

THE MIRAGE OF META PIXEL CODE: REDEFINING PII IN THE ERA OF GENERATIVE AI

Sophie Venter*

Data privacy laws are intended to put consumers in control of whether their identifying data can be sold and used for targeted advertising. However, these laws do not provide adequate protections in the era of generative artificial intelligence (AI). This Note examines one way that existing privacy law permits companies to profit from selling data for targeted advertising without obtaining user consent: transferring video-watching data in a pixel code. Some U.S. Courts of Appeals have determined that these data transfers do not sufficiently identify users and the videos they watched to constitute violations of user privacy. This has led to a circuit split over the Video Privacy Protection Act's (VPPA) definition of personally identifiable information (PII). The VPPA requires consent before disclosing PII but does not precisely define which data constitutes PII. The U.S. Court of Appeals for the First Circuit uses a reasonable foreseeability standard to determine whether data constitutes PII, and the U.S. Courts of Appeals for the Second, Third, and Ninth Circuits use the ordinary person standard. There is a further split among the courts that apply the ordinary person standard over whether the ability of AI tools to decode the pixel data should factor into a court's analysis.

In addressing this issue, this Note considers widespread access to generative AI that can decode pixel code. It poses two possible solutions to the circuit split and AI's impact on the encryption of pixel code: implementing a new federal privacy law and clarifying whether pixel codes constitute personally identifiable information according to the U.S. Supreme Court. This Note argues that courts should use the ordinary person standard with consideration of the availability and advancement of generative AI.

INTRODUCTION	418
I. THE VPPA AS A MECHANISM TO REGULATE DATA	422
A. The History of the VPPA	422

* J.D. Candidate, 2027, Fordham University School of Law; B.A., 2024, Georgetown University. Thank you to Professor Olivier Sylvain and my primary editor, copyeditors, and footnoters from the *Fordham Law Review* for their editing and guidance. Thank you to my parents, grandparents, and friends for their encouragement and support.

B. Targeted Advertising and the Attention Economy.....	423
C. The Role of AI in Targeted Advertising.....	424
D. Cookies and Meta Pixels.....	426
II. THE TARGETED ADVERTISING LOOPHOLE IN THE VPPA AND THE FAILED ATTEMPTS TO RESOLVE IT	427
A. The Reasonable Foreseeability Standard.....	429
B. The Ordinary Person Standard	430
C. Considering Generative AI When Evaluating Pixel Codes	432
D. Approaches for Resolving the Circuit Split.....	435
E. Data Protections in the European Union.....	437
F. Proposed U.S. Regulation of Targeted Ads.....	438
III. REGULATING THE SALE OF PERSONAL DATA FOR TARGETED ADVERTISING	440
A. Counteracting the Unwillingness to Meaningfully Consent.....	441
B. Evaluating Existing Solutions.....	441
C. Limiting Data Collected Without Consent	443
1. The First Path: A Federal Privacy Law Regulating Targeted Advertising.....	443
2. The Second Path: Addressing Privacy Concerns About the VPPA Directly.....	445
CONCLUSION	445

INTRODUCTION

Each time Detrina Solomon watched a video through her subscription to Flippo Media, Inc. (“Flippo”), Flippo sent Facebook a sequence of characters that revealed Solomon’s video-watching history and Facebook ID.¹ When Solomon discovered that her data had been sold to Facebook without her consent, she pursued legal action against Flippo.² Solomon’s ability to choose how Flippo could use her data turned on whether the characters Flippo sent to Facebook were considered personally identifiable information (PII) under the Video Privacy Protection Act³ (VPPA).⁴ The VPPA is a data privacy law that applies to subscribers’ video-watching data.⁵ The VPPA defines PII as “information which identifies a person as having requested or obtained specific video materials or services from a video tape service

1. See *Solomon v. Flippo Media, Inc.*, 136 F.4th 41, 43 (2d Cir. 2025).

2. See *id.*

3. 18 U.S.C. § 2710.

4. See *Solomon*, 136 F.4th at 44.

5. See § 2710(b)(1).

provider.”⁶ When PII is transmitted from video service providers without consent, the VPPA provides the subscribers with a private cause of action.⁷

Solomon’s data is valuable to Facebook for its ability to inform targeted ads based on Solomon’s streaming history.⁸ At issue in *Solomon v. Flippis Media, Inc.*⁹ and other Meta Pixel¹⁰ cases¹¹ was Meta’s¹² use of data from video streaming services to create targeted ads on Meta sites.¹³ Through incorporating predictive artificial intelligence (AI) tools, Meta and Google have created even more precise targeted ads, increasing each company’s value to \$1 trillion.¹⁴ Until relatively recently, few VPPA cases were litigated.¹⁵ It is only within the last six years that consumers and policymakers have really begun to understand the “scale and pervasive integration of the market for user data” and turned to the VPPA for redress.¹⁶ Now, subscribers can bring lawsuits against streaming services and other websites under the VPPA.¹⁷ Subscribers argue that streaming services like Triller TV (formerly known as FITE) are infringing on their privacy rights under the VPPA when the services sell subscriber information to companies that create targeted ads without asking for consent.¹⁸

Unlike walking into a video rental store and renting videos, modern subscribers like Detrina Solomon may not be aware that they are subscribers

6. *Id.* § 2710(a)(3).

7. *See id.* § 2710(b)(1).

8. *See* Matt Dumiak, *Avoiding Meta Pixel Lawsuits*, WIPFLI: BLOG (Dec. 11, 2024), <https://www.compliancepoint.com/privacy/avoiding-meta-pixel-lawsuits/> [<https://perma.cc/5AQ8-UG99>].

9. 136 F.4th 41 (2d Cir. 2025).

10. Meta Pixel is a piece of code applied to websites that operates as a targeting tool to automatically extract data from website users and predict which users will be interested in certain products, and then, using AI, push ads for those products to the consumers. *See How Does Facebook Use AI for Advertising?*, DATAFEEDWATCH: BLOG, <https://www.datafeedwatch.com/blog/ai-facebook-advertising/> [<https://perma.cc/4STA-28KM>] (last visited June 19, 2026). Meta Pixel is also informed by how users interact with Meta’s AI. *See* Alex Valdes, *Meta Will Use Your AI Interactions to Personalize Ads and Content*, CNET (Oct. 2, 2025, at 13:19 PT), <https://www.cnet.com/tech/services-and-software/meta-will-use-your-ai-interactions-to-personalize-ads-and-content/> (on file with the *Fordham Law Review*).

11. *See, e.g.*, *Hughes v. NFL*, No. 24-2656, 2025 U.S. App. LEXIS 15216, at *3 (2d Cir. June 20, 2025); *Manza v. Pesi, Inc.*, 784 F. Supp. 3d 1110, 1116 (W.D. Wis. 2025); *Garcia v. Bandai Namco Ent. Am. Inc.*, No. 25-cv-00967, 2025 U.S. Dist. LEXIS 152616, at *8 (C.D. Cal. Aug. 7, 2025); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 981 (9th Cir. 2017).

12. Meta is the parent company of networking websites including Facebook, Instagram, and WhatsApp. Iain Wicks, *What Is Meta: A Comprehensive Overview*, STONEHOUSE COMM’NS (Feb. 3, 2025), <https://stonehousecomms.co.uk/one-pagers/what-is-meta-a-comprehensive-overview> [<https://perma.cc/7Q3H-9HPN>].

13. *See Solomon*, 136 F.4th at 46; Dumiak, *supra* note 8.

14. MADHUMITA MURGIA, CODE DEPENDENT: LIVING IN THE SHADOW OF AI 4 (2024).

15. *See* Elizabeth Gemdjan, Note, *The Extraordinary Extension of the Video Privacy Protection Act: Why the “Ordinary Course of Business” of an Analog Era Is Anything but Ordinary in the Digital World*, 90 BROOK. L. REV. 553, 554 (2025).

16. Olivier Sylvain, *The Market for User Data*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1087, 1097 (2019).

17. *See Solomon*, 136 F.4th at 47.

18. *See id.* at 46–47.

or that they access content that falls under the VPPA. The language of the VPPA is facially vague, stating that it protects subscribers of goods or services without defining subscribers, goods, or services in a manner that applies to modern streaming.¹⁹ For example, the U.S. Court of Appeals for the Second Circuit in *Salazar v. National Basketball Association*²⁰ established that an online newsletter published by the NBA constitutes a “good or service” under the VPPA, explaining that the Act is not limited to audiovisual content.²¹ Meanwhile, the U.S. Court of Appeals for the First Circuit found that consumers do not need to pay for video content to be a subscriber.²² Free video content is often available at no cost because companies extract users’ personal data to sell: “[T]hese companies offering free online video content rely on consumers’ personal information to operate and often need to share this information with third parties to be able to function, which means that consumers’ data privacy is put at risk on a regular basis.”²³

The Federal Trade Commission’s (FTC) adjudication of data privacy claims demonstrates a punitive approach to resolving unlawful data transfers.²⁴ The FTC regulates data transfers through its prohibition of “unfair methods” and “deceptive acts and practices” in commerce, though its regulations do not define PII.²⁵ One notable instance where the FTC regulated data transfers was a class action against VIZIO, a smart television company, that allegedly collected data from eleven million televisions without consumer consent.²⁶ The complaint alleged that VIZIO sold the data to third parties for targeted advertising.²⁷ After purportedly collecting IP addresses in connection with the date, time, and channels that viewers

19. 18 U.S.C. § 2710.

20. 118 F.4th 533 (2d Cir. 2024).

21. *Id.* at 536. *Salazar* also held that the plaintiff had standing for the disclosure of their video-watching history. *See id.* at 544; Jeeyoon Lim, Note, *Is Your Data Good, Bad, or Neutral?: Redefining Concreteness for Data Breach Harms*, 94 FORDHAM L. REV. 299, 327 (2025) (“[D]isclosure can be sufficiently ‘public,’ even if only to one party, depending on the ‘nature of the companies involved, intended and potential uses of the disclosed information, and the resulting enhanced disclosure risks.’” (quoting *Salazar*, 118 F.4th at 544)).

22. *Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482, 487–89 (1st Cir. 2016) (finding that downloading the *USA Today* app was sufficient to establish a subscription where there is “seamless access” to the content via the app and plaintiff provided valuable personal information as consideration).

