Maine Law Review

Volume 69 | Number 2 Article 4

August 2017

Yershov v. Gannett: Rethinking the VPPA in the 21st Century

Ariel A. Pardee
University of Maine School of Law

YERSHOV V. GANNETT: RETHINKING THE VPPA IN THE 21ST CENTURY

Ariel Pardee

YERSHOV V. GANNETT: RETHINKING THE VPPA IN THE 21ST CENTURY

*Ariel Pardee**

I. INTRODUCTION

Information privacy in the twenty-first century is a slippery concept. It exists in the shadows of technology, peeking out in companies' privacy policies, or being dragged out by the media after a data breach or a new technology oversteps consumers' personal privacy boundaries.[1] The collection of personal information from mobile devices by mobile applications has also generated significant concerns for some users. What information are these companies collecting? What are they doing with it? With whom are they sharing it? Much of the controversy stems from the practice of interest-based advertising.

While interest-based advertising is not a new phenomenon, modern technology coupled with advanced data collection techniques and data analysis methods have shaped the practice into an exponentially more sophisticated—and ubiquitous—industry than it was before.[2] From the standpoint of some mobile users the practice feels tantamount to being constantly surveilled,[3] while other users seem to understand that part of conducting one's affairs online means, in many cases, one's informational data is going *somewhere*.[4] For better or worse, only limited guidance for the practice has been provided by federal legislation or regulation.[5] In particular, the agency charged with "protecting America's consumers," the Federal Trade Commission ("FTC"), has promulgated almost no regulations that restrict or control the collection and disclosure of mobile device data by private companies.[6] As a

---

* J.D. Candidate, University of Maine School of Law, Class of 2018. The Author thanks Professor Peter Guffin for his time and guidance in helping her navigate the nuances of Information Privacy Law.

1. *See, e.g.*, Nicole Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, N.Y. TIMES, (Sept. 22, 2016), http://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html?action=click&contentCollection=Technology&module=RelatedCoverage&region=Marginalia&pgtype=article; Herb Wisebaum, *'Hell No Barbie': Social Media Campaign Targets Talking Doll*, NBC NEWS, (Nov. 9, 2015, 1:20 PM), http://www.nbcnews.com/business/consumer/hell-no-barbie-social-media-campaign-targets-talking-doll-n459936.

2. *See* CRAIG DEMPSTER & JOHN LEE, THE RISE OF THE PLATFORM MARKETER: PERFORMANCE MARKETING WITH GOOGLE, FACEBOOK AND TWITTER, PLUS THE LATEST HIGH-GROWTH DIGITAL ADVERTISING PLATFORMS 2-3 (2015); *see also* Shea Bennett, *The Evolution of Marketing Data—From Direct Mail to Twitter (1960-2012)*, ADWEEK: SOCIALTIMES, (July 3, 2013, 3:00PM), http://www.adweek.com/socialtimes/marketing-data-history/487271.

3. *See* Natasha Singer, *Sharing Data but Not Happily*, N.Y. TIMES (June 4, 2015), http://www.nytimes.com/2015/06/05/technology/consumers-conflicted-over-data-mining-policies-report-finds.html.

4. *Id.*

5. Despite the introduction of multiple over-arching data protection laws, Congress has only managed to enact one, the *Children's Online Privacy Protection Act*, which specifically regulates the collection of data by online companies designed to serve children. 15 U.S.C. §§ 6501-6506 (2012).

6. FEDERAL TRADE COMMISSION, https://www.ftc.gov/ (last visited Jan. 24, 2017). The FTC specifically regulates the collection and disclosure of data in the Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2013). Excluding COPPA, the FTC does not regulate the general collection and disclosure of data by ad tech companies, but instead relies on existing regulations prohibiting unfair trade and deceptive practices, such as when a company violates its own stated privacy policy. *See* Jennifer

result, some disconcerted mobile device users have asked courts to interrupt the practice using the only means available to them: arguably outdated privacy laws written long before the information age went mobile.

Yershov v. Gannett is just such a case.[7] Plaintiff Alexander Yershov asked the United States District Court for the District of Massachusetts, and later the First Circuit Court of Appeals, to find defendant Gannett Satellite Information Systems, Inc. ("Gannett"), the owner of the *USA Today Mobile App*, in violation of a law written long before mobile applications—or mobile internet technology in general—became mainstream.[8] The 1988 law, called the Video Privacy Protection Act ("VPPA" or "the Act"), was originally enacted to prohibit individuals' video cassette rental histories from being disclosed to third parties.[9] In deciding Gannett's motion to dismiss the claim, both the district court and the First Circuit were tasked with deciding whether to interpret two definitions within the Act so broadly that: (1) certain data collected from a mobile application on a smartphone would fall within the statutory definition of "personally identifiable information"; and (2) whether the use of a free downloaded mobile application would make a user a "consumer," within the meaning of the statute.[10] The district court found that while the data was personally identifiable information, Yershov was not a consumer under the VPPA definition, and subsequently granted Gannett's motion to dismiss.[11] On appeal by Yershov, the First Circuit reversed the district court's dismissal, holding that not only was the data personally identifiable information, but that Yershov was in fact a consumer within the definition provided by the VPPA.[12]

This Comment will challenge the courts' characterization of the mobile device's GPS location and the associated unique device identifying number collected and disclosed by Gannett as personally identifiable information ("PII") under the VPPA, as neither piece of information fits within the bounds of the definition as identifying a "particular person."[13] Furthermore, this Comment will argue that the First Circuit interpreted the statutory definition of "consumer" too broadly when it held that the simple act of downloading a free mobile application is synonymous with becoming a "subscriber," a subset of the VPPA's definition of "consumer." Rather than reading

---

Woods, *Federal Trade Commission's Privacy and Data Security Enforcement Under Section 5*, AMERICAN BAR ASSOCIATION: YOUNG LAWYERS DIVISION, http://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/federal_trade_commissions_privacy.html (last visited Jan. 24, 2017). However, the FTC recently published a consumer privacy report that outlines best practices for businesses and policymakers. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations /120326privacyreport.pdf.

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

8. Many see the introduction of the iPhone in 2007 as the moment when smartphones—and the mobile internet—moved beyond rudimentary web browsers and email checking. *See, e.g.*, Fred Vogelstein, *The Day Google Had to 'Start Over' on Android*, THE ATLANTIC (Dec. 18, 2013), https://www.theatlantic.com /technology/archive/2013/12/the-day-google-had-to-start-over-on-android/282479/.

9. 18 U.S.C.A. § 2710 (2012).

10. *Yershov*, 104 F. Supp. 3d at 141, 148; Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 484 (1st Cir. 2016).

11. *Yershov*, 104 F. Supp. 3d at 146, 149.

12. *Yershov*, 820 F.3d at 486, 489-90.

13. S. Rep. No. 100–599, at 12 (1988).

the word "subscriber" as it is plainly and ordinarily understood, the First Circuit interpreted the term "subscriber" as virtually synonymous with the term "user" or "viewer,"[14] and in doing so has expanded the application of the statute far beyond the intention of the legislation's authors. A statute such as this one is best read narrowly, so as to avoid requiring the courts to read contemporary legislative intent into antiquated legislation. As Justice Samuel Alito has suggested, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[15]

This Comment will also attempt to shed a bit of light on the mobile advertising technology ("ad tech") ecosystem from which *Yershov* and similar cases have arisen. It will explore the curious reliance that mobile technology has on data collection by the mobile ad tech industry, and the direction of information privacy regulation in the mobile ad tech universe by both the companies themselves, and government regulators.

To these ends, Part II sets the stage of the modern ecosystem of mobile internet advertising technology; Part III takes the reader back to examine the VPPA's origins and purpose; Part IV provides the procedural background of *Yershov v. Gannett*; Part V analyzes the courts' decisions and reasoning in *Yershov*, and the implications thereof; and Part VI examines the possible future of information privacy law relating to mobile internet technology and the collection of data from mobile devices.

