifier and geolocation data may be more easily and more reliably able to identify an individual based on the unique device identifier than based on the geolocation data. See supra note 304 (discussing characteristics of GPS coordinates).
issue in In re Nickelodeon, where information was disclosed—not to an ordinary person—but to “a company whose entire business model is purportedly driven by the aggregation of information about Internet users.” Moreover, the court’s reasoning undervalues advances in big data analytics and the growth of re-identification science, which, over the past ten years, have rendered the ability to draw inferences of identity from seemingly anonymous data commonplace among aggregators of transactional Internet data.

The court begins its discussion with an observation that the VPPA’s definition of PII is ambiguous, in that it “does not reveal congressional intent with sufficient precision.” Accordingly, the court examines the VPPA’s legislative history to understand the definition of PII in the context of the law’s “basic purpose.” Although the court acknowledges that the VPPA’s definition of PII is “amenable” to a broad interpretation that would include the type of information at issue here, the court declined to ascribe such a broad meaning to the text of the statute. The court found support for its narrow construction of the Statute in an examination of the Statute’s pre-enactment history, its statutory context, and its amendment in 2013.

First, in its examination of the VPPA’s legislative history, the court limited itself to an examination of the committee report accompanying S. 2361

325. In re Nickelodeon, 827 F.3d at 289. In the court’s view, the allegation that an Internet company like Google would use “otherwise anonymous pieces of data” to learn the identity of the individuals who interact with its services is “simply too hypothetical to support liability under the [VPPA].” Id. at 290. However, data breaches widely reported as early as 2012 and security vulnerabilities reported even earlier illustrate the extent to which Internet companies use mobile device identifiers not only to track users, but to identify them. See, e.g., Andy Greenberg, Anonymous Hackers Didn’t Steal Your Apple ID from the FBI—Thanks to Apple, They Didn’t Need to, FORBES (Sept. 10, 2012 2:24 PM), https://www.forbes.com/sites/andygreenberg/2012/09/10/anonymous-hackers-didnt-steal-your-apple-id-from-the-fbi-thanks-to-apple-they-didnt-need-to [https://perma.cc/TJ61-6K6Y] (reporting the theft of user data, including unique device identifiers for 12 million Apple devices, from “an extensive data-sharing network most users aren’t aware of”); Aldo Cortesi, Blog Post, De-anonymizing Apple UDIDs with OpenFeint, CORTESI (May 4, 2011), https://cortesi.publications.io/security/openfeint-uid-deanonymization/index.html [https://perma.cc/N55L-HV6X] (describing a security vulnerability exploiting whereby the hacker was able to link mobile device identifiers to real-world individuals).

326. See, e.g., Crawford & Schultz, supra note 87, at 96 (discussing the “serious privacy problems” implicated by the growth of big data analytics); Ohm, supra note 48, at 1704 (discussing the growth of re-identification and the resulting disruptive effect on privacy policy).

327. In re Nickelodeon, 827 F.3d at 284 (quoting Jensen v. Pressler & Pressler, 791 F.3d 413, 418 (3d Cir. 2015)).

328. Id. at 284–85 (quoting Twentieth Century Music Corp. v. Aiken, 442 U.S. 151, 156 (1975)).

329. Id. at 285–86.

330. Id. at 284–88; see infra notes 331–34, 339–42, 349–52 and accompanying text.
and statements made during the committee hearings. Specifically, the court focused on statements by Senator Leahy and Representative Kastenmeier. Perhaps most supportive of the court’s narrow interpretation is the statement by the latter, “decr[ying] ‘attempts to obtain patrons’ [library] records, under circumstances that . . . would violate most peoples’ perceptions of their right to privacy.” Importantly, because no other statement cited by the court explicitly addresses the circumstances or context the VPPA was intended to cover, the court’s formulation of its “ordinary person” test likely derives from this particular statement. However, this language is strikingly similar, at least in its effect, to language that appears elsewhere in the legislative history. H.R. 3523, introduced shortly after the publication of Judge Bork’s video rental history, would have prohibited “a disclosure that occurs in circumstances in which the individual . . . has a reasonable expectation of privacy.” But when Representatives McCandless and Kastenmeier rewrote the bill, this language was removed, suggesting an intention not to limit the

331. See In re Nickelodeon, 827 F.3d at 284–86.
332. See id. at 285.
333. Id. (emphasis added) (second and third alterations in original) (quoting Joint Hearing on H.R. 4947 and S. 2361, supra note 140, at 21–22 (statement of Rep. Robert W. Kastenmeier, Chairman, Subcomm. on Courts, Civil Liberties & the Admin. of Justice of the H. Comm. on the Judiciary)). Although the statement explicitly refers to S. 2361’s library provision, which was subsequently removed, the court explains, “we think that legislators’ initial focus on both libraries and video stores indicates that the Act was meant to prevent disclosures of information capable of identifying an actual person’s reading or video-watching habits.” Id.
334. See id. at 284 (“Our review of the legislative history convinces us that Congress’s purpose in passing the [VPPA] was quite narrow: to prevent disclosures of information that would, with little or no extra effort, permit an ordinary recipient to identify a particular person’s video-watching habits.” (emphasis added)). A review of the legislative history does not reveal any statements concerning the recipients of information, let alone any characterizations of “ordinary” or “average” ones. See supra Sections III.A.1–2. The term most people appears nowhere else in the VPPA’s legislative history. However, in 1973, DHEW characterized the perceptions of “most people” with respect to identifying information, stating that “most people feel that their names are the most salient features of personal identification.” DHEW REPORT, supra note 49, at 208 (emphasis added); cf. In re Hulu II, No. C11–03764 LB, 2014 WL 1724344, at *14 (N.D. Cal. Apr. 28, 2014) (“The [VPPA] does not require an actual name and requires only something akin to it.”).
335. See infra note 336 and accompanying text.
336. H.R. 3523 § 2(a)(2); see supra notes 153–58 and accompanying text. Courts have often framed the “reasonable expectation of privacy” in terms of the expectations of “most people.” See, e.g., Smith v. Maryland, 442 U.S. 735, 742 (1979) (holding that use of a pen register to capture the phone numbers dialed from a particular phone did not violate a reasonable expectation of privacy because “most people” are presumably aware that such a device can be used to aid in the identification of annoying callers).
prohibition on disclosure to such circumstances.\textsuperscript{337} Thus, the VPPA’s pre-enactment history provides unpersuasive, if not dubious, support for the court’s narrow reading.\textsuperscript{338}