23. Gemdjian, *supra* note 15, at 556.

24. *See Vizio Agrees to \$17M Settlement to Resolve Smart TV Class Action Suit*, HUNTON ANDREWS KURTH LLP (Oct. 8, 2018), <https://www.hunton.com/privacy-and-information-security-law/vizio-agrees-17m-settlement-resolve-smart-tv-class-action-suit> [<https://perma.cc/25WM-6HYC>].

25. 15 U.S.C. § 45(a)(1).

26. *See* Press Release, Fed. Trade Comm’n, VIZIO to Pay \$2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions Without Users’ Consent (Feb. 6, 2017), <https://www.ftc.gov/news-events/news/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it-collected-viewing-histories-11-million> [<https://perma.cc/QV4E-XHC3>].

27. *See id.*

watched without their consent, VIZIO settled the claim for \$17 million.²⁸ The FTC has also tightened restrictions on the sale of personal data for targeted advertising by health companies, though they have not yet addressed the sale of all types of data.²⁹ When the FTC discovered that BetterHelp, a mental health provider, violated section 5 of the Federal Trade Commission Act³⁰ (“FTC Act”) in its disclosure of consumers’ health data for targeted advertising, the FTC did not just require consent for the sale to occur but also banned BetterHelp from sharing “individually identifiable information relating to the past, present, or future physical or mental health or condition(s) of a consumer with any third party,” regardless of consent.³¹

This Note explores the extent to which consent is needed for personal data to be sold for targeted advertising. While there are a variety of ways companies monetize consumers’ personal data, this Note focuses on targeted advertising as one way that current law has enabled companies to exploit consumer data.³² It investigates the VPPA’s protection of video-watching history as an area where there is a lack of clarity in existing law that leaves consumers and companies vulnerable. Appellate judges have come to varying conclusions about how to best adapt the VPPA to streaming services and novel video platforms.³³ These conclusions do not provide lasting consumer protections when AI is widely used to extract consumer information and increase profits.

This Note focuses on the split judicial interpretations of PII under the VPPA. It then suggests an approach to the sale of targeted ads that resolves the circuit split and closes the loophole in which companies can collect data without user consent. Part I discusses the history of the VPPA and its attempts to safeguard consumers’ PII, as well as the role of personal data and the effects of AI on the attention economy. Part II delves into the circuit split between the U.S. Court of Appeals for the First Circuit and the U.S. Courts of Appeals for the Second, Third, and Ninth Circuits concerning the definition of PII under the VPPA. Part III proposes solutions for regulating the consent requirement, including resolving the circuit split via a new federal data privacy law or the U.S. Supreme Court.

28. See *Vizio Agrees to \$17M Settlement to Resolve Smart TV Class Action Suit*, *supra* note 24.

29. See BetterHelp, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 88 Fed. Reg. 15717, 15719 (Mar. 14, 2023).

30. 15 U.S.C. §§ 41–58.

31. *Id.*

32. Another pertinent way is the collection of data to train AI models. See *How Your Data Is Used to Improve Model Performance*, OPENAI (Oct. 8, 2025), <https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance> (on file with the *Fordham Law Review*).

33. See *Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482, 484 (1st Cir. 2016); *Solomon v. Flipp Media, Inc.*, 136 F.4th 41, 52 (2d Cir. 2025).

I. THE VPPA AS A MECHANISM TO REGULATE DATA

To delve into the application of the VPPA to Meta Pixel cases and consumer privacy issues, it is necessary to provide context on the history of the VPPA and the information that it regulates. Part I.A discusses the history of the VPPA, Part I.B introduces the attention economy and the role of targeted advertising, Part I.C explores the use of AI in targeted advertising, and Part I.D provides information on cookies and Meta Pixel.

A. *The History of the VPPA*

The VPPA was enacted in 1988 in the wake of the publication of the video rental history of U.S. Supreme Court nominee, Judge Robert H. Bork.³⁴ At this time, prior to the enactment of the VPPA, there were very few codified consumer privacy protections. During Judge Bork's confirmation hearings, it became clear that he did not want to extend privacy protections beyond those "specifically conferred by legislation."³⁵ In response to Judge Bork's views on data privacy, a journalist asked Judge Bork's video rental store for an exhaustive list of videos he had rented within the past two years.³⁶ The store lawfully provided the list identifying Judge Bork and his video rental history, consisting of 146 titles.³⁷ Once the journalist published the list, members of Congress were stunned that Bork's video rentals could so easily become public knowledge.³⁸ While debating the passage of the VPPA, U.S. Senator Patrick Leahy argued, "[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 free and we cherish our freedom and we want our freedom. We want to be left alone."³⁹ Congress passed the VPPA within the year.⁴⁰

The VPPA was intended to increase privacy protections and expand consumers' right to privacy; its U.S. Senate report states that it was enacted to "preserve personal privacy with respect to the rental, purchase or delivery of video tapes or similar audio visual materials."⁴¹ Adequately stating a claim under the VPPA requires the plaintiff to "plausibly allege that (1) a

34. See Anna O'Donnell, *Why the VPPA and COPPA Are Outdated: How Netflix, YouTube, and Disney+ Can Monitor Your Family at No Real Cost*, 55 GA. L. REV. 467, 471 (2020).

35. See Brett Burney, *From Blockbuster to Meta: The Evolution of the Video Privacy Protection Act to Class Action Lawsuits*, PAGEFREEZER (Oct. 30, 2023), <https://blog.pagefreezer.com/the-video-privacy-protection-act-class-action-lawsuits> [<https://perma.cc/9BTK-DZXN>].

36. See *id.*

37. See *id.*

38. See *id.* Though Judge Bork's confirmation hearings were contentious, his video choices were not. See Burney, *supra* note 35.

39. S. REP. NO. 100-599, at 6 (1988) (quoting *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. 1374 (1987)).

40. See Burney, *supra* note 35.

41. S. REP. NO. 100-159, at 1 (1988).

video tape service provider (2) knowingly disclosed to any person (3) personally identifiable information concerning her use of the service.”⁴² The VPPA defines “personally identifiable information” as “information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.”⁴³

Despite being enacted to address specific problems, VPPA litigation now concerns a variety of online video streaming services.⁴⁴ In 2013, the VPPA was amended to clarify that it was applicable to online media as well as the brick-and-mortar shops its writers had in mind at the time of its enactment.⁴⁵ In recent years, digital media streaming has displaced the video stores of the 1980s and the VPPA is now mostly relevant for streaming services.⁴⁶ Yet, Congress has left the VPPA largely unchanged since its initial enactment, producing a circuit split as appellate courts strive to uphold the VPPA and protect PII amid a changing media landscape.⁴⁷ With the advent of Meta Pixel, streaming services have a strong monetary incentive to sell subscribers’ video-watching data to Meta platforms, underscoring the need for a uniform definition of PII that protects consumers and prioritizes privacy over profit.

B. Targeted Advertising and the Attention Economy

Years ago, there were areas of life deemed “sanctuaries” protected from commercial advertising.⁴⁸ As technology has become further and further integrated into daily life, so have advertisements; now “nearly every bit of our lives is commercially exploited to the extent it can be.”⁴⁹ Over the past two centuries, adults have gone from being ambivalent about news outside of their local communities, as delivered by regional newspapers,⁵⁰ to being

42. *Solomon v. Flippis Media, Inc.*, 136 F.4th 41, 44 (2d Cir. 2025).

43. 18 U.S.C. § 2710(a)(3).

44. See Nicola Menaldo, James G. Snell, Charles C. Sipos & Stephanie Duchesneau, *Be Kind, Don't Rewind: The VPPA's Reemergence in Privacy Class-Action Litigation*, PERKINS COIE (Mar. 28, 2023), <https://perkinscoie.com/insights/update/be-kind-dont-rewind-vppas-reemergence-privacy-class-action-litigation> [<https://perma.cc/35CY-VWZS>] (“As the manner in which people consumed video content evolved, so too did the potential considerations raised by the VPPA. In 2013, as rising tech company Netflix was launching its streaming service, it successfully lobbied Congress for an exception that allowed for the disclosure of VPPA-covered PII with a consumer’s consent, unlocking new possibilities for the social sharing of viewing information.”).

45. See Gemdjian, *supra* note 15, at 554.

46. *Id.* at 554–55.

47. See, e.g., *Solomon*, 136 F.4th at 52–54; *Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482, 487–89 (1st Cir. 2016).

48. See TIM WU, *THE ATTENTION MERCHANTS: THE EPIC SCRAMBLE TO GET INSIDE OUR HEADS* 5 (2016) (“There was once a time when, whether by convention or technological limitation, many parts of life . . . were sanctuaries, sheltered from advertising and commerce.”).

49. *Id.*

50. Benjamin Day created the *New York Sun* in 1833, which was novel for two reasons: (1) it was aimed at the general public, not just the elite; and (2) it was created at a financial loss. See *id.* at 11–12. Day financed the business by reselling audiences’ attention to

invariably connected to the rest of the world, including marketers.⁵¹ Savvy companies know that human attention is a commodity, and their strategy of breaking into these “sanctuaries” has succeeded in harvesting attention at such a rate that it has now become “a major part of our economy.”⁵²

In the early 2000s, as Google became ubiquitous, it decided to include advertisements as a revenue stream.⁵³ Google capitalized on the fact that its users were “plainly expressing a commercial intent” to show them fewer, but more specific advertisements tailored to what they had input into the search engine—an approach known as targeted advertising.⁵⁴ At an event hosted by the Electronic Privacy Information Center in 2015, the chief executive officer of Apple remarked that “some of the most prominent and successful companies have built their businesses by lulling their customers into complacency about their personal information They’re gobbling up everything they can learn about you and trying to monetize it. We think that’s wrong.”⁵⁵

Trading attention and data in exchange for advertisements and deals is not innately problematic, nor is it something that privacy laws such as the VPPA seek to ban altogether. Rather, the VPPA attempts to define what data is sufficiently identifying and to require that companies involve subscribers in the decision to sell that data.⁵⁶ The VPPA prioritizes subscriber consent because consent “legitimizes activities that would otherwise be illegitimate, immoral, or illegal.”⁵⁷ When consumers consent, they agree to share their data with advertisers, a process that one scholar describes as turning “the crash crop of attention into an industrial commodity.”⁵⁸ When subscribers are not asked for their consent, companies make this deal on their behalf. Whether this is lawful depends on the standard used to determine whether the data, such as Meta Pixel code, constitutes PII.