II. MOBILE TECHNOLOGY AND THE AD TECH ECOSYSTEM

A. "If You're Not Paying for It, You're the Product"[16]

No one could have predicted the radical evolution of targeted marketing during the twentieth and twenty-first centuries. The advent of internet technology, and later the mobile internet, transformed targeted marketing—now called interest-based advertising—into a complex and sophisticated ecosystem that runs largely on the synergistic interactions of four big players: website and app publishers; users and consumers of mobile internet technology; advertisers; and third party advertising companies.[17] Simply put, mobile app and website publishers create, maintain, and improve the mobile internet, and have a reasonable expectation to get paid for these contributions. Mobile users want a high quality and innovative mobile internet experience, but expect most websites and apps to be accessible at marginal or zero

14. That Congress chose to use the word "subscriber" and not "user" or "viewer" was noted by the Eleventh Circuit in its interpretation of the VPPA. Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1256-57 (2015).

15. United States v. Jones, 565 U.S. 400, 429 (2012).

16. The saying—and the underlying idea—are not easily attributed to any one person, but can be found throughout the marketing sector's history as early as the 1980's. *See* Jonathan Zittran, *Meme Patrol: "When Something Online is Free, You're Not the Customer, You're the Product."* HARVARD UNIVERSITY: THE FUTURE OF THE INTERNET AND HOW TO STOP IT (Mar. 21, 2012), http://blogs.harvard.edu/futureofthe internet/2012/03/21/meme-patrol-when-something-online-is-free-youre-not-the-customer-youre-the-product/.

17. *See How Does It Work,* NETWORK ADVERT. INITIATIVE, http://www.networkadvertising.org/understanding-online-advertising/how-does-it-work (last visited Jan. 29, 2017).

cost. So how can publishers expect to be compensated for their work if consumers are unwilling to pay for it? Taking a page from the playbook of traditional media operations, webpage and in-app advertising has provided a significant source of revenue for publishers.[18] Advertisers are willing and eager to pay for the opportunity to advertise to publishers' users; and the more likely a particular user is to be interested in purchasing the advertised product or service, the more valuable that advertising opportunity is to the advertiser.[19] Third party advertising companies enter the system to connect the dots—they collect, organize, and analyze interest-based and demographic information about users collected from various sources, so as to better predict who those interested users are, thus increasing the value of advertising opportunities online—hence, interest-based advertising's integral role in the internet as we know it.[20]

B. A Primer on Mobile Application Advertising

As alluded to above, most advertisements one sees in a mobile application are not virtual billboards seen by all who happen to use a particular app. Rather, the point of modern advertising technology is to get "the right message, to the right person, in the right place, at the right time."[21] By collecting and analyzing demographic information and information about users' interests, companies are able to target marketing efforts to the users most likely to be interested in—and then purchase—the product or service.[22] From the perspective of a user, her online experience is—dare I say—*enhanced* by being shown ads that are relevant to her interests. Some in the ad tech industry would go even further and say advertising companies are actually providing a *service* to users by educating them about new products they are likely to find useful.[23]

The techniques developed by third party advertisers to collect user information from internet sources have evolved alongside internet technology. Methods that have worked in a desktop internet browser are not as effective on a mobile internet browser.[24] Moreover, a significant portion of time spent on a mobile device is not in

---

18. Spending on digital advertising in 2015 reached $59.6 billion, and over half of that was spent on mobile advertising. *See* Kristine Lu & Jesse Holcomb, *Digital News Revenue: Fact Sheet*, PEW RESEARCH CENTER (June 15, 2016), http://www.journalism.org/2016/06/15/digital-news-revenue-fact-sheet/.

19. DEMPSTER & LEE, *supra* note **Error! Bookmark not defined.**, at 13-14.

20. *See* NETWORK ADVERT. INITIATIVE, *supra* note 17.

21. DEMPSTER & LEE, *supra* note 2, at 116; *see also* Mike Sands, *How the Cookie Crumbles in a Mobile-First World*, MARTECH TODAY, (Dec. 15, 2015), https://martechtoday.com/cookies-crumble-mobile-first-world-154114.

22. *See* FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 2 (2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400/behavadreport.pdf; *see also* Carol Hildebrand, *3 Signs That Mobile Data is the New Marketing Overlord*, FORBES: ORACLEVOICE, (Nov. 16, 2016, 5:00 AM), http://www.forbes.com/sites/oracle/ 2015/11/16/3-signs-that-mobile-data-is-the-new-marketing-overlord/#49e4a34e46f6.

23. *See generally* Adam Thierer & Berin Szoka, *The Hidden Benefactor: How Advertising Informs, Educates, & Benefits Consumers*, PROGRESS SNAPSHOTS, Feb. 2010, at 1-2.

24. Sands, *supra* note 21. While ad tech companies can and do employ the use of third-party "cookies," (text files placed in a desktop browser for the purpose of data collection by companies other than the website's publisher) most mobile browsers have blocked third-party cookies from being used. Additionally, cookies simply do not work in mobile apps. Additionally, as users have begun to use more than one device—smartphones, laptops, tablets, smart TVs, etc.—the ad tech sector has developed technology to track users' online behavior across multiple devices, called cross-device targeting. This

a browser at all, but rather in various mobile applications.[25] Apps are programmed to collect data, often by permission, directly from users' devices.[26] Upon downloading and opening the app, a user may be asked to sign into an existing user profile, or to create a new profile with a user name or email address. Once registered and signed in, the publisher of the app can track the user's viewing habits and purchasing history within that publisher's internet presence, and across multiple devices.[27] This type of data collection—the collection of data by a mobile application with which the user has a direct relationship—is known in the ad-tech sector as "first party data."[28] An app publisher may also provide that same data to a third party advertising company, making the data "third party data,"[29] a concept that will be discussed further below.

But not all first party or third party data is organized using identifiable information like names or email addresses. Instead, many app publishers and third party advertising companies organize collected information by linking it to a pseudonymous number associated with a particular device.[30] Prior to 2012, this number—a unique alpha-numeric sequence called a "mobile device identifier"—was a number permanently associated with the specific device's hardware.[31] The user of the device had little or no ability to prevent apps from using the mobile device identifier for advertising purposes and therefore had little control over what information was being associated with it.[32] In 2012, after Congress voiced concerns about mobile device identifiers and consumer privacy,[33] the industry abandoned them for another pseudonymous identifier referred to as a "mobile advertising identifier."[34] A mobile advertising identifier operates in a way similar to its

---

technology is not without its critics. *See* The Editorial Board, *Monitoring Your Every Move*, N.Y. TIMES (Oct. 9, 2013), http://www.nytimes.com/2013/10/10/opinion/monitoring-your-every-move.html (explaining cross-device targeting and asserting a need for more federal regulation).

25. *How Mobile Apps Stack Up Against Mobile Browsers*, EMARKETER, (Jan. 14, 2016), https://www.emarketer.com/Article/How-Mobile-Apps-Stack-Up-Against-Mobile-Browsers/1013462.

26. Kenneth Olmstead, *Mobile Apps Collect Information About Users, With Wide Range of Permissions*, PEW RESEARCH CENTER (Apr. 29, 2014), http://www.pewresearch.org/fact-tank/2014/04/29/mobile-apps-collect-information-about-users-with-wide-range-of-permissions/.

27. *See id.*

28. *See Getting to Know You*, THE ECONOMIST, (Sept. 13, 2014), http://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party.

29. *See id.*

30. Many companies see the benefit of maintaining users' trust and privacy, and have joined self-regulatory agencies committed to developing best practices of the ad tech industry. *See About the NAI*, NETWORK ADVERT. INITIATIVE, http://www.networkadvertising.org/about-nai/about-nai, (last visited Jan. 29, 2017); *see also How Does It Work,* NETWORK ADVERT. INITIATIVE, http://www.networkadvertising.org/understanding-online-advertising/how-does-it-work (last visited Jan. 29, 2017).