Next, the court examined the statutory context, juxtaposing the VPPA’s definition of \textit{PII} with COPPA’s definition of that term.\textsuperscript{339} The court found it significant that, unlike the VPPA, COPPA authorizes the FTC to promulgate regulations that may extend the type of information included within the definition of \textit{PII}.\textsuperscript{340} Of particular significance to the court, the FTC promulgated rules expanding COPPA’s definition of \textit{PII} to include persistent identifiers, such as customer numbers, IP addresses, or any other information that enables the tracking and identification of a user.\textsuperscript{341} By contrast, the court observed, the VPPA’s definition of \textit{PII} does not include the built-in flexibility of authorizing the FTC to expand the definition “to keep pace with evolving technology.”\textsuperscript{342}

The court’s analysis of the statutory context, however, begs the question of whether the comparison of the definition of \textit{PII} between the VPPA and COPPA is instructive.\textsuperscript{343} As privacy scholars have noted, Congress’s definitions of \textit{PII} have taken different forms over the years, including COPPA’s “specific-types” approach and the VPPA’s “tautological” approach.\textsuperscript{344} The specific-types approach is a rule-based definition, which enumerates specific categories of information that are included within the definition.\textsuperscript{345} This approach has the potential to be restrictive because it requires the rule to be de-

\begin{thebibliography}{99}
\footnotesize
\item 337. See H.R. 4947, 100th Cong. § 2(a)(2) (1988); \textit{supra} notes 156–60.
\item 339. \textit{In re Nickelodeon}, 827 F.3d 262, 286–87 (3d Cir. 2016).
\item 341. \textit{Id.} at 287; see Children’s Online Privacy Protection Rule, 16 C.F.R. § 312.2 (defining “personal information” to include “[a] persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an [IP] address, a processor or device serial number, or unique device identifier”).
\item 342. \textit{In re Nickelodeon}, 827 F.3d at 287.
\item 343. See \textit{infra} notes 344–55 and accompanying text.
\item 344. See Schwartz & Solove, \textit{supra} note 56, at 1828–36 (discussing three predominant approaches to defining \textit{PII}, including the “tautological” approach, the “non-public” approach, and the “specific-types” approach, including the advantages and disadvantages of each approach).
\item 345. \textit{Id.} at 1831.
\end{thebibliography}
fined in advance, and only the types of information enumerated in the definition are included, making this approach susceptible to the risk of under-inclusion as a result of technological advances. On the other hand, the tautological approach is a standards-based definition, which has the advantage of being open-ended. Arguably, therefore, the decision to use an open-ended definition of PII in the VPPA may reflect an intention to provide broad protection of video privacy.

Finally, the court found it significant that Congress had an opportunity to expand the definition of PII when it amended the VPPA in 2013, but it chose not to do so. In the court’s view, this is a strong indication of Congress’s intent not to expand the VPPA’s definition of PII to include IP addresses, device identifiers, or browser fingerprints. Importantly, the court focused on the written testimony of the Electronic Privacy Information Center, recommending an amendment to the VPPA’s definition of privacy to include IP address and account identifiers. The Third Circuit suggests that the decision not to update the definition of PII confirms that Congress did not intend to include digital identifiers such as a user’s IP address within the scope of the VPPA’s definition of PII.

However, the court’s analysis overlooks the primary purpose of the amendment, which was apparently to enable streaming video companies, in-

346. Id. at 1835.
347. Id. at 1829.
348. See supra notes 346–47.
350. See id. at 288. Although it is true that Congress chose to leave the definition of PII intact, it is also true that Congress declined to change other antiquated language in the VPPA, including references to “video tape service provider” and “prerecorded video cassette tapes.” Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(a)(4) (2012). Moreover, the Third Circuit does not suggest that the VPPA’s protections extend only to the viewing of video cassette tapes, or that the VPPA’s definition should exclude all manner of digital identifiers relating specifically to Internet-based video transactions. See In re Nickelodeon, 827 F.3d at 281 n.119 (noting the issue of whether Google was a video tape service provider was not argued on appeal, and therefore there was no need for the court to address that issue); id. at 289 n.174 (citing In re Hulu II, No. C11–03764 LB, 2014 WL 1724344, at *5 (N.D. Cal. Apr. 28, 2014), and noting that numeric identifiers might qualify as PII in some circumstances under the VPPA).
351. Id. at 288; see VPPA 2012 Amendment Hearing, supra note 134, at 59–60 (statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center) (proposing that the VPPA’s definition of PII be amended to specifically include IP address and account identifiers).
352. In re Nickelodeon, 827 F.3d at 288–89.
cluding Netflix, to expand their businesses with social networking integration.\textsuperscript{353} To that end, the Congressional effort was narrowly crafted to update only the informed consent provision, and Congress was careful not to expand the scope of the amendment beyond that limited purpose.\textsuperscript{354} Therefore, it is reasonable to infer that Congress’s decision to leave the VPPA’s definition of PII intact reflected an acknowledgement that the definition was already sufficiently flexible to cope with evolving technology.\textsuperscript{355}

The court provides only minimal guidance for applying its ordinary person test to disclosures of information alleged to be PII.\textsuperscript{356} This guidance centers on an evaluation of the kind of information involved, rather than the context in which that information is used.\textsuperscript{357} First, the court suggests that the various kinds of information can be arranged on a spectrum, based on the likelihood that an ordinary person would be able to infer the identity of the data subject:\textsuperscript{358}

At one end of the spectrum . . . is a person’s actual name. Then there are pieces of information, such as a telephone number or a physical

\textsuperscript{353} See supra Section III.A.2 (examining the legislative history of the 2013 amendment to the VPPA’s informed consent provision).

\textsuperscript{354} See supra Section III.A.2. Efforts in the Senate to include amendments to another privacy statute were rejected, presumably to ensure quick passage of the amendment. See supra notes 177–78.

\textsuperscript{355} See supra text accompanying notes 344–54. Other courts to consider the effect of the 2013 amendment have rejected narrower interpretations based on Congress’s decision to change only the informed consent provision. See In re Vizio, Inc., Consumer Privacy Litig., 238 F. Supp. 3d 1204, 1225 (C.D. Cal. 2017) ("As the Supreme Court has instructed, this kind of [post-enactment legislative history (a contradiction in terms) is not a legitimate tool of statutory interpretation.") (alterations in original) (quoting Bruesewitz v. Wyeth LLC, 562 U.S. 223, 242 (2011)); Yershov v. Gamett Satellite Info. Network, Inc., 820 F.3d 482, 488 (1st Cir. 2016) ("Congress left untouched the definition of "consumer" in the statute, which we believe supports an inference that Congress understood its originally-provided definition to provide at least as much protection in the digital age as it provided in 1988.").

