NOTE

The Video Privacy Protection Act and Consumer Data: Are You Plugged In?

Lucas Urgoiti[*]

TABLE OF CONTENTS

INTRODUCTION 1691
I. BACKGROUND OF THE VPPA 1698
A. *Statute and Statutory Language* 1698
B. *Enactment of the VPPA in Response to the Debate on the Right to Privacy* 1699
C. *Technological Advancement* 1700
D. *Cookies, Pixels, and Similar Technologies* 1702
E. *The VPPA's 2012 Amendment* 1706
II. THE *HULU* COURT'S INTERPRETATION OF CODE IN TRANSMITTING DATA IS FLAWED AND RENDERS THE VPPA INAPPLICABLE TO DIGITAL MEDIA 1707
III. THE *HULU* COURT MISAPPLIED THE ECPA'S DEFINITION OF THE TERM "KNOWINGLY" 1721
IV. USE OF SOCIAL PLUGINS SHOULD CONSTITUTE ACTUAL KNOWLEDGE UNDER THE VPPA 1727
V. SOCIAL PLUGINS AS A PROPOSED LEGAL RULE 1733
A. *The Futility of a Legislative Solution* 1733
B. *Judicial Solution: Recognizing Social Plugins' Implications for "Knowledge"* 1735
CONCLUSION 1737

 J.D. Candidate, University of California, Davis, School of Law, 2020. Thank you to Professor David Horton for his valuable feedback and guidance throughout the writing process. I would also like to thank Senior Notes and Comments Editor Jae Ha and Senior Articles Editor Kevin Boutin for their helpful comments. Lastly, thanks to the Members and Editors of the UC Davis Law Review for their contributions to earlier drafts of this Note.

***

INTRODUCTION

The California Consumer Privacy Act ("CCPA") was signed into law by Governor Jerry Brown in June 2018.[1] The new law, which took effect on January 1, 2020,[2] gives California residents the right to know what kinds of personal information data companies have collected and why data was collected. Additionally, it provides the right to opt out of the sale of personal information to third parties or request its deletion.[3] The CCPA creates certain obstacles for companies that utilize consumer data for online marketing. For example, because it provides Californians with the right to request the deletion of data about themselves, such as their browsing history on a retailer's website, the CCPA may reduce the amount of personal data available to businesses.[4] This is significant because businesses generate substantial revenue from targeted advertising to customers that are users on internet platforms such as Facebook and Google.[5] Consequently, targeted advertising might become less precise due to a decrease in information about those consumers that request the deletion of their data.[6]

Similarly, companies that collect data about consumers and sell that data to others for marketing purposes, commonly known as third-party data brokers,[7] will likely also be impacted by the CCPA.[8] Third-party data brokers do not have a direct relationship with the consumers from

[1] *See* California Consumer Privacy Act of 2018, Cal. Assemb. B. No. 375 (to be codified as amended at CAL. CIV. CODE § 1798.100 (2019)).

[2] *Id.*

[3] Dipayan Ghosh, *What You Need to Know About California's New Data Privacy Law*, HARV. BUS. REV. (July 11, 2018), https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law. These rights are similar to those outlined in the European Union's General Data Protection Regulation ("GDPR"), which took effect in May 2018 and is considered to be the world's toughest set of rules for protection of people's online data. *See* Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (June 28, 2018, 5:57 PM), https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill; *see also* Adam Satariano, *G.D.P.R., A New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. TIMES (May 24, 2018), https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html.

[4] *See* Ghosh, *supra* note 3.

[5] *See id.*

[6] *See id.*

[7] Yael Grauer, *What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?*, VICE (Mar. 27, 2018, 7:00 AM), https://www.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection.

[8] *See* Antonio García Martínez, *Why California's Privacy Law Won't Hurt Facebook or Google*, WIRED (Aug. 31, 2018, 8:00 AM), https://www.wired.com/story/why-californias-privacy-law-wont-hurt-facebook-or-google.

whom they are collecting data.[9] Instead, they develop consumer profiles using information from various sources (e.g., a pharmacy chain that knows your phone number which you entered at checkout to save five percent) and organize the data based on categories such as age, ethnicity, education level, income, number of children, and interests.[10] These profiles can be purchased by businesses to better tailor marketing.[11] The CCPA directly addresses the information gathering practices of third-party data brokers by providing the consumer's right to opt out of the sale of personal information.[12]

Despite the progress it signals, the CCPA does not adequately address certain important privacy issues. First, internet platforms such as Facebook and Google may not be regulated in a meaningful way because the CCPA focuses on personal data collected by or shared with third parties.[13] In general, Facebook's data collection is based on a direct relationship with its users such that personal information is voluntarily provided on its website and its affiliated applications such as Instagram and WhatsApp.[14] Second, the CCPA provides a narrow private right of action[15] that only permits consumer lawsuits in instances of data loss or theft, such as when an individual's credit card information is stolen.[16] Lastly, companies are only required to disclose the kinds of data being shared rather than naming the third parties that gain access to the data.[17]

Privacy activists, looking for a sword to wield against Silicon Valley's tech companies,[18] are focused on pushing for the passage of new legislation as the primary means to effectuate change.[19] So far, such

[9] Grauer, *supra* note 7.