31. Apple called the number the "unique device identifier" ("UDID"), while Google called it the "Android ID." *See* Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You: A Journal Investigation Finds That iPhone and Android Apps Are Breaching the Privacy of Smartphone Users*, WALL ST. J. (Dec. 17, 2010), https://www.wsj.com/articles/SB10001424052748704694004576020083703574602.

32. *See id*. ("The great thing about mobile is you can't clear a UDID like you can a cookie.").

33. *See* Connie Guglielmo, *Congress Queries Apple, iPhone Developers About Privacy*, FORBES, (Mar. 22, 2012), http://www.forbes.com/sites/connieguglielmo/2012/03/22/congress-queries-apple-iphone-app-developers-about-privacy/#348781ca3885.

34. Apple calls this number the Identifier for Advertisers ("IDFA"), where Android calls the number the Google Advertising ID ("GAID"). *See Understanding Online Advertising: Glossary*, NETWORK ADVERTISING INITIATIVE, http://www.networkadvertising.org/understanding-online-advertising/glossary

predecessor, in that apps and advertising companies may use it as a common tag for data that mobile apps collect about a user. However, unlike the mobile device identifier, the mobile advertising identifier is designed to be reset or turned off entirely at any time by the user simply by the press of a button in the device's settings, thus returning some control of data collection by apps to the user and generally reducing some users' privacy concerns.[35]

As indicated previously, mobile application and website publishers may employ third party advertising companies to analyze the data that they collect. These companies, which sometimes operate as data analysis firms or "data brokers," gather information from sources on the web, mobile apps, and sometimes from offline sources in order to compile comprehensive dossiers of users' information.[36] Some firms claim to have up to 100 data points on mobile users.[37] While it is likely that identifiable information like names, home addresses, or email addresses are incorporated into these dossiers, companies in the business of online advertising are less interested in that type of information, and more interested in demographic and interest data.[38] After all, the principal purpose of this type of data collection and analyzation is to meet the advertiser's ultimate goal: to show their online ads to those users who are most likely to purchase whatever they are selling. Names and addresses have a limited ability to help make this determination. On the other hand, demographic information (e.g. age and gender), interest data (e.g. topics of articles read within media apps), and even geo-location information can give a much better idea to the advertising company about whether an advertisement will be successful with a viewer, without directly revealing his or her identity.[39] With this type of information, an advertising company can then advertise to all viewers who match a particular category or demographic, for instance all users who are of a particular age range, who live in a particular area, and who are bicycle enthusiasts. The more demographic and interest information an advertising company can collect—even without names or home addresses—the better they can predict which ads are relevant to which users.

C. The Spectrum of Personally Identifiable Information

Rather than being easily demarcated between identifiable and non-identifiable, personal information, like that mentioned above, is better described as falling along

---

(last visited Jan. 29, 2017).

35. Laura Stampler, *Here's Everything We Know About IFA, the iPhone Tracking Technology in Apple's iOS6*, BUSINESS INSIDER, (Oct. 15, 2012, 3:59 PM), http://www.businessinsider.com/everything-we-know-about-ifa-and-tracking-in-apples-ios-6-2012-10.

36. For a helpful infographic illustrating the collection of information by data brokers, see FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 2 (2014).

37. THE ECONOMIST, *supra* note 28.

38. *See* Ilana*, What Advertisers Know About You: Online Privacy and Personally Identifiable Information*, RETARGETER, http://blog.retargeter.com/general/what-advertisers-know-about-you-online-privacy-and-personally-identifiable-information (last visited Jan. 30, 2017); *see also Frequently Asked Questions,* NETWORK ADVERTISING INITIATIVE, https://www.networkadvertising.org/faq, (last visited Jan. 30, 2017) ("As a general rule, [interest-based advertising] . . . does not depend on information that personally identifies you . . . .").

39. THE ECONOMIST, *supra* note 28.

a spectrum.[40] At one end of the spectrum is the clearest category of PII: a person's actual name.[41] Further down the spectrum, but still widely considered PII, is data that is easily traced to a particular person using information in the public domain like home addresses, phone numbers, and email addresses.[42] Highly sensitive data like social security numbers and financial account numbers are also widely accepted as PII, not because they can be easily traced to a particular person, but because of the harm that can come from an unauthorized person gaining access to that type of information.

Toward the other end of the spectrum is pseudonymous identifiers like user names, unique device identifiers, mobile advertising identifiers, IP addresses, and browser fingerprints. This is data that is not generally considered highly sensitive, and cannot be easily re-identified by an ordinary person.[43] It is also at this end of the spectrum, perhaps at the farthest end, where anonymous information like interest and demographics belong; things like age or hobbies ("18-24" and "video games"). As suggested above, and perhaps surprisingly, many ad tech companies prefer the pseudonymous and anonymous information at this end of the spectrum. By using a mobile advertising identifier tag instead of a name, companies in the ad tech industry can capture and organize much of the demographic and interest data they need to market their products successfully, while maintaining the trust and confidence of their users.[44]

Two other pieces of data sometimes collected by mobile apps are at issue in *Yershov*: a user's geo-location, and the titles of videos a user has watched. First, mobile applications may collect a user's location data using IP addresses, global positioning systems ("GPS"), Wi-Fi triangulation, or beacons.[45] For advertisers, location data can provide a cache of inferential information: demographic information like income and education can be inferred by comparing a user's primary location data to public census data; information about a user's interests can be inferred by noting visits to museums, theme parks, or the wilderness.[46] Location information can even indicate more narrow preferences like where a user prefers to

---

40. *In re* Nickelodeon, 827 F.3d 262, 282-83 (3d Cir. 2015); *see also* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U L. REV. 1814, 1877 (2011) (discussing a spectrum of "information [that] can be about an (1) identified, (2) identifiable, or (3) non-identifiable person.").

41. *In re* Nickelodeon, 827 F.3d at 282-83.

42. *Id.*

43. *See id.* at 290.

44. Timothy Morey, Theodore Forbath & Allison Schoop, *Customer Data: Designing for Transparency and Trust*, HARVARD BUSINESS REVIEW, (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust (last visited April 14, 2017).

45. MOBILE MKTG. ASS'N, *Demystifying Data Location Accuracy: The New Frontier and Biggest Mobile Opportunity*, http://www.mmaglobal.com/files/documents/location-data-accuracy-v3.pdf (last visited April 14, 2017).

46. *See id.* at 4. *But see* John Koetsier, *80-90% Of Mobile Ad Location Data Is Wrong, Says Top Ad Exec*, FORBES, (Dec. 2, 2016, 2:14 PM) (suggesting that a substantial amount of the geo-location data used by advertisers is wrong), http://www.forbes.com/sites/johnkoetsier/2016/12/02/80-90-of-mobile-ad-location-data-is-wrong-says-top-ad-exec/2/#4f9cb69b666e.

shop or which restaurants a user frequents.[47]

Second, some advertisers are gathering data based on users' mobile video consumption. Americans in 2016 are spending an average of over three hours a day consuming media on mobile devices, and more than thirty minutes of that time is spent watching video content. This represents a 300 percent increase since 2012.[48] The average length of videos viewed on a mobile device are of shorter duration than those watched on a television or computer; full length television shows and movies are watched far less than videos with a duration of five minutes or less.[49] This means the average person is likely to watch multiple short videos a day, probably consisting of some combination of comedic video clips (i.e. "viral videos"), music videos, movie trailers, sports clips, how-to videos, and news clips.[50] As one might imagine, the aggregate of these videos watched over a period of time can reveal quite a bit of information about a user's interests; information that is valuable to companies looking to market their products to a targeted audience.

So how does the modern ad-tech industry's collection of this type of pseudonymous and anonymous data fit into a 1988 statute written to restrict the disclosure of rental records of "prerecorded video cassette tapes" [51] by video rental stores? Not easily.