\textsuperscript{356} See infra text accompanying notes 357–63.

\textsuperscript{357} See In re Nickelodeon, 827 F.3d at 282–83 (delineating a spectrum of various kinds of information, ranked by the probability an ordinary person would be able to use that information to identify an individual).

\textsuperscript{358} Id. As noted above, the Third Circuit’s arrangement of the kinds information on a “spectrum” differs substantially from proposals by privacy scholars who advocate for a risk-based analysis. See supra note 258. Despite the similarities, the Third Circuit’s emphasis on what an “ordinary person” would be able to determine disregards important contextual information, which is important to an assessment of risk. See In re Nickelodeon, 827 F.3d at 282–83, 290; see also discussion infra Section IV.B (proposing a factor-based analysis for assessing the risk of identification).
address, which may not by themselves identify a particular person but from which it would likely be possible to identify a person by consulting publicly available sources, such as a phone book or property records. Further down the spectrum are pieces of information, like social security numbers, which are associated with individual persons but might not be easily matched to such persons without consulting another entity, such as a credit reporting agency or government bureau. The kind of information at issue here—static digital identifiers—falls even further down the spectrum.359

The court’s holding places the last category delineated on the spectrum beyond the scope of the VPPA’s definition of PII.360 It is unclear, however, whether a social security number or a state-issued driver’s license number would fall within the scope of PII as defined by the court.361 Although these numbers exist in government databases, an ordinary person would probably not be able to match these numbers to a person’s identity.362 On the other hand, the court suggests that some static digital identifiers “might” fall within the scope of the VPPA’s definition of PII, deferring such a determination to a later case.363 Thus, the contours of the court’s “ordinary person” test are not clearly defined.364

B. Factors for Determining PII under the VPPA

Through the enactment of the VPPA in 1988, and its amendment in 2013, Congress has recognized that information about the videos a person watches is deeply personal information that should be protected as private information.365 The VPPA’s open-ended definition of PII reflects an intention not to restrict the types of information that can be used to link the videos that a

360. See id. at 290 (holding that the static identifiers at issue here are “simply too hypothetical to support liability under the [VPPA]”).
361. Cf. supra notes 286–95 and accompanying text (discussing the First Circuit’s treatment of social security numbers).
362. See In re Nickelodeon, 827 F.3d at 282–83.
363. Id. at 289 n.174. The court’s admission that some static digital identifiers might qualify as PII within the meaning of the VPPA is confusing, given that the court has determined that Congress did not intend for the VPPA to protect against disclosure of static digital identifiers. See id. at 290.
364. See supra notes 356–63 and accompanying text.
365. See discussion supra Section III.A.
person has watched to that person’s identity.\textsuperscript{366} The evolution of technology has presented notable challenges to the concept of PII generally.\textsuperscript{367} Statutes, such as COPPA, that define PII to include specific kinds of data struggle to keep pace with technology, often requiring an amendment or regulatory rule change to adjust the definition of PII to ensure that privacy protections are not undermined by changes in technology.\textsuperscript{368} The VPPA’s definition, on the other hand, presents a different problem: whether policy objectives will be furthered by courts who grapple with factual circumstances involving unanticipated technological innovation.\textsuperscript{369} As the decisions of the First and Third Circuits demonstrate, the determination of what constitutes PII in a given case is not as straightforward as it might seem.\textsuperscript{370}

Rather than asking whether the disclosed information is of a 	extit{kind} that fits within the VPPA’s definition of PII, courts should instead consider the context in which the information is disclosed and evaluate the 	extit{risk} that a person’s identity will be revealed as a result of disclosing the information.\textsuperscript{371} Moreover, courts must be sensitive to evolving technical standards that may cause prior observations about a particular kind of information to be inadequate.\textsuperscript{372}

\textsuperscript{366} See discussion supra Section III.A.1.

\textsuperscript{367} See Schwartz & Solove, supra note 56, at 1836–48; Ohm, supra note 48, at 1716–31; see also discussion supra Section II.B.

\textsuperscript{368} See Schwartz & Solove, supra note 56, at 1834–35 (noting that despite the apparent flexibility provided by COPPA’s delegation of authority to expand the definition of PII to the FTC, the pace of technological development may still undermine the efficacy of this approach).

\textsuperscript{369} See id. at 1829 (observing that because the VPPA’s definition may be reduced to the proposition, “PII is PII,” “[i]t is unhelpful in distinguishing PII from non-PII”); see also In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 281 (3d Cir. 2016) (“What counts as PII under the [VPPA] is not entirely clear.”), cert. denied, 137 S. Ct. 624 (2017).

\textsuperscript{370} See discussion supra Sections IV.A.1–2.

\textsuperscript{371} See Ohm, supra note 48, at 1764–68 (advocating context-sensitive privacy regulation reform that focuses on the risks of privacy harm, and suggesting five factors that should be considered); Schwartz & Solove, supra note 56, at 1836 (“Whether information is identifiable to a person will depend upon context and cannot be determined \textit{a priori}.”); Nissenbaum, supra note 63, at 155 (“Whether a particular action is a violation of privacy is a function of several variables, including the nature of the situation, or context; the nature of the information in relation to that context; the roles of agents receiving information; their relationships to information subjects; on what terms the information is shared by the subject; and the terms of further dissemination.”).