C. The Role of AI in Targeted Advertising

The use of AI to enhance the effectiveness and profitability of targeted advertisements has heightened their hypnotizing impact on the attention

advertisers in his newspaper. *See id.* Wu argues that “the world was never really the same” once Day’s business model succeeded. *Id.* at 14.

51. *See id.* at 11–12.

52. *See id.* at 6.

53. *See id.* at 263.

54. *Id.* at 263–64 (“Imagine a television channel that read your mind and showed you just one commercial an hour, keyed to your interests, reasoning that it would make you like that channel better: that was the early Google’s idea.”).

55. Matthew Panzarino, *Apple’s Tim Cook Delivers Blistering Speech on Encryption, Privacy*, TECHCRUNCH (June 2, 2015, at 14:34 PT), <https://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/> [https://perma.cc/TVH3-B4NA].

56. *See* 18 U.S.C. § 2710.

57. Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593, 596 (2024).

58. *See* WU, *supra* note 48, at 9.

economy.⁵⁹ Examining the role of AI in targeted advertising is necessary to understand the consequences of adequately defining PII under the VPPA in the era of generative AI. Advertisers know that inevitably every “once entrancing means of harvesting attention starts to lose its charm” as part of the “disenchantment effect.”⁶⁰ In response, “the attention merchant’s approach is always trending in the direction of going too far, almost to the point, sometimes even reaching it, of causing shock.”⁶¹ These effects have been exacerbated by the integration of AI.⁶² AI has become a ubiquitous presence in people’s lives, though it may often be invisible; author and AI journalist Madhumita Murgia wrote that “algorithm-based decisions and generative AI are woven deeply into our daily lives.”⁶³ One concern with companies’ use of AI is that people do not know that this technology is being used at all.⁶⁴ Even if people are aware of the use of AI, they may be powerless against its influence, while the companies that deploy it reap the benefits and profit from user data.⁶⁵

AI has greatly increased the efficacy of targeted advertising; it can evaluate the large quantities of data gathered via scraping⁶⁶ and make “highly accurate predictions that often outperform humans in executing important tasks.”⁶⁷ Though overemphasis on machine predictive algorithms has been criticized because machines cannot account for human decisions involving emotions or illogical factors,⁶⁸ AI still provides an opportunity for companies to more precisely target consumers than before.⁶⁹ Previously, advertisers would

59. See Melissa Russell, *AI Will Shape the Future of Marketing*, PRO. & EXEC. DEV.: HARV. DIV. CONTINUING EDUC. (Mar. 6, 2026), <https://professional.dce.harvard.edu/blog/ai-will-shape-the-future-of-marketing/> [<https://perma.cc/H6SK-FEX8>].

60. WU, *supra* note 48, at 23.

61. *Id.*

62. See Russell, *supra* note 59.

63. MURGIA, *supra* note 14, at 207.

64. See *id.*

65. Companies also use AI to create advertisements more quickly and at a more advanced level. See Russell, *supra* note 59.

66. Scraping is the collection of data in a manner that evades data privacy laws entirely. Daniel J. Solove & Woodrow Hartzog, *The Great Scrape: The Clash Between Scraping and Privacy*, 113 CAL. L. REV. 1521, 1523 (2024). AI often gathers data by scraping, which is “the automated extraction of large amounts of data from the internet.” *Id.* Scraping is cheap, quick, and does not involve asking for user consent or providing notice. See *id.* Scraping is not a new practice; “[i]t was used to build what we know as the World Wide Web.” *Id.* However, the introduction of AI systems that process scraped data has resulted in an increase in the amount of data scraped and the number of companies that use scraped data. See *id.* AI increases the utility of the scraped data. See *id.*

67. Daniel J. Solove & Hideyuki Matsumi, *AI, Algorithms, and Awful Humans*, 92 FORDHAM L. REV. 1923, 1926 (2024).

68. See *id.* at 1925 (“Machine decision-making currently cannot incorporate emotion, morality, or value judgments, which are essential components of decisions involving people’s welfare.”).

69. See Russell, *supra* note 59 (“When marketers develop strategies to figure out what consumers want, they traditionally have examined demographic trends and surveys, plus intuition and assumptions based on past performance. AI has changed that approach dramatically.”).

analyze market trends across demographics and buying habits.⁷⁰ Now, companies can analyze data from individual consumers, serving quicker and more personalized advertisements and prompting purchases based on predicted interests.⁷¹ One author noted that consumers even “expect brand interactions to feel customized to their needs,” and pitched AI to companies as a way to fulfill consumers’ expectations.⁷²

When companies collect data, including video-watching data, they can use AI to learn more information about consumers and, in turn, can extract profits at a novel rate.⁷³ The role of data privacy law is not to police the use of AI but rather to provide consumers with agency over their personal data. Given the deployment of AI for targeted advertising, the only mechanism through which consumers can have agency over their data is through the ability to consent. Their right to consent under the VPPA turns on whether the data is PII, even though non-PII data can still be used to inform companies about a consumer and their video-watching habits.⁷⁴

D. Cookies and Meta Pixels

Recent VPPA litigation concerns the transmission of user data to third-party advertisers.⁷⁵ The U.S. Court of Appeals for the Third Circuit defined cookies in *In re Nickelodeon Consumer Privacy Litigation*⁷⁶ as a “small text file that a web server places on a user’s computing device,” which “allow[s] a website to ‘remember’ information about a user’s browsing activities.”⁷⁷ The court further distinguished third-party cookies from first-party cookies.⁷⁸ Third-party cookies are placed on a computer by a party other than the host website.⁷⁹ First-party cookies are placed on a user’s computer by the website they visited.⁸⁰ Advertisers use third-party cookies because they, rather than the host website, place the cookies onto a user’s

70. *See id.*

71. *See id.* Companies use AI tools, including ChatGPT, Copilot, Gemini, Jasper AI, HubSoft, Optmyzer, and Synthesia to achieve this. *See id.*

72. *Id.*

73. *See id.* There is a concern that AI can detect sensitive information; scholars are investigating whether large language models can detect PII in code, finding that they have the potential to detect sensitive information such as PII but need additional training. *See* Ambarish Gujar, Jean L. Camp, Tatiana Ringenberg, Xinyao Ma, & Anesu Chaora, *Can Large Language Models Detect PII in Code?*, (Oct. 31, 2023) (unpublished manuscript) (<https://ssrn.com/abstract=4619112>) (on file with the *Fordham Law Review*).

74. *See* 18 U.S.C. § 2710(b)(1).

75. *See, e.g.,* *Solomon v. Flippis Media, Inc.*, 136 F.4th 41, 46 (2d Cir. 2025) (“Facebook then uses this information to build detailed profiles about FITE’s consumers, which enables FITE to present those same consumers with targeted advertisements.”).

76. 827 F.3d 262 (3d Cir. 2016).

77. *Id.* at 268.

78. *See id.*

79. *See id.*

80. *See id.*

browser.⁸¹ Using personal data to create user profiles has caused controversy in other industries as well.⁸²

Like cookies, pixels are also used to track consumers' data online and have been the concern of recent VPPA litigation.⁸³ Pixels are pieces of code that companies can embed in their website content to collect user data more reliably and quickly than cookies.⁸⁴ While cookies are stored directly on users' devices, pixels are part of the website's content.⁸⁵ Pixels are also more difficult for users to clear than cookies.⁸⁶ Meta Pixel is the pixel used to track consumer activity and the corresponding effectiveness of advertisements on Meta websites, such as Facebook and Instagram.⁸⁷ Subscribers often visit websites or streaming platforms that transmit their video-watching history to advertisers through Meta Pixel.⁸⁸

Although the VPPA applies whether cookies or pixels are used to track users, the pixel is perhaps more pernicious than the cookie for its efficacy at transmitting data and its difficulty to clear.⁸⁹ The central question courts are considering is whether the sale of users' pixel code violates the VPPA's privacy protections, or whether the pixel is sufficiently anonymized to prohibit identification of consumers and their video-watching history.

II. THE TARGETED ADVERTISING LOOPHOLE IN THE VPPA AND THE FAILED ATTEMPTS TO RESOLVE IT

The VPPA defines PII simply as "information which identifies a person as having requested or obtained specific video materials or services from a

81. See *id.*; Masha Komnenic, *First Party Cookies vs. Third Party Cookies: The Differences Explained*, TERMLY (Nov. 4, 2025), <https://termly.io/resources/articles/first-party-cookies-vs-third-party-cookies/#first-party-cookies-vs-third-party-cookies> [https://perma.cc/49MU-D9E3].

82. Delta Air Lines recently clarified that it does not require collection of personal information to purchase a Delta flight in response to public outrage at rumors that Delta's AI-powered pricing tool individualizes flight prices based on consumers' data. See *Delta Responds to Misinformation Around AI Pricing*, DELTA NEWS HUB (Aug. 7, 2025, at 16:30 ET), <https://news.delta.com/delta-responds-misinformation-around-ai-pricing> [https://perma.cc/K56C-TQLQ] (demonstrating response to public backlash where consumers' personal, individualized data was used against them for corporations' profits). Delta Air Lines confirmed that they do not share personal information with their AI tool. See *id.*

83. See *Pixel Tracking vs Cookies: Key Differences Explained*, INTUIT MAILCHIMP, <https://mailchimp.com/resources/pixel-tracking/> [https://perma.cc/4L36-JXES]; *Solomon v. Flippis Media, Inc.*, 136 F.4th 41, 46 (2d Cir. 2025).

84. See *Pixel Tracking vs Cookies: Key Differences Explained*, *supra* note 83.

85. See *id.*

86. See *id.*

87. See Michael Keenan, *Meta Pixel: Setup Guide for Facebook Ads (2026)*, SHOPIFY: BLOG (June 29, 2026), <https://www.shopify.com/blog/72787269-relax-advertising-on-facebook-just-got-a-lot-easier> [https://perma.cc/4CAH-6T33].

88. See Christina Newberry, *What Is the Meta Pixel, and How Do You Make the Most of It?*, HOOTSUITE (Feb. 10, 2025), <https://blog.hootsuite.com/meta-pixel/> [https://perma.cc/7RNB-EXWP].