III. THE VIDEO PRIVACY PROTECTION ACT OF 1988

A. Origins

The collection of personal information by both governmental and private organizations became routine with the arrival of modern record-keeping technology after the Second World War.[52] Following the advent of computers in the 1960s and further advances in data processing in the 1970s and 80s, Congress became concerned with the breadth and depth of this information.[53] They enacted a series of federal statutes regulating the disclosure of particular kinds of personal information collected and held by particular entities. These included credit records,[54] student education records,[55] federally stored personal information,[56] tax returns,[57] bank

47. *See* MOBILE MKTG. ASS'N, *supra* note 45, at 4; *see also* THE ECONOMIST, *supra* note 28.

48. Media Buying, *Growth in Time Spent with Media Is Slowing*, EMARKETER, (June 6, 2016), https://www.emarketer.com/Article/Growth-Time-Spent-with-Media-Slowing/1014042.

49. *Mobile Video 2015: A Global Perspective (2015)*, ONDEVICE RESEARCH, http://www.iab.com/wp-content/uploads/2015/06/IAB_Mobile_Video_Usage_FINAL.pdf (last visited April 14, 2017).

50. *Id.*

51. 18 U.S.C.A § 2710(a)(4) (2012).

52. *See generally* Schwartz & Solove, *supra* note **Error! Bookmark not defined.**, at 1820; *see also* U.S. DEP'T OF HEALTH EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS, U.S. DEPT. OF HEALTH, EDUCATION, AND WELFARE 7 (1973).

53. Schwartz & Solove, *supra* note **Error! Bookmark not defined.**, at 1820.

54. Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (2012) (prohibits any person from procuring a credit report of another person without permission).

55. Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232(g) (2012).

56. Privacy Act, 5 U.S.C. § 552a (2012) (prohibiting the disclosure of any records kept by governmental agencies).

57. Tax Reform Act of 1976, 26 U.S.C. § 6103 (2012) (prohibiting the disclosure of tax return or return information).

records,[58] and individuals' cable television viewing habits.[59] The VPPA came toward the end of that trend, and arose not out of a natural progression of privacy law, but as a hasty reaction to what members of Congress saw as an intolerable breach of privacy.

It began with President Ronald Reagan's 1987 nomination of Judge Robert Bork to fill a vacancy on the United States Supreme Court.[60] While the Senate Judiciary Committee vetted Bork in confirmation hearings, an industrious *Washington City Paper* reporter obtained Bork's video rental history from the local video rental store.[61] The list of videos, which was published in the newspaper for public scrutiny, was hardly damning; it showed only Bork's penchant for Alfred Hitchcock and Cary Grant movies.[62] But the idea that a citizen's—or a legislator's—video rental history could be publicly released and published as news resonated with outrage in Congress.[63] They worked quickly to introduce and enact a law prohibiting just that sort of disclosure.

B. The Statute

The law Congress enacted was called the Video Privacy Protection Act of 1988 ("VPPA").[64] It states, "[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person . . . ."[65] The statute also provides the following definitions:

> (1) the term "consumer" means any renter, purchaser, or subscriber of goods or services from a video tape service provider; . . .
>
> (2) the term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider;
>
> (3) the term "video tape service provider" means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual

58. Right to Financial Privacy of 1978, 12 U.S.C. § 3403 (2012) (restricting the disclosure of financial records by financial institutions to governmental agencies).

59. Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2001) (prohibiting the disclosure of personally identifiable information together with "the extent of viewing or other use by the subscriber of a cable service or other service provided by the cable operator.").

60. Ann M. Schultz, *Protecting Consumer Viewing Habits: Reflections on the Video Privacy Protection Act*, WAYNE ST. U., https://blogs.wayne.edu/informationpolicy/2013/11/30/protecting-consumer-viewing-habits-reflections-on-the-video-privacy-protection-act/ (last visited Feb 2, 2017).

61. *Id.*

62. Michael deCourcy Hinds, *Personal but not Confidential: A New Debate Over Privacy*, N.Y. TIMES (Feb. 27, 1988), http://www.nytimes.com/1988/02/27/style/consumer-s-world-personal-but-not-confidential-a-new-debate-over-privacy.html.

63. *See id.*; *see also Video and Library Privacy and Protection Act of 1988: Joint Hearing on H.R. 4947 and S. 2361 Before the Subcomm. on Courts, Civil Liberties, & the Admin. of Justice of the H. Comm. Of the Judiciary and S. Subcomm. on Tech. and the Law, of the S. Comm. on the Judiciary,* 100th Cong. 18 (1988).

64. 18 U.S.C. § 2710 (2012).

65. *Id.* at § 2710(b).

materials, or any person or other entity to whom a disclosure is made . . . .[66]

The law goes on to permit the disclosure of such information in certain circumstances: to the consumer; to anyone pursuant to the consumer's written consent; in the regular course of business; "to a law enforcement agency pursuant to a warrant;" or "pursuant to a court order."[67]

In addition to Congress's primary concern (the public disclosure of video rental histories), the testimonial record from the joint congressional hearing in 1987 expresses a separate concern: the collection and disclosure of this type of information for the purpose of targeted marketing.[68] Senior Vice President of the Direct Marketing Association, Richard Barton, appeared at the hearing and was questioned about that industry's opposition to the bill. In reference to personal information collected by private companies, he stated,

> And there is no doubt that direct marketing companies use this information in an attempt to increase sales. Companies in our industry want to know about a person's interest to be better able to market products to that person. If you are a hiker, changes [sic] are you would be interested in a catalogue selling camping or fly fishing equipment . . . . These lists are closely controlled and they are used only for marketing purpose. They cannot be accessed over the counter and are maintained with a high degree of security.[69]

Reacting to Barton's testimony, Senator Patrick Leahy shared his own perception of direct marketing tactics:

> Really, 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 figure out that Patrick Leahy is this sort of person based on what he reads or what he thinks or 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. Do you see my concern?[70]

In response, Congress included a conciliatory provision in the VPPA that allows names, addresses, and video tape *subject matter* to be released for the purposes of targeted marketing, so long as the consumer has a reasonable opportunity to decline.[71]

Interestingly, Congress amended the in 2012, but the only provision that was altered was the requirement for video service providers to get written consent from the consumer every single time the provider wanted to disclose PII.[72] Netflix, a video

---

66. *Id.* at § 2710(a)(1)-(4).

67. *Id.* at § 2710(b)(2)(A)-(F).

68. *Video and Library Privacy and Protection Act of 1988: Joint Hearing on H.R. 4947 and S. 2361 Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice and S. Subcomm. on Technology and the Law,* 100th Cong. 115-118 (1988) (testimony of Richard A. Barton, Senior Vice President, Direct Marketing Association).

69. *Id.* at 95.

70. *Id.* at 115-16.

71. 18 U.S.C. § 2710(b)(2)(D) (2012).

72. *Id.*

streaming service provider,[73] successfully lobbied Congress for an amendment that would allow for a one-time electronic "opt-in" consent to be sufficient for disclosure for up to two years.[74] Both the Senate and House Reports for the amendment, as well as the Senate Subcommittee Hearing transcript, spent a majority of their time discussing this particular provision, consequently leaving the more ambiguous statutory definitions at issue in *Yershov* as is.