\textsuperscript{372} See, e.g., A. Michael Froomkin, \textit{The Death of Privacy?}, 52 STAN. L. REV. 1461, 1491 (2000) (discussing differences between the newer IPv6 IP address standard and the older IPv4 standard, and suggesting that the newer standard makes it easier to track individuals). Because the IPv6 standard incorporates elements unique to the user’s device, each IP address is globally unique and traceable over the device’s lifetime. Johanna Ulrich & Edgar Weippl, \textit{Privacy Is Not an Option: Attacking the IPv6 Privacy Extension}, in \textit{Research in Attacks, Intrusions, and Defenses}: 18th INT’L SYMP.
The VPPA’s open-ended definition means that courts may exercise discretion in determining which factors best effectuate the Statute’s underlying policy.\textsuperscript{373}

Although the First Circuit’s analysis implicitly takes some contextual factors into consideration, it does not separately analyze the various kinds of information that it confronted in its opinion.\textsuperscript{374} Additionally, it does not take into consideration other factors that would be relevant and helpful to subsequent courts to confront this issue; in particular, there is apparently no consideration of the incentives of the recipient to identify the data subject, or whether the recipient is likely to store or share the data.\textsuperscript{375} Subsequent courts confronting novel circumstances, therefore, may struggle to determine whether it is “reasonably and foreseeably likely” that a particular piece of information would be used to link video transactions to a specific person.\textsuperscript{376}

In evaluating whether information is PII within the meaning of the VPPA, courts should consider the totality of the circumstances, using the following factors to assess the risk that disclosure of such information would be used to identify a specific person: (1) the likelihood that the recipient of the information is capable of linking it to a specific person,\textsuperscript{377} (2) the extent to which the recipient of the information has access to additional information that can be used to identify the data subject;\textsuperscript{378} (3) the degree to which the information

\begin{itemize}
  \item See Schwartz & Solove, supra note 56, at 1870 (suggesting that because the VPPA’s definition of PII is a standard, the decision maker is permitted to exercise some “freedom in deciding which factors to take into account”).
  \item See discussion supra Section IV.A.1 (noting the ambiguity in the court’s decision as to whether the unique mobile device identifier alone, the GPS coordinates alone, or the combination of these in the disclosure constituted PII within the meaning of the VPPA).
  \item See Yershov v. Garnett Satellite Info. Network, Inc., 820 F.3d 482, 486 (1st Cir. 2016) (concluding that it was foreseeable to the defendant that the disclosed information could be used to identify specific individuals based solely on the accessibility of information that would enable such an identification to be made); discussion supra Section IV.A.1.
  \item See Yershov, 820 F.3d at 486; see, e.g., In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 289 (3d Cir. 2016) (interpreting Yershov to mean that GPS coordinates, but not unique mobile device identifiers, were PII within the meaning of the VPPA), cert. denied, 137 S. Ct. 624 (2017).
  \item See discussion infra Section IV.B.1.
  \item See discussion infra Section IV.B.2.
\end{itemize}
disclosed is unique or can be tied to a singular data subject,\textsuperscript{379} (4) whether the disclosed information is likely to be stored, and if so, the length of time that it will be stored;\textsuperscript{380} (5) whether the recipient of the information has an incentive to link that information to a specific person;\textsuperscript{381} and (6) whether the recipient of the information is likely to share the information with another party with the means or incentive to identify specific individuals.\textsuperscript{382} Upon finding a significant risk of identification, courts should then assess whether this risk was foreseeable, based on what the video service provider knew, or should have known, at the time of the disclosure.\textsuperscript{383}

1. Capability to Link Information to an Identified Individual

The recipient’s capability to link the disclosed information to an identified individual is a key factor that courts should consider in evaluating the risk of identification.\textsuperscript{384} Importantly, this factor focuses on the recipient’s capability, rather than on whether the information was actually linked to an identified individual.\textsuperscript{385} Google’s privacy policy, for instance, makes clear that Google collects unique device identifiers of its users and may associate them with a user’s Google account.\textsuperscript{386} Thus, Google has an apparent capability to recognize the identity of its users on the basis of such unique device identifiers.\textsuperscript{387} If a person were to watch a video on a mobile application that transmits the unique device identifier in conjunction with the title of the video to Google, then this factor would weigh in favor of finding that PII had been disclosed.\textsuperscript{388}

\begin{flushleft}
\textsuperscript{379} See discussion infra Section IV.B.3.
\textsuperscript{380} See discussion infra Section IV.B.4.
\textsuperscript{381} See discussion infra Section IV.B.5.
\textsuperscript{382} See discussion infra Section IV.B.6.
\textsuperscript{383} See Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 486 (1st Cir. 2016) (suggesting that no liability under the VPAA should attach where the ability to link information to identity is “too uncertain, or too dependent on too much yet-to-be-done, or unforeseeable detective work”).
\textsuperscript{384} See Schwartz & Solove, supra note 56, at 1877–78 (noting the importance of considering the means likely to be used to link information to identity in assessing the risk of identification); supra note 295 and accompanying text.
\textsuperscript{385} See infra notes 386–88.
\textsuperscript{387} See id.
\textsuperscript{388} See supra notes 303–07 and accompanying text.
\end{flushleft}
2. Availability of Additional Information Identifying an Individual

Access to additional information about a data subject weighs in favor of finding that the disclosed information is PII, if the additional information is sufficient to infer the identity of the individual. The additional information may be in the form of a publicly accessible database or website, a private data source to which the recipient of the disclosure has access, or a public record. In In re Hulu II, for example, defendant video provider Hulu disclosed information about the videos its users watched and their Hulu User IDs. At the time of the disclosure, publicly accessible user profiles on the Hulu website contained the first and last name of the user. Anyone in possession of a person’s Hulu User ID would be able to access the user’s profile page on the Hulu website to discover the first and last name of the person who had watched the video. Similarly, disclosure of demographic information that can be correlated with information in the public record may carry some risk of identification, particularly if the demographic information at issue is highly unique. On the other hand, lack of accessibility would lower the risk of identification. For example, unique personal identifiers contained in a set-top cable converter box, which are only decipherable with information contained in the cable company’s billing system, would carry a low risk of identification under this factor if there is no third-party access to information in

389. See Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 486 (1st Cir. 2016) (suggesting that access to additional information by the person to whom information was disclosed is an important consideration in determining whether the disclosed information identifies a specific individual); Schwartz & Solove, supra note 56, at 1878 (suggesting that access to additional data is a key factor in assessing the risk of identification); see also supra Part IV.A.1; cf. In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 290 (3d Cir. 2016), cert. denied, 137 S. Ct. 624 (2017) (suggesting that access to information by an ordinary person, rather than the person to whom the information has been disclosed, is a determining factor).

390. See infra notes 391–94 and accompanying text.


392. Id. at *4.

393. Id.

394. See Sweeney, supra note 92, at 2 (concluding that few characteristics are required to identify individuals based on demographic data). The ability to identify a data subject based on demographic information is correlated with the degree to which that data is unique. Id.; see infra Section IV.B.3. Importantly, the uniqueness of the data is of little consequence if it cannot be combined with additional information that identifies an individual. See Sweeney, supra note 92, at 3–4 (discussing the availability of patient discharge data, and suggesting that some states do not provide the data to the same extent as others).