89. See *Pixel Tracking vs Cookies: Key Differences Explained*, *supra* note 83.

video tape service provider.”⁹⁰ For there to be a viable claim for a violation of the VPPA, there must be knowing disclosure of three things: (1) identity of the viewer, (2) identity of specific video materials, and (3) the fact that the consumer requested them.⁹¹

When the case involves online data and cookies rather than an offline activity—such as the disclosure of a list of videos rented by a Supreme Court nominee—it is contested whether the Meta Pixel codes contain personally identifiable information and under which standard PII should be evaluated. Legal professionals and scholars have criticized the language of data privacy laws for their lack of clarity and transparency.⁹² To provide greater clarity to users, Professor Ari Waldman advocates for policies to be written in plain English directed at users, rather than “by lawyers and for lawyers,” as they are currently written.⁹³

Given the statutory text’s ambiguity, circuit courts have established two conflicting definitions of PII.⁹⁴ The First Circuit defines PII according to the reasonable foreseeability standard, while the Second, Third, and Ninth Circuits define PII according to the ordinary person standard.⁹⁵ The circuit split perpetuates consumer vulnerabilities; the lack of a uniform standard allows companies to argue that the data they collect is not PII and therefore does not require subscriber consent.⁹⁶ In turn, they can sell more user data and both the video service providers and third-party advertisers increase profits. User vulnerabilities increase with the deployment of generative AI to profit from and collect consumer data.⁹⁷ The Supreme Court has not ruled definitively on the definition of PII under the VPPA and recently declined to consider whether a petitioner has standing and is a valid “consumer” under the statute.⁹⁸ The Supreme Court is slated to hear a case defining “goods and

90. 18 U.S.C. § 2710(a)(3).

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

92. Mark P. Szpak addressed the VPPA’s ambiguities in responding to the Ninth Circuit’s use of the ordinary person standard to define PII. Mark P. Szpak, *Ninth Circuit Weighs In on Scope of Identifiable Information Under VPPA*, ROPES & GRAY LLP (Dec. 22, 2017), <https://www.ropesgray.com/en/insights/alerts/2017/12/ninth-circuit-weighs-in-on-scope-of-identifiable-information-under-vppa> (on file with the *Fordham Law Review*). Professor Alan Z. Rozenshtein criticized the ambiguities of 47 U.S.C. § 230, a law that immunizes online platforms from liability for content posted by its users. Alan Z. Rozenshtein, *Interpreting the Ambiguities of Section 230*, 41 YALE J. ON REG. 60, 63 (2024).

93. See Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 129, 132 (2018).

94. *Compare Yershov v. Gannett Satellite Info. Network*, 820 F.3d 482, 486 (1st Cir. 2016), with *Solomon v. Flippis Media, Inc.*, 136 F.4th 41, 52 (2d Cir. 2025) (“[W]e conclude that ‘personally identifiable information’ encompasses information that would allow an ordinary person to identify a consumer’s video-watching habits, but not information that only a sophisticated technology company could use to do so.” (quoting 18 U.S.C. § 2710(b)(1))).

95. See Nick Palmieri, *Second Circuit Rules on Scope of VPPA Protection*, JD SUPRA (June 2, 2025), <https://www.jdsupra.com/legalnews/second-circuit-rules-on-scope-of-vppa-4629494/> [<https://perma.cc/3G6B-95RS>].

96. See *Solomon*, 136 F.4th at 47.

97. See Russell, *supra* note 59.

98. See *National Basketball Association v. Salazar*, SCOTUSBLOG, <https://www.scotusblog.com/cases/case-files/national-basketball-association-v-salazar/> [<https://perma.cc/ARD9-2QAA>] (last visited June 19, 2026).

services” under the VPPA in October 2026.⁹⁹ In order to resolve the circuit split, the Supreme Court could grant certiorari in a Meta Pixel case and define PII. The circuit split could also be resolved through the enactment of a federal data privacy law, which would close the loopholes that allow companies to collect data without consent under the VPPA and other data privacy regimes.¹⁰⁰

Part II.A explores the First Circuit’s reasonable foreseeability standard, Part II.B describes the Second, Third, and Ninth Circuits’ ordinary person standard, and Part II.C details Meta Pixel cases and how district courts have diverged from *Solomon*. Part II.D then examines proposed solutions to the circuit split, Part II.E discusses data protections in the European Union (EU), and Part II.F recounts failed bills that attempted to regulate targeted advertising.

A. The Reasonable Foreseeability Standard

The First Circuit considered the definition of PII in *Yershov v. Gannett Satellite Information Network*.¹⁰¹ In that case, the plaintiff used the *USA Today* mobile app to access video news content.¹⁰² The app asked for Alexander Yershov’s consent only to enable push notifications, not to enable third-party cookies—yet the app sent his Android ID, GPS coordinates, and video-watching history to Adobe, a third party, in violation of the VPPA.¹⁰³ Adobe and its clients used Yershov’s Android ID to track Yershov across devices and apps and create a profile consisting of his personal information, online behavior, and device identifiers.¹⁰⁴ Adobe took Yershov’s information and used the videos he watched to discern his preferences and create targeted ads.¹⁰⁵ It was undisputed that Adobe used the information to identify Yershov and create targeted ads based on his video-watching history without obtaining his consent.¹⁰⁶ The question of whether Adobe violated the VPPA turned on whether the information transmitted constituted PII.¹⁰⁷

In determining whether Yershov had an actionable claim under the VPPA, the First Circuit noted that the online profile included identifying information such as “the user’s name and address, age and income, ‘household structure,’ and online navigation and transaction history.”¹⁰⁸ The court found that the VPPA’s “statutory term ‘personally identifiable information’ is awkward and unclear.”¹⁰⁹ Finding ambiguity within the statute, the court looked to the

99. *Salazar v. Paramount Global*, 146 S. Ct. 1591 (2026) (mem.)

100. *See Manza v. Pesi, Inc.*, 784 F. Supp. 3d 1110, 1117 (W.D. Wis. 2025).

101. 820 F.3d 482 (1st Cir. 2016); *id.* at 485–86.

102. *See id.* at 485.

103. *See id.* at 484–85.

104. *See id.*

105. *See id.* at 485.

106. *See id.*

107. *See id.* at 486.

108. *Id.* at 484–85.

109. *Id.* at 486 (quoting 18 U.S.C. § 2710(b)(1)).

VPPA's Senate Report and determined that "PII is not limited to information that explicitly names a person" because the statute's definition of PII was only intended to serve as a minimum standard.¹¹⁰ Instead, PII is information that is "reasonably and foreseeably likely to reveal which *USA Today* videos Yershov has obtained."¹¹¹ The court determined Yershov had an actionable claim because the Android ID, GPS coordinates, and video-watching history transmitted to Adobe could meet the reasonable foreseeability standard.¹¹²

B. The Ordinary Person Standard

The Third Circuit established a different standard for defining PII in *In re Nickelodeon Consumer Privacy Litigation*.¹¹³ The court held that the VPPA "applies only to the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior."¹¹⁴ It clarified that "digital identifiers like IP addresses[] fall outside the Act's protections" because an ordinary person could not identify a consumer by looking at their IP address.¹¹⁵

The Ninth Circuit also adopted the ordinary person standard in *Eichenberger v. ESPN, Inc.*¹¹⁶ The court determined that "the VPPA protects consumer privacy by directing video service providers not to do certain things with consumer information. To that end, 18 U.S.C. § 2710(b)(1) focuses on what information a video-service provider 'knowingly discloses,'" thus applying the ordinary person standard to the disclosing party, not the receiving party.¹¹⁷

Recently, the Second Circuit joined the Third and Ninth Circuits in applying the ordinary person standard in *Solomon*.¹¹⁸ The court stated that the VPPA's unclear definition of PII has given rise to substantial litigation and the resulting circuit split.¹¹⁹ The Second Circuit relied on the VPPA's plain meaning and the context of the statute to determine that PII "encompasses information that would allow an ordinary person to identify a consumer's video-watching habits, but not information that only a sophisticated technology company could use to do so."¹²⁰ In ruling for Flippo, the Second Circuit essentially foreclosed plaintiffs from prevailing in Meta Pixel suits under the VPPA.¹²¹ For instance, following *Solomon*, the Second Circuit deployed the ordinary person standard in *Hughes v. NFL*.¹²²

110. *Id.*

111. *Id.*

112. *Id.* at 486.

113. 827 F.3d 262, 267 (3d Cir. 2016).

114. *Id.*

115. *Id.*

116. 876 F.3d 979 (9th Cir. 2017); *id.* at 985.

117. *Id.* (quoting 18 U.S.C. § 2710(b)(1)).

118. 136 F.4th 41, 52 (2d Cir. 2025).

119. *See id.* at 51.

120. *Id.* at 52.

121. *Hughes v. NFL*, No. 24-2656, 2025 U.S. App. LEXIS 15216, at *3 (2d Cir. June 20, 2025).

122. No. 24-2656, 2025 U.S. App. LEXIS 15216 (2d Cir. June 20, 2025); *id.* at *4.

Finding for the NFL, the court rejected the plaintiff's arguments that an ordinary person could input the code transmitted to Meta Pixel into ChatGPT and decode the information to identify a person's video-watching behavior.¹²³ The court reasoned that "in *Solomon*, we focused on whether an ordinary person would be able to understand the actual underlying code communication itself, regardless of how the code is later manipulated or used by Facebook."¹²⁴ Thus, the Second Circuit held that pixel codes, like those in *Solomon* and *Hughes*, do not violate the VPPA when transmitted to Meta Pixel without subscribers' consent.¹²⁵ *Hughes* established that "*Solomon* effectively shut the door for Pixel-based VPPA claims."¹²⁶

Bound by the Second Circuit's decisions, subsequent district court cases, including *Nixon v. Pond5, Inc.*,¹²⁷ have necessarily followed *Solomon* and *Hughes*.¹²⁸ In *Nixon*, plaintiffs alleged that defendants transmitted URLs and Facebook IDs to Meta Pixel without their consent.¹²⁹ As in *Solomon* and *Hughes*, the plaintiff alleged that the video service's transmission of cookies containing coded information of users' video-watching behavior and Facebook IDs to Meta was PII.¹³⁰ The *Nixon* court summarily concluded that *Solomon* and *Hughes* foreclosed the possibility of a viable VPPA claim under these facts.¹³¹ In *Simon v. Scripps Networks, LLC*,¹³² the court again cited *Solomon* and *Hughes* in dismissing the case.¹³³ There, as in *Solomon*, the complaint did not allege that an ordinary person could identify the video watcher or the titles they viewed "with little or no extra effort."¹³⁴ Each subsequent district court case in the Second Circuit, bound by *Solomon*, has reached the same conclusion.¹³⁵ *Solomon*'s foreclosure of certain VPPA claims also affects whether Second Circuit district courts will accept class action settlements for VPPA Meta Pixel claims. Just a few days after the Second Circuit issued its opinion in *Solomon*, a district court approved a settlement of only \$900,000, citing the fact that *Solomon* likely precluded recovery moving forward.¹³⁶

123. *See id.* at *6.