IV. *YERSHOV V. GANNETT*

The question before the *Yershov* court was whether the law laid out by Congress in the VPPA applies to the newest iteration of video consumption. In 2013, Plaintiff Alexander Yershov owned a smartphone, and onto that smartphone he downloaded a free mobile application called the *USA Today Mobile App* ("the app").[75] He used the app to access news, entertainment articles, and video clips.[76] At the time Yershov downloaded the app, he was never asked to consent to the disclosure of information collected by the app to any third party.[77]

The *USA Today Mobile App* Yershov downloaded was owned by Defendant Gannett Satellite Services, Inc. ("Gannett"), an international media company.[78] The app was programmed to collect certain bits of data every time a user watched a video on the app: "(1) the title of the video viewed, (2) the GPS coordinates of the device at the time the video was viewed, and (3) certain identifiers associated with the user's device, such as its unique Android ID."[79] Gannett then sent this information to a third party data analysis firm, Adobe.[80]

Yershov, as the named party in the class action suit, filed a claim against Gannett in the Federal District Court of the District of Massachusetts under the Video Privacy Protection Act of 1988.[81] Yershov argued that Gannett, as a video service provider, illegally disclosed to a third party information that identified him as having viewed specific videos, in direct violation of the VPPA.[82] Gannett moved to dismiss the suit for failure to state a claim, asserting that Yershov did not adequately allege two elements of the claim: (1) that the data provided to Adobe was "personally identifiable information," and (2) that Yershov was a "consumer."[83]

The district court held that the information Gannett collected from Yershov and

---

73. For more information on Netflix, *see* NETFLIX, *Netflix's View: Internet TV is Replacing Linear TV*, https://ir.netflix.com/long-term-view.cfm (last visited April 14, 2017) ("Netflix is a global internet TV network offering movies and TV series commercial-free, with unlimited viewing on any internet-connected screen for an affordable, no-commitment monthly fee.").

74. *The Video Privacy and Protection Act: Protecting Viewer Privacy in the 21st Century*, *Hearing on H.R. 2471 Before S. Subcomm. on Privacy, Tech. and the Law, of the S. Comm. on the Judiciary*, 112th Cong. 5 (2012); *see also* Natasha Singer, *Put It on My Marquee: I Just Watched 'Creepshow 2'*, N.Y. TIMES (Dec. 10, 2011), http://www.nytimes.com/2011/12/11/business/bill-would-let-video-consumers-disclose-all-their-choices.html.

75. Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 138 (D. Mass. 2015) *rev'd*, 820 F.3d 482, 485 (1st. Cir. 2016).

76. *Id* at 137.

77. *Id* at 138.

78. *Id.* at 137.

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

80. *Yershov*, 104 F. Supp. 3d at 138.

81. *Id.* at 137.

82. *Id* at 140.

83. *Id.* at 142.

later disclosed to Adobe "constitutes personally identifying information within the meaning of the Video Privacy Protection Act."[84] It reasoned that a unique device identifier is the device's "address" and, "[a] person's smartphone 'address' is an identifying piece of information, just like a residential address."[85] This determination rests largely on the court's exceedingly broad interpretation of the VPPA's PII definition[86] and diverges from nearly every other court holding on the issue.[87] The court rejected the reasoning of the District Court of New Jersey, which held explicitly that an Android ID was *not* PII in the case In re *Nickelodeon*.[88] The *Yershov* court stated, "*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."[89] The court only briefly mentioned the GPS location component,

> [p]resumably, that information would be sufficient to identify a very specific location (such as a building) from which the user viewed the video. It therefore appears possible to identify, with a relatively high degree of accuracy, the residential address of users . . . .[90]

The district court noted that "[i]t is also possible . . . that third parties such as Adobe have access to databases that link Android IDs to specific persons."[91]

On Gannett's second point, however, the district court agreed and held that Yershov was not a "subscriber"[92] and therefore not a consumer under the VPPA's statutory definition.[93] The court referenced several dictionary definitions and analyzed other applications of the word "subscription" when used in the context of online activity.[94] It concluded that "where there is no payment of money, no registration of information, no periodic delivery, and no privilege to view restricted content, none of the necessary elements of a subscription are present."[95] Having found that Yershov was not a subscriber under those terms, and therefore not a consumer, the court dismissed the claim.

On appeal, the First Circuit Court of Appeals reversed the district court's ruling to dismiss the claim.[96] The First Circuit agreed with the district court's conclusion

---

84. *Id.* at 146 (internal quotations omitted).

85. *Id.* at 141.

86. Notably, the court made no reference to the Act's legislative history.

87. *See, e.g.*, *In re* Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 290 (3d Cir. 2016) ("[P]ersonally identifiable information under the Video Privacy Protection Act means the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior."); Ellis v. Cartoon Network, Inc., 2014 WL 5023535, at *3 (N.D. Ga. Oct. 8, 2014) ("Without more, an Android ID does not identify a specific person."); *In re* Hulu Privacy Litigation, 2014 WL 1724344, at *12 (N.D. Ca. Apr. 28, 2014) (holding that a Hulu user ID—"without more"— is not personally identifiable information).

88. *In re* Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 295 (3d Cir. 2016).

1. 89. *Yershov*, 104 F. Supp. 3d at 145 (quoting *In re* Nickelodeon Consumer Privacy Litigation, 2014 WL 3012873, *10 (D.N.J. 2014)).

90. *Id.* at 142.

91. *Id.* at 146.

92. *Id.* at 149.

93. 18 U.S.C. § 2710(a)(1) (2012).

94. *Yershov*, 104 F. Supp. 3d at 148.

95. *Id.* at 149.

96. Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 490 (1st Cir. 2016).

and reasoning regarding the claim's PII element. Although quite brief in its opinion, the court concluded that the statutory definition of PII is to be read broadly, and cited the accompanying Senate Report as support for this interpretation: "the drafters' aim was 'to establish a minimum, but not exclusive, definition of personally identifiable information.'"[97] The court only briefly referenced the GPS location data, analogizing it to a home address, "[g]iven how easy it is to locate a GPS coordinate on a street map, this disclosure would enable most people to identify what are likely the home and work addresses of the viewer."[98] Like the district court, the First Circuit also noted the complaint's allegation regarding Adobe's databases, and the possibility that Gannett *knew* that Adobe had the means to re-identify the Android ID.[99]

The First Circuit departed from the district court decision with regard to the statutory definition of "consumer."[100] The court concluded that Yershov was a "subscriber," despite not having made a monetary payment, not having completed a registration of information, and not having received periodic delivery or any privilege to view restricted content. The court reasoned that Yershov's "access was not free of a commitment to provide consideration in the form of that information which was of value to Gannett."[101] The court also distinguished between the act of reading news from the USA Today website, and doing the same on the app. The court reasoned that the act of downloading the app was akin to the installation of a "hotline" directly into Yershov's home through which Yershov could watch videos in exchange for providing his name and address.[102] In other words, the court felt that downloading the app was a subscribing act.

The First Circuit was explicit in its conclusion that its decision is to be read narrowly and that a claim under the VPPA is plausible when "Yershov used the mobile device application that Gannett provided to him, which gave Gannett the GPS location of Yershov's mobile device at the time he viewed a video, his device identifier, and the titles of the videos he viewed in return for access to Gannett's video content . . . ."[103]

At this time, the parties are preparing for trial in the United States District Court for the District of Massachusetts.

V. ANALYSIS

To be sure, the First Circuit is not the only court that has struggled with interpreting the VPPA. The Act has been described by other courts as "not well drafted,"[104] and "not entirely clear."[105] That the VPPA necessarily applies to a continuously evolving subject matter—video technology—makes it especially challenging to interpret thirty years after its enactment. Even the district court analogized the circumstances in *Yershov* as "an attempt to place a square peg

97. *Id.* at 486.
98. *Id.*
99. *Id.*
100. *Id.* at 489.
101. *Id.*
102. *Id.*
103. *Id.*
104. Sterk v. Redbox Automated Retail, LLC, 672 F.3d 535, 538 (7th Cir. 2012).
105. *In re* Nickelodeon, 827 F.3d 262, 281 (3rd Cir. 2016).

(modern electronic technology) into a round hole (a statute written in 1988)."[106] The Supreme Court has weighed in on interpreting statutes made ambiguous by technology: "[w]hen technological change has rendered its literal terms ambiguous, [a law] must be construed in light of [its] basic purpose."[107] This is perhaps easier said than done.

A. Personally Identifiable Information Under the VPPA

The VPPA's basic purpose is "[t]o preserve personal privacy with respect to the rental, purchase or delivery of video tapes or similar audio visual materials."[108] Fundamental to this purpose is the concept of personally identifiable information, which despite being "one of the most central concepts in privacy regulation" remains without a uniform definition.[109] In fact, depending on where one looks—at statutes, agency regulations and policy statements, industry self-regulation associations, or privacy policies of individual companies—PII is defined in a myriad of different ways.