395. See infra note 396 and accompanying text.
that billing system.\textsuperscript{396}

3. Uniqueness of the Information Disclosed

If the disclosed information has a high degree of uniqueness, then this factor weighs in favor of finding an increased risk of identification.\textsuperscript{397} Unique identifiers, including social security numbers and state driver license numbers, uniquely identify a person and occupy one end of the spectrum.\textsuperscript{398} At the opposite end of the spectrum is information that does not describe anyone in particular, such as information about the general characteristics of a computer or high-level demographic information.\textsuperscript{399} Browser fingerprints and combinations of demographic data are somewhere in between.\textsuperscript{400} For example, the combination of ZIP code, date of birth, and gender is sufficiently unique to identify 87\% of the population; therefore, this combination carries a higher risk of identification, for example, than disclosure of the combination of a person’s county, date of birth, and gender, which uniquely identifies approximately 18\% of the population.\textsuperscript{401}

4. Length of Time Information Will Be Stored

The length of time that information is stored increases the likelihood that the information can be used to identify an individual.\textsuperscript{402} Length of storage

\textsuperscript{396} See Pruitt v. Comcast Cable Holdings, 100 F. App’x 713, 716–17 (10th Cir. 2004) (holding that unique subscriber codes in set-top cable boxes were not PII, since the identity of the subscriber could not be determined without information from the cable company’s billing system).

\textsuperscript{397} See Sweeney, supra note 92, at 34 (discussing the ability to combine non-personal data to create sufficiently unique combinations that can be used to reliably identify a data subject).

\textsuperscript{398} See supra notes 286–301 and accompanying text.

\textsuperscript{399} See, e.g., In re Nickelodeon I, MDL No. 2443 (SRC), 2014 WL 3012873, at *11 (D.N.J. 2014) (“Knowing anonymized information about a computer, and an IP address associated with that computer, will not link actual people . . . to their specific video choices, any more than knowing that an [o]pinion was written on an HP Compaq running Windows XP located at a Philadelphia IP address will link an actual judge to a specific case.”); supra note 74.

\textsuperscript{400} See supra Section II.B.1–2.

\textsuperscript{401} See Sweeney, supra note 92, at 2.

\textsuperscript{402} See Schwartz & Solove, supra note 56, at 1878 (suggesting that the lifetime of stored data is an essential factor in determining the risk of identification); Ohm, supra note 48, at 1766–67 (arguing that quantity of stored data, including the length of time the data is retained, is an important factor in determining the risk of identification).
time may also be correlated with the overall quantity of data collected. Additionally, if information is stored for a prolonged period of time, advances in technology or emerging needs may increase the likelihood of identification. Thus, the greater the time that the information will be stored, the greater the risk that a data subject will be identified.

5. Incentives to Identify an Individual

When the recipient of information has an incentive to identify the data subjects referenced in the disclosed data, there is an increased risk that an identification will be made. Advertisers have an incentive to gather as much information as possible about their audience, but they may be more interested in people’s behavioral characteristics than in their actual identity. By contrast, data about identified individuals is more valuable than anonymous data to commercial data brokers, who therefore have much stronger incentives to identify individual data subjects in the data they collect. Where anonymized demographic data are shared for a specified limited purpose, then an agreement between the parties to so limit the use of that data may weigh in favor of a decreased risk of identification, insofar as such an agreement reduces the recipient’s incentive to identify individual data subjects.

404. See, e.g., Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 NW. J. TECH. & INTELL. PROP. 239, 259–60 (2013) (discussing “data minimization,” or the requirement for organizations to maintain the minimum amount of data necessary to “obtain their legitimate goals,” as a fundamental principle aimed at preserving personal privacy). Big data carries with it notable incentives to find “unanticipated secondary uses” of the data, increasing the privacy risks associated with that data. Id. at 259.
406. See Schwartz & Solove, supra note 56, at 1878 (suggesting that in assessing the risk of identification, the incentive of the person to whom data has been disclosed should be taken into consideration); Ohm, supra note 48, at 1767 (recommending that regulators weigh economic incentives in the risk assessment analysis).
407. See Tene & Polonetsky, supra note 404, at 249.
408. See Solove & Hoofnagle, supra note 294, at 362 (discussing commercial data brokers who profit by selling data to marketers and government agencies, as well as for use in background checks and credit reporting purposes).
6. Likelihood That the Data Will Be Further Shared or Disclosed

Each additional party who comes into contact with disclosed information acts as a “force multiplier,” substantially increasing the risk of identification. Thus, when information is disclosed in a manner that makes it likely that additional parties will receive and analyze the data, then this factor weighs in favor of finding an increased risk of identification. Public data releases, such as the AOL search query release, represent the highest level of risk because there is no limit to who will be able to access the data or for what purpose.

V. IMPACT AND SIGNIFICANCE OF THE RECENT VPPA DECISIONS

The split in authority that has emerged concerning the VPPA’s definition of PII highlights the difficult challenges that the evolution of technology has created within the context of American privacy law generally. Because liability under the VPPA is triggered only upon disclosure of PII, the way courts...
interpret this concept necessarily impacts the privacy interests of all Americans, as well as the responsibilities held by commercial enterprises. The privacy harm that results from a disclosure may not be immediately apparent, but may surface over time and endure for many years following the disclosure. Although Congress has sought to prevent such harms through enactment of privacy protection statutes like the VPPA, these preventive measures are undermined when courts construe PII too narrowly. In addition, the uncertainty created by these decisions may hamper innovation or increase costs unnecessarily.

A. Recent Decisions Undermine Privacy Interests and Create Uncertainty

The decisions of the Third and Ninth Circuits and a majority of the district courts that have construed PII narrowly undermine an important privacy interest. In some instances, the courts have underestimated the ability of companies who employ sophisticated data collection and aggregation techniques

---

414. See Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(b)(1) (2012); John E. Calfee & Richard Craswell, Some Effects of Uncertainty on Compliance with Legal Standards, 70 VA. L. REV. 965, 966 (1984) ("If the legal standard is uncertain, even actors who behave 'optimally'... will face some chance of being held liable because of the unpredictability of the legal rule. More important, these actors can usually reduce that chance [of being held liable]... by... modifying their behavior beyond the point that would be socially optimal.");


416. See Schwartz & Solove, supra note 56, at 1854–55 (discussing attempts by behavior marketing companies to circumvent privacy regulations by taking advantage of narrow definitions of PII to collect and use “non-PII” as a surrogate for protected data).