124. *Id.*

125. *See id.*

126. *Id.* at *3.

127. No. 24-cv-05823, 2025 U.S. Dist. LEXIS 138221 (S.D.N.Y. July 21, 2025).

128. *See id.* at *11–16.

129. *See id.* at *2–3.

130. *See id.* at *2–4.

131. *See id.* at *13.

132. No. 24-cv-8175, 2025 WL 3167915 (S.D.N.Y. Nov. 13, 2025).

133. *See id.* at *7.

134. *Id.* at *18–20 (quoting *Solomon v. Flippis Media, Inc.*, 136 F.4th 41, 54 (2d Cir. 2025)).

135. *See, e.g., Joiner v. NHL Enters.*, No. 23-CV-2083, 2025 WL 2846431, slip op. at *6 (S.D.N.Y. Aug. 29, 2025).

136. *Lee v. Springer Nature Am., Inc.*, No. 24-cv-4493, 2025 U.S. Dist. LEXIS 254425, at *15 (S.D.N.Y. Dec. 9, 2025).

*C. Considering Generative
AI When Evaluating Pixel Codes*

Several district courts in the U.S. Courts of Appeals for the Sixth, Seventh, and Ninth Circuits have diverged from *Solomon* and its foreclosure of Meta Pixel claims under the VPPA.¹³⁷ This section discusses how courts have grappled with determining whether Facebook IDs can be considered PII: while district courts in the U.S. Courts of Appeals for the Sixth and Ninth Circuits have emphasized the capabilities of the recipient to decode PII, a Seventh Circuit district court took a more categorical approach, rejecting both the ordinary person and reasonable foreseeability standards and broadly defining ID codes as PII.

A series of Ninth Circuit district court cases have determined that a Facebook ID can be PII.¹³⁸ First, in *Garcia v. Bandai Namco Entertainment America Inc.*,¹³⁹ a Ninth Circuit district court held that whether the Meta Pixel code passed the ordinary person test was a question of fact.¹⁴⁰ *Garcia* suggests that, because whether an ordinary person can identify PII from the Meta Pixel code is a fact-specific inquiry, the claim cannot be foreclosed at the outset.¹⁴¹ *Garcia* quoted the Ninth Circuit's speculation in *Eichenberger* that "modern technology may indeed alter—or may already have altered—what qualifies under the [VPPA], speculating that '[a] Facebook link . . . may very well readily enable an "ordinary person" to identify an individual.'" ¹⁴² The *Garcia* court considered access to AI, stating "code is the primary communication medium for data sharing technologies and a growing proportion of the public has the technological fluency to discern information from lines of code, particularly with the advent of artificial intelligence tools."¹⁴³ Applying the Ninth Circuit's ordinary person standard, the district court found that it was "plausible that an ordinary person could identify Plaintiff based on the information shared by Defendant's Facebook Pixel technology," and therefore that the plaintiff had sufficiently alleged disclosure of their PII under the VPPA.¹⁴⁴ Considering AI as a tool that can decode pixel code and thus render the code PII poses an alternative to the Second Circuit's position in *Solomon*.

In *Balestrieri v. SportsEdTV, Inc.*,¹⁴⁵ a Ninth Circuit district court further diverged from *Solomon* by accepting the plaintiff's argument that anyone

137. See, e.g., *Garcia v. Bandai Namco Ent. Am. Inc.*, No. 25-cv-00967, 2025 U.S. Dist. LEXIS 152616, at *22–23 (C.D. Cal. Aug. 7, 2025); *Manza v. Pesi, Inc.*, 784 F. Supp. 3d 1110, 1119 (W.D. Wis. 2025); *Chandra v. Prager Univ. Found.*, No. 25-cv-03984, 2026 WL 434938, slip op. at *3 (C.D. Cal. Jan. 27, 2026).

138. *Garcia*, 2025 U.S. Dist. LEXIS 152616, at *23; *Balestrieri v. SportsEdTV, Inc.*, No. 25-cv-04046, 2025 WL 2776356, slip op. at *10 (N.D. Cal. Sep. 16, 2025); *Lee v. Plex, Inc.*, 773 F. Supp. 3d 755, 772 (N.D. Cal. 2025).

139. No. 25-cv-00967, 2025 U.S. Dist. LEXIS 152616 (C.D. Cal. Aug. 7, 2025).

140. *Id.* at *23 (quoting *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 986 (9th Cir. 2017)).

141. See *id.* at *22–23.

142. *Id.*

143. *Id.*

144. *Id.* at *23.

145. No. 25-cv-04046, 2025 WL 2776356 (N.D. Cal. Sep. 16, 2025).

could use a Facebook ID to find a Facebook profile and identify a video watcher.¹⁴⁶ The plaintiff alleged that SportsEdTV knowingly disclosed their video-watching history and Facebook ID through pixel code to Facebook, who used the information for targeted advertising.¹⁴⁷ The plaintiff in *Balestrieri* argued that the Facebook ID is PII, not because the ID number itself identifies the plaintiff, but because “any ordinary person can look up the user’s Facebook Profile and name.”¹⁴⁸ The District Court for the Northern District of California sided with the plaintiff and found their claim that a Facebook ID is PII satisfied the plausibility standard at the pleading stage.¹⁴⁹

A Ninth Circuit district court in *Lee v. Plex, Inc.*¹⁵⁰ further clarified how a Facebook ID can be PII if it can be used to find a profile that contains identifying information.¹⁵¹ There, the plaintiff’s Facebook profile used his real name, so anyone who had his Facebook ID would be able to locate his profile and learn his name.¹⁵² Given that *Eichenberger* found names to be PII,¹⁵³ the district court concluded that disclosure of a Facebook ID constitutes disclosure of PII because it can be used to find a Facebook page and the owner’s identifying information.¹⁵⁴ The court conceded that if the Facebook page does not contain the real name of the video watcher, then disclosure of the Facebook ID may not constitute PII.¹⁵⁵ Another Ninth Circuit district court later concluded that “an ordinary person needs neither a ‘complex’ algorithm nor an ‘enormous’ vault of information held exclusively by Facebook to locate a user’s Facebook page; all that is needed is the Facebook ID itself”; therefore, Facebook IDs and viewing histories together constitute PII under the VPPA.¹⁵⁶ The Ninth Circuit and its district courts, in cases such as *Eichenberger* and *Lee*, have declined to follow *Solomon*’s interpretation of the “ordinary person” standard: “[T]he ordinary person that the Second Circuit envisions appears to be one who is particularly unsophisticated or unmotivated to understand the information presented.”¹⁵⁷

146. *Id.* at *9–10.

147. *See id.* at *1.

148. *Id.* at *9.

149. *Id.*

150. 773 F. Supp. 3d 755 (N.D. Cal. 2025).

151. *Id.* at 773.

152. *See id.*

153. *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 986 (9th Cir. 2017).

154. *See Plex, Inc.*, 773 F. Supp. at 773.

155. *See id.* A similar conclusion was reached by the U.S. District Court for the Western District of Texas in *Cochenour v. 360 Training, Inc.*, No. 25-cv-7, 2025 WL 3251719 (W.D. Tex. Nov. 3, 2025). *Id.* at *5. This court relied on another Fifth Circuit district court case, *Frawley v. Nexstar Media Group.*, No. 23-cv-2197, 2024 WL 3798073 (N.D. Tex. July 22, 2024), which determined pre-*Solomon* that Facebook IDs paired with a video URL constitute PII, whether or not the individual actually watches the video. *Id.* at *7.

156. *Chandra v. Prager Univ. Found.*, No. 25-CV-03984, 2026 WL 434938, slip op. at *2–3 (C.D. Cal. Jan. 27, 2026).

157. *Id.* (quoting *Plotsker v. Envato Pty Ltd.*, No. 24-cv-04412, 2025 WL 2481422, slip op. at *8 n.7 (C.D. Cal. Aug. 26, 2025)).

Departing from the ordinary person standard, a U.S. district court in the Sixth Circuit concluded that when determining whether information is PII, the key focus should be on the capabilities of the specific recipient, not on the discloser or any party in general.¹⁵⁸ The court found that a string of characters similar to the one in *Solomon* constituted PII and remarked that *Solomon*'s inferences are "simply unpersuasive."¹⁵⁹ The court declined to apply the ordinary person standard to the format (rather than the type) of information, thus concluding that a video-service provider cannot satisfy the VPPA by sending the identifying information in pixel code, "even though no bystander would be able to identify a video title just by looking."¹⁶⁰ This is because a bystander is not the recipient of the code—Meta is. The court asserted that "the VPPA is not primarily aimed at bystanders who might intercept a disclosure; rather it is meant to prevent an *intended recipient* from receiving a disclosure."¹⁶¹ Because Meta is certainly able to interpret the pixel code, the code constitutes PII.¹⁶² Another district court in the Sixth Circuit similarly disregarded *Solomon* at the pleading stage because "in the modern era, the ordinary person is certainly capable of typing in what is essentially a URL linked to a specific individual's Meta profile."¹⁶³

A district court in the Seventh Circuit eschewed both standards and determined that ID numbers in pixel code are PII because of their identifying power.¹⁶⁴ A district court in the Sixth Circuit came to the same conclusion by invoking the *Solomon* court's reasoning that PII is information that can "be used to" identify a consumer's video-watching history, "not just information that, by itself, identifies a consumer's video-watching history."¹⁶⁵ Though it quoted *Solomon*, the court declined to use the ordinary person standard, holding that the standard "creates a loophole that significantly undermines the basic purpose of the VPPA and is not supported by the VPPA's text."¹⁶⁶ Rather than coming up with another standard, or applying the First Circuit's reasonable foreseeability standard, the district court concluded that "ID numbers uniquely associated with a specific customer qualify as PII under the VPPA when they are paired with the names of videos the customer obtained from the defendant."¹⁶⁷

158. See *Goodman v. Hillsdale Coll.*, No. 25-CV-417, 2025 WL 2941542, slip op. at *8 (W.D. Mich. Oct. 17, 2025).

159. *Id.*

160. *Id.*

161. *Id.* at *9.