For example, when Congress enacted the Children's Online Privacy Protection Act ("COPPA")[110] in 1998, they defined PII by enumerating specific examples, including a child's name, address, email address, phone number, and social security number.[111] They also included another provision that defined PII as "any other identifier that the [Federal Trade] Commission determines permits the physical or online contacting of a specific individual."[112] This provision reflects Congress's intention to incorporate flexibility into the definition of PII by leaving the term to be further defined by the FTC, which can—and has—expanded COPPA's definition to include new technology.[113]

Other entities take a different approach to defining PII. The Network Advertising Initiative ("NAI"), a not-for-profit ad tech self-regulatory association, defines PII as "any information used or intended to be used to *identify a particular individual*, including name, address, telephone number, email address, financial account number, and government-issued identifier.[114] Thompson Reuters Westlaw's Privacy Statement, possibly the most explicit explanation of them all, marks PII as

> your name, address, phone number, email address, payment card information, and/or certain additional categories of information that identify you personally; and . . . do[es] not include username, technical

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

107. Twentieth Century Music Corp. v. Aiken, 422 U.S. 151, 156 (1975).

108. S. Rep. No. 100–599, at 1 (1988).

109. Schwartz & Solove, *supra* note 40, at 1816.

110. 15 U.S.C. §§ 6501-6506 (2012).

111. § 6501(8).

112. *Id.*

113. FTC amended COPPA in 2013, adding GPS location, cookies, IP addresses, and unique device identifiers to the definition of PII. 16 C.F.R. § 312.2 (2013); *see also* Natasha Singer, *New Online Privacy Rules for Children*, N.Y. TIMES (Dec. 19, 2012), http://www.nytimes.com/2012/12/20/technology/ftc-broadens-rules-for-online-privacy-of-children.html. Although the discussions leading up to the COPPA amendment coincided with those of the VPPA amendment in 2012, Congress did not add to that statute's definition of PII. 18 U.S.C. § 2710(a)(3) (2012).

114. *Understanding Online Advertising: Glossary*, NETWORK ADVERT. INITIATIVE, http://www.networkadvertising.org/understanding-online-advertising/glossary (last visited Feb. 10, 2017) (emphasis added).

> information (for example, Unique Device Identifier or "UDID," Media Access Control "MAC" address, Apple's Identifier For Advertising or "IFA," and Internet Protocol or "IP" address), or numbers or alpha-numeric identifiers assigned by us, third-parties, or your computer.[115]

The VPPA definition of PII, on the other hand, leaves much to be surmised. It states rather circularly that "personally identifiable information includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."[116] In the words of the First Circuit, "the definition . . . adds little clarity beyond training our focus on the question whether the information identifies the person who obtained the video."[117] Or to quote another author's paraphrased version of the definition, "PII is PII."[118] The only additional indication of what the Act's drafters considered to be PII is found embedded in an exception to the Act's general prohibition: "A video tape service provider may disclose personally identifiable information concerning any consumer to any person if the disclosure *is solely of the names and addresses of consumers* . . . ."[119] In other words, names and addresses are without question PII under the VPPA.

All frustration aside, it is likely that the drafters of the VPPA intended the definition of PII to be somewhat ambiguous in order to preserve the statute's flexibility over time. The VPPA's accompanying Senate Report supports this theory: "the word 'includes' . . . establish[es] a minimum, but not exclusive, definition of personally identifiable information."[120] The district court deciding *Yershov* interpreted the Senate Report to mean that "the universe of PII is greater than the consumer's name and address."[121] Other courts have made similar conclusions.[122] And this makes sense: email addresses and phone numbers, for example, were not mentioned in the VPPA, but are characterized as PII by any modern definition.[123] However, the Senate Report also incorporates a limiting principle. It explicitly states, "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."[124] This is where both the district court and the First Circuit went wrong: neither an Android ID nor a GPS location sufficiently identifies a particular person under the conditions set forth by Congress in the VPPA.

1. Android ID Is Not PII

An Android ID—or any similar pseudonymous number—does not identify a

---

115. *Thompson Reuters Westlaw Privacy Statement*, THOMPSON REUTERS WESTLAW, https://1.next.westlaw.com/Privacy?transitionType=Default&contextData=(sc.Default) (last visited Feb. 10, 2017).

116. 18 U.S.C. § 2710(a)(3) (2012).

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

118. Schwartz & Solove, *supra* note 40, at 1829.

119. 18 U.S.C. § 2710(b)(2)(D) (emphasis added).

120. S. Rep. No. 100–599, at 12 (1988).

121. *Yershov*, 820 F. Supp. 3d at 140.

122. *See, e.g.*, *In re* Hulu Privacy Litigation, 2014 WL 1724344, at *11, (N.D. Cal. Apr. 28, 2014).

123. *See Understanding Online Advertising: Glossary*, NETWORK ADVERTISING INITIATIVE, http://www.networkadvertising.org/understanding-online-advertising/glossary (last visited Dec. 4, 2016).

124. S. REP. NO. 100–599, at 12 (1988) (emphasis added).

particular person. It identifies a device.[125] An Android ID is a number associated with a particular device that,[126] when used for advertising purposes, acts as a point of connection in a spider web of informational data.[127] When Gannett sent an Android ID and a video title to Adobe, it is likely that Adobe added the video title to other information in their database that was also connected to that Android ID. For example, the Android ID might already be associated with the user's gender or age range, or perhaps a notation that the user plays Angry Birds, or that she has an interest in cats, or that she once searched for an Italian restaurant in Manhattan.[128] Could Adobe have linked the identifier to actually identifying information? Maybe. But, to borrow the succinctly stated words of the First Circuit, "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,"[129] and contrary to the First Circuit's actual holding, the circumstances in *Yershov* are exactly that.

Furthermore, should the definition of PII be read so broadly to include a pseudonymous number like an Android ID, video service providers are essentially forced to read an extra provision into the Act. Not only would the VPPA prohibit the "knowing[] disclos[ure], to any person, [of] personally identifiable information . . . ."[130] but also the knowing disclosure of *non-PII* to any person that *may possess or have access to information that could re-identify the non-PII*.[131] The District Court for the Southern District of New York articulated the consequences of this argument in *Robinson v. Disney*, "[i]f nearly any piece of information can, with enough effort on behalf of the recipient, be combined with other information so as to identify a person, then the scope of PII would be limitless."[132] As such, the broad interpretation of PII embraced by the *Yershov* courts has been rejected by several courts before, and, for the reasons enumerated above, I anticipate the First Circuit will be an outlier on this issue for the foreseeable future.

2. GPS Location Is Not PII

Unlike the unique device identifier there was no caselaw on point prior to *Yershov* that addressed whether GPS location data is PII. However, just like the device identifier, GPS location does not identify a particular person. Rather, it

125. *See, e.g.*, *In re* Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 290 (3d Cir. 2016) ("[P]ersonally identifiable information under the Video Privacy Protection Act means the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior."); Ellis v. Cartoon Network, Inc., 2014 WL 5023535, *12 (N.D. Ga. Oct. 8, 2014) ("Without more, an Android ID does not identify a specific person."); *In re* Hulu Privacy Litigation, 2014 WL 1724344 (holding that a Hulu user ID—"without more"— is not personally identifiable information).

126. Perhaps obvious but worth noting, a unique device identifier does not transfer when a user gets a new device, therefore, the number is somewhat transitory depending on how often a device is replaced.

127. *See Understanding Online Advertising: How Does It Work*, NETWORK ADVERT. INITIATIVE, http://www.networkadvertising.org/understanding-online-advertising/how-does-it-work, (last visited Dec. 4, 2016).

128. *See* THE ECONOMIST, *supra* note 28.

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

130. 18 U.S.C. § 2710(b) (2012).