417. See infra notes 426–29 and accompanying text.

418. See Hearings on Nomination of Robert H. Bork to be Associate Justice of the Supreme Court of the United States Before the S. Comm. on the Judiciary, 100th Cong., 1st Sess., pt. 3, at 2821 (Sept. 28, 1987) (statement of Sen. Patrick J. Leahy, Member, S. Comm. on the Judiciary) ("[Privacy] is not a conservative or a liberal or moderate issue. It is an issue that goes to the deepest yearnings of all Americans that we are here and we cherish our freedom and we want our freedom."); supra note 145.
to link “anonymous” data with an identified individual’s profile,419 and in
other cases, the courts have simply disregarded this possibility.420 Thus, video
privacy protections in the context of Internet video distribution have been sig-
nificantly eroded.421 despite the VPPA’s legislative history suggesting that
Congress intended the Statute’s definition of PII to apply broadly to any
information capable of identifying individuals and their video selections.422

One aim of privacy protection statutes like the VPPA is to prevent privacy
harm by disincentivizing a course of action that is likely to cause such harm.423
Thus, under the VPPA, video service providers are given notice that they are
prohibited from disclosing information that links a customer’s identity to the
customer’s video transactions.424 But not only do the recent VPPA decisions
undermine this disincentive, but the decisions also create uncertainty for the
video service provider.425

These differing tests for evaluating PII represent an inconsistency in the

419. See, e.g., In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 290 (3d Cir. 2016)
(“That Google will assemble otherwise anonymous pieces of data to unmask the identity of individ-
ual children is . . . simply too hypothetical to support liability under the [VPPA].” (emphasis added)),
cert. denied, 137 S. Ct. 624 (2017). But see Google Privacy Policy, supra note 386 (“We collect
device-specific information (such as your hardware model, operating system version, unique device
identifiers, and mobile network information including phone number). Google may associate your
device identifiers or phone number with your Google Account.”).
420. See, e.g., Robinson v. Disney Online, 152 F. Supp. 3d 176, 182 (S.D.N.Y. 2015) (“[PII] is the
information . . . which must itself do the identifying . . . not information disclosed by a provider, plus
other pieces of information collected elsewhere by non-defendant third parties.”); see also Eichen-
berger v. ESPN, Inc., 876 F.3d 979, 985 (9th Cir. 2017) (acknowledging that online marketing and
analytics companies may be able to match device identifiers to consumer identities, but declining to
extend the VPPA’s definition of PII “to cover circumstances so different from the ones that motivated
its passage”).
421. See supra notes 419–20 and accompanying text. Despite the accuracy with which big data
analytics may be used to identify individuals, companies engaged in behavior targeting may circum-
vent privacy protections by claiming that the information they collect is not PII. See Schwartz &
Solove, supra note 56, at 1818.
422. See supra Section III.A.
423. See Ohm, supra note 48, at 1734 (noting that in enacting privacy laws beginning in the 1970s,
Congress sought to reduce the risk of harm associated with collection and dissemination of personal
information).
425. See In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 290 (3d Cir. 2016) (“Our deci-
sion necessarily leaves some unanswered questions about what kinds of disclosures violate the
[VPPA]. Such uncertainty is ultimately a consequence of our common-law system . . . and the rapid
evolution of contemporary technology.”), cert. denied, 137 S. Ct. 624 (2017); infra notes 426–29 and
accompanying text.
law that creates difficulty for businesses who must comply with it.\textsuperscript{426} When the legal standard is unclear, businesses are unable to perform an accurate self-assessment of compliance with the legal requirement.\textsuperscript{427} This may induce over-compliance with the effect of either increasing costs unnecessarily or stifling innovation.\textsuperscript{428} On the other hand, there is also a possibility of under-compliance, with the attendant risk of high damage awards.\textsuperscript{429}

B. Recent Decisions Highlight the Need for Forward-Looking Privacy Regulations

Despite Congressional intent to protect the reasonable privacy interests of consumers without overburdening commerce in a way that “keep[s] up to date with changing technology,”\textsuperscript{430} the reality is that lawmakers are unable to keep pace with the rapid advances of technology.\textsuperscript{431} Privacy protection statutes thus may convey seemingly “antiquated” conceptions of the risk associated with activities to which the statute was meant to apply.\textsuperscript{432} When the VPPA was enacted in 1988, Congress was deeply concerned about the harmful effects that disclosure of the video-watching activity might have, not only with respect to the intellectual development of the individual, but also with respect to the impact on the foundations of our democracy.\textsuperscript{433} These concerns transcend the modes of information disclosure that were foreseeable in 1988.\textsuperscript{434}

\textsuperscript{426} See infra text accompanying notes 427–29.
\textsuperscript{427} See Calfee & Craswell, supra note 414, at 966.
\textsuperscript{428} Id.
\textsuperscript{429} Id.
\textsuperscript{430} Joint Hearing on H.R. 4947 and S. 2361, supra note 140, at 19 (statement of Rep. Robert W. Kastenmeier, Chairman, Subcomm. on Courts, Civil Liberties & the Admin. of Justice of the H. Comm. on the Judiciary).
\textsuperscript{431} See VPPA 2012 Amendment Hearing, supra note 134, at 8 (statement of Sen. Patrick J. Leahy, Chairman, S. Comm. on the Judiciary) (“Today the social networking, video streaming, the cloud, mobile apps, and other new technologies have revolutionized the availability of Americans’ information. But they are also outpacing our privacy laws.”).
\textsuperscript{432} See id. at 4 (statement of Sen. Tom Coburn, Member, Subcomm. on Privacy, Technology, and the Law of the S. Comm. on the Judiciary) (characterizing the VPPA as “antiquated,” considering “all the new technology that is out there”).
\textsuperscript{433} See S. REP. NO. 100-599, at 6–8 (1988) (noting the importance of books and films to the intellectual development of individuals, and the chilling effect on the pursuit of ideas outside the mainstream that can result when privacy in these materials is not protected).
\textsuperscript{434} See, e.g., Susan W. Brenner, The Privacy Privilege: Law Enforcement, Technology, and the Constitution, 7 U. FLA. J. TECH. & POL‘Y 123, 161 (2002) (“The reality [is] that privacy is a construct which must transcend the methodological differences between the real world as it existed when
Thus, if deeply personal information, such as the titles of videos a person watches, is to be protected, the courts must analyze alleged disclosure of PII by taking into consideration the contextual factors relevant to assessing the probable risk of privacy harm.\(^{435}\)