162. *Id.*

163. *Lovett v. Continued.com, LLC*, No. 24-cv-590, 2026 WL 835833, slip op. at *7 (S.D. Ohio Mar. 26, 2026).

164. See *Manza v. Pesi, Inc.*, 784 F. Supp. 3d 1110, 1122 (W.D. Wis. 2025).

165. *Goodman*, 2025 WL 2941542, slip op. at *9 (quoting *Solomon v. Flipp Media, Inc.*, 136 F.4th 41, 51 (2d Cir. 2025)).

166. *Id.*

167. *Id.*

D. Approaches for Resolving the Circuit Split

Though the VPPA circuit split is rapidly evolving as courts consider *Solomon* and the implications of AI, the split standards have been litigated long enough for scholars to develop potential solutions.¹⁶⁸ This section summarizes scholarly suggestions for resolving the circuit split and defining personal data.

To address the circuit split over the VPPA, one suggested approach is to repeal the VPPA altogether and replace it with a new privacy law.¹⁶⁹ The new statute would be more flexible to new technology and extend the protections of the VPPA (requiring affirmative consent before disclosure and creating a private right of action) to all data, not just video-watching information.¹⁷⁰ Rather than throwing out the VPPA, another approach predating *Solomon* and the prevalence of generative AI proposed a six-factor test for determining whether information constitutes PII.¹⁷¹ Courts applying this framework would consider factors including (1) the likelihood that the specific recipient of the information is capable of identifying the video watcher, (2) the extent to which the specific recipient has additional information that can be used to identify the video watcher, (3) the degree to which the information is unique to the video watcher, (4) whether the information is likely to be stored and for how long, (5) whether the specific recipient has incentive to identify the video watcher, and finally (6) whether the specific recipient is likely to share the information with another party who could identify the video watcher.¹⁷² Then, if the six factors indicate that there is a “significant risk of identification,” courts should “assess whether this risk was foreseeable, based on what the video-service provider knew, or should have known, at the time of disclosure.”¹⁷³

Another solution that disregards both the reasonable foreseeability and ordinary person standards is to categorize data based on its potential for harm.¹⁷⁴ Privacy laws such as the VPPA provide litigated definitions of personal data.¹⁷⁵ Some privacy laws provide additional protections for so-called “sensitive data.”¹⁷⁶ However, distinctions between data may be collapsing in the era of advanced technology.¹⁷⁷ Professor Daniel J. Solove suggests reconciling the varying definitions of personal information and the

168. See, e.g., Gemdjan, *supra* note 15, at 582–85.

169. See *id.* at 583.

170. See *id.*

171. See Daniel L. Macioce Jr., Comment, *PII in Context: Video Privacy and a Factor-Based Test for Assessing Personal Information*, 45 PEPP. L. REV. 331, 389–90 (2018).

172. See *id.*

173. *Id.* at 390.

174. See Daniel J. Solove, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 118 NW. L. REV. 1081, 1081 (2024).

175. See, e.g., *Solomon v. Flippis Media, Inc.*, 136 F.4th 41, 52 (2d Cir. 2025).

176. See, e.g., Regulation 2016/679 of Apr. 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

177. See Solove, *supra* note 174, at 1083.

increasingly blurred distinctions between data types by examining the harms and risks posed by data, rather than the nature of the data itself.¹⁷⁸

Professor Solove writes about the futility of defining “sensitive data,” which is a subcategory of personal data and receives additional legal protections.¹⁷⁹ Sensitive data often includes information regarding race, religion, sexual orientation, biometric and genetic data, and more.¹⁸⁰ The EU was the first to recognize sensitive data, followed by the United States in 2020.¹⁸¹ Solove argues that this distinction is meaningless: “nearly all personal data can be sensitive” because “in the age of Big Data, powerful machine learning algorithms facilitate inferences about sensitive data from nonsensitive data.”¹⁸² If this is true, Solove posits that many companies violate heightened sensitive data restrictions in their handling of user data.¹⁸³ Rather than sticking with an inflexible delineation between personal and sensitive data, Solove suggests that the law impose restrictions based on the data’s use and sale; in other words, the law should focus not on what the data is but what it does.¹⁸⁴

The premise for Solove’s suggestion is that technology erodes previous data distinctions by enabling the identification of people from data that is not directly identifying and was not previously capable of identifying users.¹⁸⁵ This premise has significant implications for defining PII under the VPPA because it calls into question the capabilities of the ordinary person using modern technology such as AI. Using Solove’s approach, interpretations of PII under the VPPA would not turn on whether the pixel code is sufficiently identifying, but rather on its identifying power and the consequences of such identification.

Yet another approach similar to both Solove’s¹⁸⁶ and the reasoning in *Eichenberger*¹⁸⁷ suggests revising the definition of PII to include all information that is reasonably likely to identify someone’s video-watching history.¹⁸⁸ Under this approach, personal information that appears “meaningless” on its own is considered in the context of all other information that can be used to “assemble detailed behavioral profiles.”¹⁸⁹ Storing data would not provide a cause of action under the VPPA if it is used for “record keeping or other operative purposes,” but liability would attach if the same

178. *See id.*

179. *See id.*

180. *See id.*

181. *See id.*

182. *Id.* at 1084.

183. *See id.*

184. *See id.*

185. *See id.* at 1086–87.

186. *See id.* at 1086.

187. *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 985 (9th Cir. 2017).

188. *See* Luke J. Camel, Casenote, *Now Streaming Your Identity: How Solomon and the “Ordinary Person Standard” Erode the VPPA’s Reach*, 72 LOY. L. REV. 145, 164 (2025).

189. *See id.* at 164–65.

data is used for targeted advertising, for example, and companies should be required to disclose how the data is used.¹⁹⁰

E. Data Protections in the European Union

European data protection laws provide another example of recategorizing data that differs from definitions in privacy statutes such as the VPPA. In 2018, the EU imposed what has been referred to as “the toughest privacy and security law in the world”: the General Data Protection Regulation¹⁹¹ (GDPR).¹⁹² The GDPR governs any organization that targets or collects data from citizens or people who live in the EU.¹⁹³ As a result, U.S.-based companies that collect data from people in the EU are subject to more stringent requirements under GDPR than under U.S. privacy laws such as the VPPA.

The GDPR protects a wider array of data than U.S. laws.¹⁹⁴ Companies that collect “personal data”—defined as “any information relating to an identified or identifiable natural person”—without one of six lawful bases for doing so are subject to large fines.¹⁹⁵ One lawful basis for processing personal data is consent.¹⁹⁶ “Identifiable natural person” is further defined as “one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the . . . identity of that natural person.”¹⁹⁷ Indirect identification requires “reasonable access” to other information that is used in combination with personal data to identify the individual.¹⁹⁸ The GDPR also considers whether the purpose of collecting the data is to identify an individual.¹⁹⁹ Since identification numbers are clearly considered personal data, and the GDPR specifies that cookie identifiers and pixel codes containing Facebook IDs are personal data, pixel codes are protected under the GDPR.²⁰⁰

190. See *id.* at 165.

191. Regulation 2016/679 of Apr. 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

192. Ben Wolford, *What Is GDPR, the EU's New Data Protection Law?*, GDPR.EU, <https://gdpr.eu/what-is-gdpr/> [<https://perma.cc/2D4J-RT28>] (last visited June 28, 2026).

193. See Wolford, *supra* note 192.

194. See *id.*; 18 U.S.C. § 2710.

195. See Regulation 2016/679 of Apr. 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1; see also Richie Koch, *What Is Considered Personal Data Under the EU GDPR?*, GDPR.EU, <https://gdpr.eu/eu-gdpr-personal-data/> [<https://perma.cc/XX5C-RMSX>] (last visited June 19, 2026) (“Looking back at the GDPR’s definition, we have a list of different types of identifiers: ‘a name, an identification number, location data, an online identifier.’”).

196. See Regulation 2016/679 of Apr. 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

197. *Id.*

198. See *id.*

199. See *id.*

200. See Koch, *supra* note 195.

In addition to an alternative method of categorizing data, the GDPR and litigation before the Court of Justice of the European Union (CJEU) highlight the disparities between the GDPR and U.S. privacy laws.²⁰¹ In July 2020, the CJEU restricted data transfers to the United States because its privacy laws were not compliant with the stringent GDPR.²⁰² In *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* (*Schrems II*),²⁰³ Facebook Ireland transferred EU data to Facebook U.S.²⁰⁴ Prior to *Schrems II*, the United States was part of a privacy shield network that allowed the transfer of data from the EU to the United States, provided that companies comply with privacy shield principles.²⁰⁵ The FTC enforced noncompliance under section 5 of the FTC Act by imposing liability or removing companies from the network.²⁰⁶ *Schrems II* invalidated the privacy shield because of the “shortcomings” of U.S. data protection laws.²⁰⁷ Under the GDPR, data transfers are only permitted between countries with “essentially equivalent” data protections.²⁰⁸ All companies that make EU data available in other countries must also evaluate the privacy laws of the recipient country;²⁰⁹ this evaluation must be done before transferring any data outside of the EU.²¹⁰ The *Schrems II* ruling represents the goal of ensuring relatively equivalent, strong data protection laws across countries and the fact that this is not yet a reality.²¹¹

F. Proposed U.S. Regulation of Targeted Ads

Congress has nearly passed two bills in recent years addressing data privacy protection and targeted ads that would comply with the GDPR.²¹² Had the bills passed, circuit courts would have relied on the bills’ use of “unique persistent identifier” to define PII.²¹³

201. See generally HENDRIK MILDEBRATH, EUR. PARLIAMENT, THE CJEU JUDGMENT IN THE *SCHREMS II* CASE (2020), [https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA\(2020\)652073_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf) (on file with the *Fordham Law Review*).

202. See *id.*; see also Ana Mishova, *Pixel GDPR Compliance: Key Insights and Best Practices*, GDPR LOCAL (June 26, 2025), <https://gdprlocal.com/meta-pixel-gdpr-compliance/> [<https://perma.cc/LQG2-SLGD>]; see MILDEBRATH, *supra* note 201.

203. Case C-311/18, *Data Prot. Comm’r v. Facebook Ir. Ltd. & Maximillian Schrems* (*Schrems II*), ECLI:EU:C:2020:559 (July 16, 2020).