131. *See also* Kristian Stout, *Pushing Ad Networks Out of Business: Yershov v. Gannett and the War Against Online Platforms*, TRUTH ON THE MARKET (May 10, 2016), https://truthonthemarket.com/2016/05/10/pushing-ad-networks-out-of-business-yershov-v-gannett-and-the-war-against-online-platforms/.

132. Robinson v. Disney, 152 F. Supp. 3d 176, 181 (S.D.N.Y. 2016).

identifies a location. The *Yershov* courts equated the GPS location data to a home address.[133] However, while every home address is a location, certainly not every location is a home address. The GPS location would show wherever the video was watched—and maybe it *was* watched at a house, but not *necessarily* a house that identifies the particular viewer, which is what the statute requires.[134] The user might only watch videos away from home where he can find Wi-Fi access, if he is one of the one-third of Americans without home broadband service.[135] A GPS location might also identify a supermarket checkout line or a classroom at a law school, or any other place where there are people watching video clips daily. Or it could identify a building in Manhattan, but perhaps not the floor the video was watched on, because a smartphone GPS may not be able to calculate elevation.[136] While it is tempting to equate GPS location to a home address, it is simply too far a stretch and requires too many assumptions to be considered PII.

Even taken together, the Android ID and GPS location require too many additional steps and too many assumptions to be PII. The statute requires that information "identify a person," and that standard is simply not met with a video viewed on an anonymous device in a location that cannot be assumed to be associated in any identifiable way to the owner of the device—or the viewer of the video.

B. Yershov Is Not a Consumer

In order to trigger a VPPA violation, the disclosed PII must identify a "consumer" of the video service provider. The Act defines a consumer as "a renter, purchaser, or subscriber."[137] Yershov claims to be a "subscriber," a term which is neither statutorily defined nor elucidated in the legislative history. The First Circuit came to two conclusions in its analysis of the word "subscriber": (1) a monetary payment is not a necessary element;[138] and (2) subscription need only be "an agreement to . . . be allowed access to electronic text or services."[139]

First, the court pursued the "plain and ordinary meaning" of the word "subscriber" by surveying dictionary definitions.[140] However, instead of relying on "consensus dictionary definitions,"[141] the First Circuit selected what appears to be the *only* definition available that does not require monetary payment, signature, or other additional affirmative action.[142] The definition of "subscription" that the court

---

133. Yershov v. Gannett Satellite Network, Inc., 104 F. Supp. 3d 135, 142 (D. Mass. 2015) *rev'd*, 820 F.3d 482, 486 (1st Cir. 2016).

134. *See* 18 U.S.C. § 2710(a)(3) (2012); S. REP. NO. 100–599, at 12 (1988).

135. John B. Horrigan & Maeve Duggan, *Home Broadband 2015*, PEW RESEARCH CENTER (Dec. 21, 2015), http://www.pewinternet.org/2015/12/21/home-broadband-2015/.

136. Craig Timberg, *Cell Phone Tracking: Find an Address? Easy. But New Devices Can Calculate Your Altitude*, THE WASH. POST (Nov. 19, 2014), https://www.washingtonpost.com/business/technology/cellphone-tracking-find-an-address-easy-but-new-devices-can-calculate-youraltitude/2014/11/19/a47a85b2-6a85-11e4-b053-65cea7903f2e_story.html?utm_term=.9234f83265a3.

137. 18 U.S.C. § 2710(1).

138. Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 488 (1st Cir. 2016).

139. *Id.* at 487 (quoting AMERICAN HERITAGE DICTIONARY 1726 (4th ed. 2000)).

140. *Id.* at 487 (quoting *In re* Hill, 562 F.3d 29, 32 (1st Cir. 2009)).

141. WILLIAM N. ESKRIDGE, INTERPRETING LAW: A PRIMER ON HOW TO READ STATUTES AND THE CONSTITUTION app. at 409 (2016) (collecting the Supreme Court's canons of statutory interpretation).

142. *See* Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1255 (11th Cir. 2015); Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 147 (D. Mass. 2015).

favors reads, "[a]n agreement to receive or be given access to electronic texts or services."[143] But even under this definition, to classify Yershov's unilateral act of downloading Gannett's free app, with no other communication between the two parties, cannot be called an "agreement." The court goes on to describe the interaction a different way, as Yershov having "provided Gannett with consideration," the consideration being Yershov's information.[144] But this too is misleading. To "provide" something to someone infers the element of knowledge or intent,[145] yet it would seem that Yershov was oblivious to Gannett's collection of the data. That Gannett took the data cannot be evidence of an agreement.

The court also seems to have overlooked the first step of the ordinary meaning rule: "Follow the ordinary (also, 'everyday'; or 'commonsense') meaning of the statutory texts . . . . A statute has an ordinary meaning if you'd use its terminology in normal conversation 'without having other people look at you funny.'"[146] Most people, either in 1988 or today, would not question what Congress meant by "subscriber." It is not a highly technical term like PII, but rather, in the context of "renter, purchaser, or subscriber,"[147] it is a word used in everyday speech to mean one of two things: (1) "[a] person who makes a regular payment in return for entitlement to receive a periodical, membership of a society, access to a commercially provided service, etc.;"[148] or (2) "[a] person who adds his or her details to an electronic newsgroup, mailing list, etc., in order to receive, or contribute to, its contents; a person who has signed up to receive messages or other information from a newsgroup, mailing list, etc."[149] According to the complaint, Yershov neither paid money, nor did he actually sign up to receive any information from Gannett. Thus, the action cannot fall under the ordinary, everyday meaning of "subscriber."

In sum, under no definition of "subscriber" does the relationship between Yershov and Gannett fall. Even the definition embraced by the First Circuit fails, without more, to evidence an "agreement" between Yershov and Gannett. Moreover, the broad interpretation by the First Circuit creates a definition that is vastly over-inclusive, and would almost certainly apply not only to viewers of videos via free mobile app download, but to viewers of videos on websites as well, a consequence that the First Circuit explicitly attempted to exclude from its decision.[150]

C. The Implications of the 2012 Amendment to the VPPA

One additional argument in support of a narrower interpretation of the definitions for both PII and subscriber is the fact that Congress amended the Act in

---

143. Yershov, 820 F.3d at 487 (quoting AMERICAN HERITAGE DICTIONARY 1726 (4th ed. 2000)).

144. *Id.* at 489.

145. *See Provide*, MERRIAM-WEBSTER THESAURUS, https://www.merriam-webster.com/thesaurus/provide (last visited Dec. 4, 2016) ("to put (something) into the possession of another for use or consumption;" synonyms include "deliver, feed, give . . . furnish supply.").

146. ESKRIDGE, *supra* note 141, at 407.

147. 18 U.S.C.A. § 2710(a)(1) (2012).

148. *Subscriber*, OED ONLINE, http://www.oed.com/view/Entry/192954?redirectedFrom=subscriber (last visited Dec. 03, 2016).

149. *Id.*

150. Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 489 (1st Cir. 2016); *see also* Kristian Stout, *Pushing Ad Networks Out of Business: Yershov v. Gannett and the War Against Online Platforms*, TRUTH ON THE MARKET (May 10, 2016), https://truthonthemarket.com/2016/05/10/pushing-ad-networks-out-of-business-yershov-v-gannett-and-the-war-against-online-platforms/.

2012 without updating either definition.[151] Included in the appendix of the Senate Subcommittee Hearing transcript was a submission by the Electronic Privacy Information Center ("EPIC"). EPIC urged the committee to: (1) reject the proposed amendment regarding electronic opt-in consent; and (2) enact an amendment to the definition of PII that would plainly include IP addresses and unique identifying numbers.[152] Unfortunately, the Senate Subcommittee did not explicitly address EPIC's second recommendation at the hearing, leaving the VPPA's definition of PII as ambiguous as it ever was.