Because the Congressional approach to privacy protection has been to enact statutes that address privacy concerns within specific contexts, the VPPA decisions are unlikely to directly impact broader privacy concerns under the current regulatory scheme.\(^{436}\) Although PII, as a general concept, is prevalent in every privacy protection statute enacted since the early 1970s, each statute defines PII uniquely within the context of the privacy interest that the statute was enacted to protect.\(^{437}\) Thus, analysis of what constitutes PII in the context of the VPPA is unlikely to provide direct assistance to courts confronting PII issues in other areas.\(^{438}\)

Nevertheless, the circuit split that has emerged over the definition of PII within the meaning of the VPPA underscores the need for forward-looking privacy law reforms.\(^{439}\) Congress must eventually confront the question of whether PII, as a central concept of American privacy protection law, remains a useful construct in light of advancements in the ability to identify individuals using a plethora of data not traditionally included within the definition of PII.\(^{440}\) Whether or not PII retains its central place in information privacy law, it is clear that for privacy protection statutes to be effective, a clear statement of the interests to be protected, as well as an assessment of the factors relevant to determining the risks of privacy harm to be avoided, must be taken into account.\(^{441}\) The PII approach to privacy protection, despite its flaws, has the

---

\(^{435}\) See discussion supra Section IV.B.

\(^{436}\) See, e.g., In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 286–89 (3d Cir. 2016) (noting the separate evolution of PII under COPPA and VPPA, and declining to apply recent changes in COPPA’s regulatory rule to the VPPA context), cert. denied, 137 S. Ct. 624 (2017).

\(^{437}\) See discussion supra Section II.A.

\(^{438}\) See supra text accompanying notes 436–37.

\(^{439}\) See, e.g., Ohm, supra note 48, at 1742–43 (describing the problem resulting from the interaction of advances in technology and PII as a “whack-a-mole” game, and advocating for an end to PII-based regulatory schemes); see also discussion supra Section IV.A.

\(^{440}\) See, e.g., Ohm, supra note 48, at 1742 (noting that protecting PII only as it is defined by our laws and regulations leads to inadequate protections of privacy, due to the “ever-expanding” categories of information that computer scientists have used to identify specific individuals); see Section II.B.2.

\(^{441}\) See sources cited supra note 63. Despite the apparent disagreement between privacy scholars over whether the concept of PII should be abandoned or revamped, most of those to examine the issue
potential to be an effective way of protecting information privacy, but only if contextual factors are taken into account. But simply providing an open-ended, tautological definition of PII cannot suffice; nor can an enumeration of the specific types of information that constitute PII.

Historically, however, Congress has been slow to act on calls for privacy law reform. And when it does amend privacy legislation, the effort is often incomplete—as evidenced by the VPPA’s amendment in 2013.

C. Absent Congressional Action, Courts Should Adopt a Factor-Based Test

The Supreme Court’s denial of certiorari in In re Nickelodeon provides an opportunity for the lower courts to study the issue further to refine competing rules. Thus, the courts may ultimately advance an approach that more clearly assesses PII within the context of Internet video streaming. Given the VPPA’s open-ended definition of PII and a legislative history that supports a contextual approach to defining PII, there is much support for—and

have recommended a contextual approach. See, e.g., Chung, supra note 63, at 414–16 (advocating use of contextual privacy regulations in the area of behavioral targeting); Schwartz & Solove, supra note 56, at 1872–79 (advocating a PII revamp incorporating assessment of contextual factors); Ohm, supra note 48, at 1764–69 (advocating contextual factors for assessing risk of re-identification in public and private data releases); see generally HELEN FAY NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 140–47 (2009) (arguing that privacy must be understood in its social context, through a framework that the author calls “contextual integrity”).

442. See Schwartz & Solove, supra note 56, at 1872–79 (advancing a framework for using contextual factors to classify information on a continuum based on risk of identification); supra Section IV.B.

443. See Schwartz & Solove, supra note 56, at 1828–35 (discussing the inadequacies of the current approaches to PII).


445. See supra notes 349–52.


447. See Amanda Frost, Overvaluing Uniformity, 94 VA. L. REV. 1567, 1578 (2008) (“The courts of appeals are generally hesitant to depart from precedent set in other jurisdictions, despite being under no obligation to adhere to decisions by sister circuits.”). Since the Supreme Court will not take up this issue, courts that have not yet considered PII within the VPPA’s meaning may have an opportunity to genuinely consider alternative approaches. See id. at 1630 (noting that arriving at the correct statutory interpretation may be more important than uniformity of interpretation).

448. See discussion supra Section IV.B.
no statutory barriers preventing—such an approach.\textsuperscript{449} Indeed, the First Circuit's decision in \textit{Yershov}\textsuperscript{450} is, at its core, a determination based on consideration of contextual factors.\textsuperscript{451}

Both the First and Third Circuits acknowledge that there is a point at which the linkage between seemingly anonymous digital identifiers and an identifiable individual becomes so far attenuated as to present little to no risk of identification.\textsuperscript{452} The courts differ not only with respect to where that point is,\textsuperscript{453} but also as to its determination.\textsuperscript{454} The tests adopted by each court are guided by implicit factors, with little guidance as to how future courts should apply them to novel circumstances.\textsuperscript{455}