204. See MILDEBRATH, *supra* note 201.

205. See *id.*

206. See *id.*

207. Sharp Cookie Advisors, *Schrems II A Summary—All You Need to Know*, GDPR SUMMARY (Nov. 23, 2020), <https://www.gdprsummary.com/schrems-ii/> (on file with the *Fordham Law Review*). These shortcomings were particularly focused on data that, if necessary for a national security investigation, is unprotected. *Id.*

208. MILDEBRATH, *supra* note 201.

209. See Sharp Cookie Advisors, *supra* note 207.

210. See *id.*

211. MILDEBRATH, *supra* note 201.

212. See generally American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022); American Privacy Rights Act, H.R. 8818, 118th Cong. (2024).

213. See H.R. 8152 § 2(34); H.R. 8818 § 101(54)(A).

The American Data Privacy and Protection Act²¹⁴ (ADPPA) was introduced in June 2022 and intended to provide “foundational data privacy rights.”²¹⁵ The ADPPA defined targeted advertising as “presenting to an individual or device identified by a unique identifier, . . . an online advertisement that is selected based on known or predicted preferences, characteristics, or interests associated with the individual or a device identified by a unique identifier,” excluding contextual advertisements shown to everyone, processing covered data to measure advertisement performance, or advertisements in response to the individual’s request for information or feedback.²¹⁶ The ADPPA provided a right to opt out of targeted advertising of all types, which is already provided for video service providers under the consent requirement of the VPPA.²¹⁷ For covered minors (anyone under the age of seventeen),²¹⁸ first-party advertising would have been prohibited if the entity knew that the individual was a covered minor, though third-party advertising would be allowed with “affirmative express consent” from parents.²¹⁹

The American Privacy Rights Act²²⁰ (APRA), modeled after its unsuccessful predecessor, was a bipartisan proposal introduced in April 2024.²²¹ The APRA would have established the “first ever federal standard for comprehensive data policy and security regulation,” including the right to opt out of “covered algorithms and AI decisions.”²²² The APRA defined targeted advertising similarly to the ADPPA, with the language of “unique persistent identifier.”²²³ The APRA only excluded first-party advertising from its definition of targeted advertisements; its scope was therefore broader than its 2022 predecessor.²²⁴ Unlike the ADPPA, the APRA allows first-party advertisements directed at covered minors so long as they are (1) age-appropriate and (2) not informed by personal information of the minor other than their status as a minor.²²⁵ As under the ADPPA, third-party advertisements involving the sale of covered minors’ data would be permitted without those restrictions, requiring only “affirmative express consent” from the minors’ parents.²²⁶

214. H.R. 8152, 117th Cong. (2022).

215. *Id.* pmbl.

216. *Id.* § 2(34).

217. *See id.* § 204(c).

218. *See id.* § 2(11).

219. *Id.* § 205(a)–(b).

220. H.R. 8818, 118th Cong. (2024).

221. *See* Kirk J. Nahra, Ali A. Jessani & Amy Olivero, *New Federal Privacy Bill Draft Hits Congress*, WILMERHALE (Apr. 19, 2024), <https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240418-new-federal-privacy-bill-draft-hits-congress> [https://perma.cc/L7HU-TA46].

222. *Id.*

223. H.R. 8818 § 101(54)(A).

224. *Compare* H.R. 8818, *with* H.R. 8152 (excluding only first-party advertising from the APRA’s definition of targeted advertisements but providing additional exclusions under the APRA).

225. *See* H.R. 8818 § 120(a).

226. *Id.* § 120(b).

III. REGULATING THE SALE OF PERSONAL DATA FOR TARGETED ADVERTISING

Regulation of personal data must be responsive to technological advances, such as the evolution of generative AI. Generative AI increases the efficacy of targeted ads²²⁷ and can be used to decode pixel code, making it increasingly important to regulate data transmitted to third parties for the use of targeted advertising as AI evolves. Regulating personal data in the era of generative AI requires ensuring that companies ask for consent prior to disclosing this data. To do so, the loophole created by the VPPA's ambiguous definition of PII must be closed. The VPPA, as currently written, has created a circuit split, such that some circuits require consent before transmitting personal information in code to Meta Pixel for targeted advertising, while others do not.²²⁸ Courts have come to different conclusions on how access to AI changes what they view as information that is "capable of being used to" identify a consumer.²²⁹ As a result, major technology companies ("Big Tech") can use the ordinary person standard as interpreted by *Solomon* to profit from consumer data without consent.²³⁰ Instead, this Note argues that any data that can, with AI, identify a video watcher and their watch history should be considered PII and require consent before being disclosed to a third party. Whether the standard applies to the disclosing or the receiving party should make no difference in determining whether pixel code constitutes PII.

Strengthening data privacy laws in the United States by eliminating this loophole is one step toward harmonizing international data privacy protections to the high standard of the GDPR.²³¹ This approach evaluates pixel code based not on what it is but on its identifying potential, given that virtually all data can be used to identify people.²³² Though this approach does not attempt to predict all of the potential harms and risks of disclosing the data under Solove's approach, it does consider the potential of pixel code to be identifying.²³³ Rather than "swallowing up nearly all personal data," this approach incorporates pixel code into a flexible definition of PII but does not unreasonably extrapolate to all types of code.²³⁴ Congress could effectuate this new approach by enacting a new federal privacy law to redefine PII, or the Supreme Court could clarify the VPPA's definition of PII and adopt a uniform standard.

Part III.A explains why the solutions this Note poses are especially important to counteract the inefficacy of the VPPA's consent requirement.

227. See Russell, *supra* note 59 and accompanying text.

228. See, e.g., *Yershov v. Gannett Satellite Info. Network*, 820 F.3d 482, 486 (1st Cir. 2016); *Solomon v. Flips Media, Inc.*, 136 F.4th 41, 52 (2d Cir. 2025).

229. *Solomon*, 136 F.4th at 51.

230. See *id.* at 52.

231. See Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶ 10 (July 16, 2020).

232. See Solove, *supra* note 174, at 1084.

233. See *id.* ("To be effective, privacy law must focus on harm and risk rather than on the nature of personal data.").

234. See *id.* at 1103.

Part III.B explores the benefits and drawbacks of previously posed solutions as mechanisms to achieve the goals stated above. Part III.C suggests two paths for Congress and the Court to better protect personal data, including pixel code.

*A. Counteracting the Unwillingness
to Meaningfully Consent*

In examining the VPPA circuit split and defining PII, this Note seeks to draw a line between what types of data can and cannot be collected without consent under the VPPA. Consent opens the door to data collection and sale for targeted advertising. However, the opaque nature of companies' data collection and sale renders consent less effective.²³⁵ Most people do not read consent or opt-out information when it pops up on a video service provider's website.²³⁶ The natural inclination is to consent to cookies for targeted advertising so that consumers can quickly access their video content.²³⁷ Rather than imposing duties on companies to legitimize consent, as one privacy scholar advocates,²³⁸ this Note considers the so-called fiction of consent²³⁹ in its recommendation that PII include pixel code. In response to the inadequacies of consent, the law should ensure that the definition of PII includes all data that could be used to identify users and the content they view, including data that is in pixel code that an ordinary person can decode using AI. At a minimum, companies should ask for consent before collecting and profiting from the sale of video watchers' data, even in pixel form that can be used to identify subscribers. Video subscribers can still freely consent to the sale of their data; requiring consent is not paternalistic but rather puts the choice in users' hands. Some subscribers may like to receive advertisements connected to their video-watching content,²⁴⁰ and may consent to receive such advertisements even under a new federal data privacy law.

B. Evaluating Existing Solutions

As discussed in Part II, other scholars and members of Congress have proposed new laws to regulate the sale of personal data.²⁴¹ This section

235. See Solove & Matsumi, *supra* note 67, at 593 ("Individuals are often pressured or manipulated, undermining the validity of their consent.").

236. See Josh Koeber & Kalleigh Lane, *Cookies Study: 1 in 4 Americans Blindly Accept Internet Cookies, but Most Don't Know What They Are*, ALL ABOUT COOKIES (Sep. 23, 2025), <https://allaboutcookies.org/internet-cookies-survey> (on file with the *Fordham Law Review*).

237. See *id.*

238. Solove proposes a "(1) duty to obtain consent appropriately; (2) duty to avoid thwarting reasonable expectations; (3) duty of loyalty; (4) duty to avoid unreasonable risk." Solove & Matsumi, *supra* note 67, at 594.

239. See *id.* at 596.

240. See *id.* at 597–98 (finding government control of data problematic because it eliminates the ability for people to choose to trade their data).

241. See *supra* Part II; American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 2 (2022); American Privacy Rights Act, H.R. 8818, 118th Cong. § 101 (2024); see also Macioce, *supra* note 171, at 389–90.

examines the benefits and drawbacks of the proposed legislation to regulate personal data, and also evaluates solutions posed before *Solomon* to resolve the circuit split.

The ADPPA and APRA represent a congressional willingness to regulate the sale of data for targeted advertisements. Aside from failing to garner enough support to pass, the ADPPA and APRA fell short because their definitions of “unique persistent identifier” contained too many exceptions.²⁴² The ADPPA defined “unique persistent identifier” as information that “is reasonably linkable to an individual . . . including a device identifier, Internet Protocol address, cookie, beacon, pixel tag, mobile ad identifier, or similar technology, customer number, unique pseudonym, user alias, telephone number,” but excluded “an identifier assigned by a covered entity for the specific purpose of giving effect to an individual’s exercise of affirmative express consent or opt-outs of the collection, processing, and transfer of covered data . . . or otherwise limiting the collection, processing, or transfer of such information.”²⁴³ The APRA shared the ADPPA’s definition of “unique persistent identifier.”²⁴⁴ The ADPPA and APRA would have considered pixel code to be PII regardless of which standard is applied, but both bills allowed exceptions for entities with less than \$41 million annual gross revenue, if they collected data from less than 100,000 people each year, or if they did not derive more than 50 percent of revenue from selling covered data each year.²⁴⁵ These exceptions were too broad to adequately protect subscriber data, though both pieces of legislation would have significantly advanced privacy rights by treating pixel code as PII.