However, an earlier House Report may suggest a narrower reading of the PII definition. The Report explicitly states, "[t]his legislation does not change . . . the definition of 'personally identifiable information' . . . ."[153] It goes on to explain, "the committee does not intend for this clarification to negate in any way existing laws, regulations and practices designed to protect the privacy of children on the Internet,"[154] referring specifically to the broader, and more technologically current, definition of PII in COPPA,

> [COPPA] and its regulations apply to individually identifiable information about a child that is collected online, such as full name, home address, email address, telephone number or any other information that would allow someone to contact the child. The Act and Rule also cover other types of information—for example, hobbies, interests and *information collected through cookies or other types of tracking mechanisms*—when they are tied to individually identifiable information.[155]

The House Report seems to mark the clear differences between the definitions of PII in the VPPA and in COPPA. Essentially, the House Report acknowledges that while the VPPA amendment will *not* broaden the definition of PII to include all that is covered by COPPA, the narrower definition of PII in the VPPA does not negate COPPA's definition when regulating videos watched by children.

Some might argue that because Congress had the opportunity to expand the VPPA's definitions of PII and subscriber but chose not to, that this is an indication that Congress intended the definitions of both terms to be construed narrowly.[156] However, a better argument for the narrow interpretation of each term is that the VPPA is, by most opinions, an antiquated statute and to stretch the scope of the statute to encompass the facts of this situation, and others like it, is a misapplication of the law.

---

151. Video Privacy Protection Act Amendments Act of 2012, Pub. L. No. 112-258 § 2, 126 Stat. 2414 (codified as amended at 18 U.S.C.A. § 2710(2)(B) (2012)).

152. *Id.* at 59-60.

153. H.R. REP. NO. 112-312, at 3 (2011).

154. *Id.*

155. *Id.* (emphasis added).

156. It is generally understood that Congress's inaction is not firm ground on which to base an argument for a particular interpretation of a statute. *See, e.g.*, United States v. Craft, 535 U.S. 274, 287 (2002) ("We have elsewhere held, however, that failed legislative proposals are 'a particularly dangerous ground on which to rest an interpretation of a prior statute,' reasoning that '[c]ongressional inaction lacks persuasive significance because several equally tenable inferences may be drawn from such inaction . . . .'") (citations omitted).

VI. CONCLUSION: TRANSPARENCY AND CONSUMER CHOICE

In recent years, both the House of Representatives and the Senate have introduced sweeping legislation aimed at the collection, maintenance, security, and disclosure of consumer data, especially that by third-party data collectors.[157] In 2015 alone, five bills legislating commercial use and storage of data—which would delegate rulemaking authority to the FTC—were introduced in Congress.[158] None of these bills have been enacted, perhaps due to significant lobbying efforts in opposition to such regulation.[159]

While the FTC itself has advocated for more government regulation of consumer data collection,[160] it has also made statements in support of the ad tech community's effort to self-regulate.[161] It has repeatedly applauded the efforts of self-regulatory associations,[162] and continues to work with these associations to advance best practices in the industry as technology evolves.[163] This is largely because self-regulation is flexible in a way that federal and state legislation and regulation is not. Advertising technology is a constantly evolving landscape; which means the ability for self-regulation to respond quickly—and even stay ahead of—changes in the

---

157. In addition to the legislative action of recent years, the Obama Administration had paid significant attention to the collection of consumer data, and advocated for more regulation. *See, e.g.*, THE WHITE HOUSE, EXEC. OFFICE OF THE PRESIDENT, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf; *see also* Natasha Singer, *White House Proposes Broad Consumer Privacy Bill*, N.Y. TIMES, Feb. 27, 2015, http://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data-privacy-bill.html?_r=0. It remains unclear how the Trump Administration views the practices of the ad tech industry, although it appears President Trump tends to lean toward less regulation of industry in general. Perhaps the best clue in support of this view thus far is the roll back by Congress and President Trump of an FCC rule approved in October 2016 that required ISPs to get consumer consent before collecting a user's online activity data. *See* Steve Lohr, *Trump Completes Repeal of Online Privacy Protections From Obama Era*, N.Y. TIMES (Apr. 3, 2017), https://www.nytimes.com/2017/04/03/technology/trump-repeal-online-privacy-protections.html?_r=0.

158. Data Security Act of 2015, H.R. 2205, 114th Cong. (2015); Data Security Act of 2015, S.961, 114th Cong. (2015); Data Security and Breach Notification Act of 2015, H.R.1770 (114th Cong. (2015); Data Security and Breach Notification Act of 2015, S.177, 114th Cong. (2015); and Secure and Protect Americans' Data Act, H.R. 4187 (114th Cong. (2015).

159. *See, e.g.*, Kate Kaye, *Big Data Goes to Washington—And Spends Lots of Money*, AD AGE (March 11, 2013), http://adage.com/article/dataworks/big-data-washington-spends-lots-money/240232/.

160. *See generally* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

161. *See* FED. TRADE COMM'N, FEDERAL TRADE COMMISSION ISSUES REPORT ON ONLINE PROFILING (July 27, 2000), https://www.ftc.gov/news-events/press-releases/2000/07/federal-trade-commission-issues-report-online-profiling ("The Commission unanimously applauded the Network Advertising Initiative (NAI) for developing an innovative self-regulatory proposal which addresses the privacy concerns consumers have about online profiling."); FED. TRADE COMM'N, CROSS-DEVICE TRACKING (2017), https://www.ftc.gov/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017 ("FTC staff commends these self-regulatory efforts to improve transparency and choice in the cross-device tracking space.").

162. *See id.*

163. *See* Jessica Rich, *Keeping Up with Online Advertising*, FED. TRADE COMM'N: BUSINESS BLOG (Apr. 21, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry.

market is a critical benefit.[164] Moreover, businesses that align themselves with self-regulatory associations indicate to consumers an organizational character for trustworthiness. Research has shown that consumers are concerned with the commercial collection of data,[165] and will share data more willingly with trustworthy companies.[166] Therefore, in a Darwinian fashion, the companies that maintain data trustworthiness will flourish, and those who do not will wither.

To build consumer trust, both the FTC and self-regulatory associations agree that companies must embrace data collection transparency.[167] Transparency is three-fold: first, companies—including both first- and third-party data collectors—should develop and present simple and clear data collection and security policies to consumers. Second, companies should educate consumers about what data they collect, and how it is used and secured. Third, companies should create pathways for consumers to access the data that is collected, and create procedures to correct any inaccuracies.[168]

A related principle to transparency generally encouraged by both the FTC and self-regulatory associations is consumer choice. Developing company policies and programs that allow consumers to choose which data they share and to whom it is disclosed is an important policy with which consumer advocates and the ad tech sector are still grappling.[169]

It can be said that the self-regulation model is a healthy compromise between pure market control and rigid government regulation. In this sense, with regard to the VPPA and the evolution of video data and advertising technology, consumers would be best-served outside of the court system. Instead, such concerns are better addressed by self-regulatory policies and enforcement procedures. The fact is, more and more mobile technology consumers are becoming educated about data collection and dissemination, and mobile companies will be forced to comply with the recommendations of such self-regulatory associations, or be abandoned by their customers. And while information privacy in the world of the mobile internet will likely remain a slippery issue, a combination of consumer education and market forces may be the key to achieving a satisfactory balance between consumer privacy and the mobile internet as we know it.

---

164. *See* Maureen K. Ohlhausen, Commissioner, Fed. Trade Comm'n, Address at the BBB Self-Regulation Conference: Strategies to Bring to the Mobile and Global Era (June 24, 2014); Siona Listokin, *Industry Self-Regulation of Consumer Data Privacy and Security*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 15, 16 (2015).

165. Morey, Forbath & Schoop, *supra* note 44.

166. *Id.*

167. *Id.*; *see also* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, at 60 (2012); *Who We Are: History*, NETWORK ADVERTISING INITIATIVE, http://www.networkadvertising.org/about-nai/history (last visited Feb. 17, 2017); Listokin, *supra* note 164, at 20.

168. *E.g.* FED. TRADE COMM'N, *supra* note 167, at 60.

169. *Id.* at 35.