Courts that confront this issue in the future should, therefore, take an opportunity to advance a factor-based analysis of the context in which information was disclosed when deciding whether such information constitutes PII within the meaning of the VPPA.\textsuperscript{456} Identification of these factors can help to advance the law toward a resolution of the issues confronting American privacy law insofar as the concept of PII is concerned.\textsuperscript{457}

\begin{itemize}
\item[449.] \textit{See} discussion \textit{supra} Section III.A.
\item[450.] \textit{Yershov} v. \textit{Gannett Satellite Info. Network, Inc.}, 820 F.3d 482, 484 (1st Cir. 2016).
\item[451.] \textit{See} discussion \textit{supra} Section IV.A.1.
\item[452.] \textit{In re Nickelodeon}, 827 F.3d at 290; \textit{Yershov} v. \textit{Gannett Satellite Information Network, Inc.}, 820 F.3d 482, 486 (1st Cir. 2016).
\item[453.] \textit{Compare} \textit{In re Nickelodeon}, 827 F.3d at 290 (holding that a unique mobile device identifier was not PII within the meaning of the VPPA), \textit{with} \textit{Yershov}, 820 F.3d at 486 (holding that a unique mobile device identifier was PII within the meaning of the VPPA).
\item[454.] \textit{Compare} \textit{In re Nickelodeon}, 827 F.3d at 290 (ruling that PII within the meaning of the VPPA is "the kind of information that would readily permit an ordinary person to identify a specific individual’s video-watching behavior"), \textit{with} \textit{Yershov}, 820 F.3d at 486 (ruling that PII within the meaning of the VPPA is information that is "reasonably and foreseeably likely" to identify a specific individual's video-viewing activities).
\item[455.] \textit{See} discussion \textit{supra} Section IV.A. The First Circuit's test, for example, considers whether the party to whom the information has been disclosed is likely to be in possession of (or have access to) data such that the combination of information would facilitate identification. \textit{See} discussion \textit{supra} Section IV.A.1. The Third Circuit's test, on the other hand, considers whether the information disclosed is the kind of information that directly identifies a specific person, or whether required additional information is so publicly available that an ordinary person would be able to combine it with the disclosed information to determine a specific individual's identity. \textit{See} discussion \textit{supra} Section IV.A.2.
\item[456.] \textit{See} discussion \textit{supra} Section IV.B.
\item[457.] \textit{See} discussion \textit{supra} Section IV.B.
\end{itemize}
VI. CONCLUSION

Advances in technology over the past two decades have blurred the boundaries of PII.458 But the drafters of the VPPA were certainly aware of the dangers to privacy that frequently accompany technological innovation.459 The VPPA’s open-ended definition of PII reflects Congress’s intent for the Statute to “keep up to date with changing technology and changing social patterns with respect to the use of materials which ought to be clearly private.”460

Nevertheless, the VPPA’s recent jurisprudence illustrates the great difficulty courts encounter as they grapple with the concept of PII in an age of ubiquitous data aggregators and big data analytics.461 Because the central aim of information privacy protection statutes like the VPPA is to recognize and enforce one’s right to control information about oneself,462 the degree to which such laws are effective in achieving that goal depends substantially on how the contours of PII are defined.463 Privacy protection statutes protect our personal information and provide us with some measure of control over the collection, storage, processing, disclosure, and use of that information.464 But when information is deemed non-PII, the individual’s right to control that information—if such a right exists at all—is substantially diminished.465

The factor-based analysis proposed by this Comment represents a clear and practical approach to evaluating whether information is PII within the meaning of the VPPA,466 in a manner that is sensitive to Congress’s intent “to preserve personal privacy with respect to the rental, purchase, or delivery of

458. See discussion supra Section II.B.
459. See discussion supra Section III.A.
461. See discussion supra Sections III.C–D, IV.A.
462. See S. REP. NO. 100-599, at 2 (1988) (“The [VPPA] follows a long line of statutes passed by the Congress to extend privacy protection to records that contain information about individuals.”); supra notes 37–51 and accompanying text.
463. See discussion supra Section IV.A.
464. See supra notes 37–51 and accompanying text.
465. See supra note 65 and accompanying text; see also DHEW REPORT, supra note 49, at 40 (“[The data subject’s] opportunity to participate in [decisions about records containing the data subject’s personal information] depends on the willingness of the record-keeping organization to let him participate and, in a few instances, on specific rights provided by law.”).
466. See discussion supra Section IV.B.
video tapes or similar audio visual materials.\textsuperscript{467} Expanding on the approach articulated in \textit{Yershov}, the proposed test examines the context in which the purported personal information was disclosed.\textsuperscript{468} Drawing on the work of privacy scholars who have advanced alternative approaches to the PII problem, the proposed test suggests factors that are aimed at assessing the risk of identification.\textsuperscript{469}

American federal privacy law in general has been criticized for its failure to protect personal privacy interests on the Internet, and there have been many calls for reform, particularly with respect to its predominant focus on narrow protections of PII.\textsuperscript{470} The split in authority over PII within the meaning of the VPPA provides a unique opportunity to focus on and refine a central concept of privacy law, because it touches on activities that are directly impacted by technological innovation.\textsuperscript{471} Moreover, the Statute’s open-ended definition and legislative history promote adaptation to new technology.\textsuperscript{472} The VPPA’s success or failure with respect to preserving personal privacy interests in an Internet context can help to inform efforts to reform privacy law in general.\textsuperscript{473}

Daniel L. Macioce, Jr.*

\textsuperscript{467} S. REP. NO. 100-599, at 1.
\textsuperscript{468} See discussion supra Section IV.B.
\textsuperscript{469} See discussion supra Section IV.B.
\textsuperscript{470} See, e.g., Schwartz & Solove, supra note 77 (proposing a new concept of PII in the context of reforming privacy law in the United States and European Union); Ohm, supra note 48, at 1742–43 (calling for an end to the reliance concept of PII for the purposes of determining what information should be protected); see also Elizabeth D. De Armond, \textit{A Death of Remedies}, 113 PENN ST. L. REV. 1, 52 (2008) (arguing that states should exercise their full lawmaking capacities to protect the privacy of their citizens, given the inefficacy of federal law to provide real privacy protection); Solove & Iooftage, supra note 294, at 357 (recommending specific reforms aimed at incorporating FIPs into privacy regulation).
\textsuperscript{471} See supra notes 446–57 and accompanying text.
\textsuperscript{472} See discussion supra Section III.A.
\textsuperscript{473} See discussion supra Section II.A. Although the scope of information considered to be PII may vary depending on the way PII is defined in each privacy protection statute, see Schwartz & Solove, supra note 77, at 888, jurisprudence relating to the concept of PII makes clear that relevant analysis from other areas of law may be incorporated by analogy where ambiguity exists. See \textit{In re Hulu II}, No. C11–03764 LB, 2014 WL 1724344, at *9–11 (N.D. Cal. Apr. 28, 2014) (relying to some extent on jurisprudence relating to identifying information in the contexts of copyright law, the Freedom of Information Act, and the Cable Communications Act for its understanding of PII within the meaning of the VPPA).

* J.D. Candidate, Pepperdine University School of Law; B.A. in English, University of California, Los Angeles. The author thanks his wife Faye and his son William for their abiding love and
encouragement. The author also thanks the members of the Pepperdine Law Review for their assistance throughout the editorial process.