Additionally, the proposed multifactor test provides a flexible solution that would resolve the VPPA circuit split but is likely too fact intensive to provide lasting clarity.²⁴⁶ As stated in Part II.D, the test involves consideration of six factors: (1) the likelihood that the recipient can identify the video watcher, (2) the extent to which the recipient has additional information that can be used to identify the video watcher, (3) the degree to which the information transmitted is unique to the video watcher, (4) if and for how long the information is likely to be stored, (5) if the recipient has incentive to identify the video watcher, and finally, (6) if the recipient is likely to share the information with another party who could identify the video watcher.²⁴⁷

Factors (1) and (2) are particularly well suited to protect consumers given the emerging AI tools recipients can use to identify video-watching individuals and their watch history. However, the multifactor test is too fact intensive for companies to use to prevent liability and predict litigation

242. H.R. 8152 § 2(34); H.R. 8818 § 101(54)(A).

243. H.R. 8152 § 2(39).

244. H.R. 8818 § 101(e)(59).

245. See Omer Imran Malik, *American Data Privacy and Protection Act (ADPPA): Explained*, SECURITI AI (Jan. 3, 2025), <https://securiti.ai/american-data-privacy-protection-act-adppa/> [https://perma.cc/NC75-52Y3].

246. See Macioce, *supra* note 171, at 389–90.

247. See *id.*

outcomes. Because of this, the six-factor test does not provide sufficient clarity in resolving the VPPA circuit split for Meta Pixel cases.

C. Limiting Data Collected Without Consent

There are two paths that Congress or the Supreme Court could take to strengthen the protection of personal data sold for targeted advertising and cure the VPPA circuit split. The first path is for Congress to pass another bill, potentially as a revenue reconciliation bill, to more precisely define PII and incentivize video-service provider compliance without sacrificing profit.²⁴⁸ The second path preserves the VPPA and calls on the Supreme Court to rule on the circuit split. Part III.C.1 poses a new bill that Congress could enact to achieve the privacy goals stated above. Part III.C.2 suggests how the Supreme Court could resolve the VPPA circuit split by granting certiorari on a pixel case and adopting a uniform standard.

1. The First Path: A Federal Privacy Law Regulating Targeted Advertising

Congress could strengthen the protection of personal data used for targeted advertising by proposing a new federal privacy bill. This bill, like the ADPPA and APRA, would define PII to include pixel code that an ordinary person can use to identify a video watcher and the videos they watched. Because the ordinary person standard is more widely accepted among circuits and is relatively more straightforward to implement than the reasonable foreseeability standard, the bill should incorporate the ordinary person standard to define pixel code that constitutes PII rather than the reasonable foreseeability standard. Maintaining the standard and not including all pixel code in the definition of PII would allow for a more flexible application of the new federal privacy law while still requiring stringent protections. Additionally, the First Circuit's finding in *Yershov* that the VPPA's definition of PII was intended to be a minimum standard can still be upheld through a new interpretation of the ordinary person standard.²⁴⁹ Rather than following the Second Circuit's approach in *Solomon*, the federal data privacy

248. This path could also close another loophole: companies can collect children's data for contextual advertising without consent. 16 C.F.R. § 312 (2025). The Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (COPPA) regulates the data for children under thirteen and permits data collection for contextual advertising. *See generally id.* Contextual advertising is advertising that matches the content viewers are currently looking at or listening to. *See How Contextual Targeting Works in Advertising*, AMAZON ADS <https://advertising.amazon.com/library/guides/contextual-advertising#2b> [<https://perma.cc/76L8-92D7>] (last visited June 19, 2026). However, there are similarities between contextual advertising and targeted advertising; commenters on COPPA's 2025 amendment noted that both forms of advertising rely on people's data and employ inferences and AI, and so consent should be required for collection of children's data for both contextual and targeted advertising. *See* 16 C.F.R. § 312. To close this loophole, Congress could use the new federal data privacy law to require consent for data collected from children under thirteen for the purpose of contextual advertising, not just for targeted advertising.

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

bill should include pixel code in the definition of PII, following the logic of *Goodman*, to account for widespread access to artificial intelligence.²⁵⁰

An alternative method to pass the measure would be to propose a revenue reconciliation bill. This bill would aim to overcome the obstacles that prevented its predecessors, the ADPPA and APRA, from passing despite bipartisan support.²⁵¹ Revenue reconciliation bills, or tax bills, can be passed through an expedited debate process that does not require a three-fifths Senate majority vote.²⁵² Each provision of a revenue reconciliation bill must be “germane” to revenue collection to survive inspection by the parliamentarian, who is in charge of assuring revenue reconciliation bills are reasonably related to revenue.²⁵³

Congress uses tax expenditures for a variety of policy reasons;²⁵⁴ for example, an income tax law does not necessarily have to be designed to accurately measure income. In this case, the bill could provide a tax deduction²⁵⁵ to better incentivize compliance. This incentive is critical because the threat of litigation under the VPPA has not effectively deterred violations, as evidenced by the recent proliferation of VPPA litigation.²⁵⁶

The bill could grant tax deductions for video service providers who require consent for the sale of code that can be used by an ordinary person, including one with access to widespread AI tools, to identify the video watcher and the videos they watched. Compliant video service providers could deduct a small portion of their operating expenses, modeled after the GDPR’s noncompliance penalty of 2 percent of an organization’s annual revenue, but here it would act as an incentive rather than a penalty.²⁵⁷ The deduction would target video service providers, making the sale of consumer data more profitable to them if they ask for consent than if they do not. This bill would

250. See *Goodman v. Hillsdale Coll.*, No. 25-cv-417, 2025 WL 2941542, slip op. at *8 (W.D. Mich. Oct. 17, 2025).

251. See Anne Godlasky, *American Data Privacy and Protection Act (ADPPA) Didn’t Pass but Got Further Than Ever*, NAT’L PRESS FOUND. (Nov. 30, 2022), <https://nationalpress.org/topic/data-privacy-act-addpa-us-lacks-law-eu-standard/> [<https://perma.cc/C9HK-H6YJ>]; see also Nahra, Jessani & Olivero, *supra* note 221.

252. 2 U.S.C. § 641; TORI GORMAN, CONG. RSCH. SERV., R48444, THE RECONCILIATION PROCESS: FREQUENTLY ASKED QUESTIONS 1 (2026).

253. GORMAN, *supra* note 252, at 5.

254. See *The Weird Way Taxes Impact Behavior*, TAXEDU, <https://taxfoundation.org/tax-edu/primers/primer-the-weird-way-taxes-impact-behavior/> [<https://perma.cc/8FAJ-26JV>] (last visited June 19, 2026).

255. A deduction paired with the sale of data may help to satisfy the germaneness requirement. See GORMAN, *supra* note 252, at 5.

256. See Tyler Lacoma, *Amazon’s Alexa AI Upgrade Remains in Early Access. CNET Survey Shows 73% of Device Users Express Privacy Worries*, CNET (May 14, 2025, at 16:00 ET), <https://www.cnet.com/home/smart-home/amazons-alexa-ai-upgrade-remains-in-early-access-cnet-survey-shows-73-of-device-users-express-privacy-worries/> (on file with the *Fordham Law Review*).

257. Ben Wolford, *What Are the GDPR Fines?*, GDPR.EU, <https://gdpr.eu/fines/> [<https://perma.cc/HC92-7LFP>] (last visited July 15, 2026).

most closely follow *Goodman*'s application of the ordinary person standard.²⁵⁸

2. The Second Path: Addressing Privacy Concerns About the VPPA Directly

Given the difficulty Congress has faced in passing bills regulating the sale of personal data for targeted advertising, including opposition from Big Tech lobbyists,²⁵⁹ regulating the sale of pixel data may be too difficult or too lengthy a process, even through a provision in a revenue reconciliation bill. In the meantime, harm to both consumers and companies persists as the legal standard is unclear and cases continue to be litigated on the same issue.²⁶⁰ Thus, the second path is for the Supreme Court to grant certiorari and establish a uniform definition of PII. The Court should adopt the ordinary person standard, consistent with how most circuits have already ruled, to create stability and predictability in data privacy law. Including the ordinary person's access to AI when considering which form of code can identify an individual and the videos they watched ensures that the VPPA protects sufficiently identifiable information. Otherwise, the accessibility and capabilities of generative AI would erode the VPPA's protections.

CONCLUSION

The VPPA is intended to require video service providers to obtain consent before selling personally identifying data.²⁶¹ Its purpose is thwarted when companies can send data in pixel codes that can be decoded using widely available AI tools. Excluding subscribers from the decision to sell their data should be recognized as not only violating the VPPA, but also as exploiting their attention and infringing on their freedoms.²⁶²

This Note's solutions provide a new regulatory approach to the consent requirement for data sold for targeted advertising, closing a loophole that leaves consumers powerless to meaningfully consent to or deny the sale of their data.²⁶³ The first path is to enact a new federal privacy law that defines PII using the ordinary person standard and considers the capabilities of generative AI in the ordinary person's hands. The second solution achieves

258. See *Goodman v. Hillsdale Coll.*, No. 25-CV-417, 2025 WL 2941542, slip op. at *8 (W.D. Mich. Oct. 17, 2025).

259. The twenty-hour limit on the Senate debate time of a revenue reconciliation bill may help ensure its passage. See GORMAN, *supra* note 252, at 8.

260. See *generally* *Joiner v. NHL Enters.*, No. 23-CV-2083, 2025 WL 2846431 (S.D.N.Y. Aug. 29, 2025) (litigating the legal standard for determining what data constitutes PII); *Nixon v. Pond5, Inc.*, No. 24-CV-05823, 2025 U.S. Dist. LEXIS 138221 (S.D.N.Y. July 21, 2025) (same); *Hughes v. NFL*, No. 24-2656, 2025 U.S. App. LEXIS 15216 (2d Cir. June 20, 2025) (same); *Balestrieri v. SportsEdTV, Inc.*, No. 25-CV-04046, 2025 WL 2776356 (N.D. Cal. Sep. 16, 2025) (same); *Goodman*, 2025 WL 2941542 (same).

261. See S. REP. NO. 100-159, at 1 (1988).

262. See WU, *supra* note 48, at 23 (arguing that "an awareness that the exploitation of human attention is in some deeper way the exploitation of our persons").

263. *Manza v. Pesí, Inc.*, 784 F. Supp. 3d 1110, 1122 (W.D. Wis. 2025).

the same goals but through different means: the Supreme Court's granting of certiorari in a PII case. Had either one of this Note's solutions been enacted prior to *Solomon*, Detrina Solomon would have been given the freedom to choose whether her data could be sold in exchange for targeted advertisements related to her video-watching history. Instead, Flippis made a deal to commodify her attention on her behalf.