[10] *See id.*

[11] *Id.*

[12] Ghosh, *supra* note 3; *see also* García Martínez, *supra* note 8.

[13] *See* García Martínez, *supra* note 8.

[14] *See id.*

[15] Nicholas Confessore, *The Unlikely Activists That Took on Silicon Valley – and Won*, N.Y. TIMES (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html [hereinafter *The Unlikely Activists*].

[16] García Martínez, *supra* note 8.

[17] Confessore, *The Unlikely Activists*, *supra* note 15.

[18] *See Privacy Coalition Opposition to Exempting Online Advertising in CA Privacy Law*, ELECTRONIC FRONTIER FOUND. (Aug. 28, 2018), https://www.eff.org/document/privacy-coalition-opposition-exempting-online-advertising-ca-privacy-law [https://perma.cc/VPC7-KE9M] (describing opposition by privacy organizations to industry efforts to amend AB 375 (California Consumer Privacy Act) through SB 1121 and exempt online advertising from privacy protections).

[19] *See* Issie Lapowsky, *The Fight Over California's Privacy Bill Has Only Just Begun*, WIRED (Aug. 29, 2018, 10:27 AM), https://www.wired.com/story/california-privacy-bill-

efforts have been ineffective.[20] Only three months after passing the CCPA, California's governor signed the first round of revisions to the statute.[21] And while the revisions did not include the entire "wish list" of the tech industry's leading lobbying groups,[22] they did include a clarification for the private cause of action that provides a degree of leniency to the tech industry.[23] The revision states that a civil suit for data breaches may only be brought if a consumer provides a business thirty days' written notice and an opportunity to cure any violation.[24] History shows that effective enforcement of privacy statutes has been determined by an individual's ability to pursue civil action.[25] Within the

tech-lobbying [hereinafter *Fight Over California's Privacy*]; *see also* Andy Green, *The California Privacy Act (CCPA) Clones Are Coming: States Draft Copycat Laws*, VARONIS (Sept. 4, 2019), https://www.varonis.com/blog/the-california-privacy-act-ccpa-clones-are-coming-states-draft-their-own-laws/ (outlining the important differences between the proposed state laws mirroring the CCPA); Rachel R. Marmor et al., *"Copycat CPPA" Bills Introduced States Across Country*, DAVIS WRIGHT TREMAINE LLP (Feb. 8, 2019), https://www.dwt.com/blogs/privacy--security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou [https://perma.cc/7YRD-HPAD] (listing nine states that have introduced draft bills similar to the CCPA).

[20] *See* 2019 *Privacy Legislation Related to Internet Service Providers – 2019*, NAT'L CONF. OF ST. LEGISLATURES (June 17, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/2019-privacy-legislation-related-to-internet-service-providers.aspx [https://perma.cc/YR4D-NU8E] (explaining that five out of fourteen states that are considering measures in 2019 to restrict how internet service providers can collect or share consumer data have already failed); *2018 Privacy Legislation Related to Internet Service Providers – 2018*, NAT'L CONF. OF ST. LEGISLATURES. (May 13, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers-2018.aspx [https://perma.cc/3C8F-86V8] (listing states that are considering measures in 2018 to restrict how internet service providers can collect or share consumer data).

[21] *See* Dena M. Castricone & Daniel J. Kagan, *California Governor Approves Revisions to Consumer Privacy Act*, NAT'L L. REV. (Sept. 25, 2018), https://www.natlawreview.com/article/california-governor-approves-revisions-to-consumer-privacy-act [https://perma.cc/VFN5-NS59].

[22] A coalition of nearly forty organizations from within the banking and film industries, and including the tech industry's leading lobbying groups, signed a twenty-page letter proposing amendments and modifications to the lawmakers behind SB-1121. *See* Letter from Privacy Coalition to Senator Bill Dodd (Aug. 6, 2018), http://netchoice.org/wp-content/uploads/SB-1121-Final-Author-Coalition-Letter-2.8.7.2018.pdf [https://perma.cc/H4CQ-3CSN].

[23] Jason C. Gavejian et al., *California Consumer Privacy Act Amendment Signed into Law*, NAT'L L. REV. (Sept. 25, 2018), https://www.natlawreview.com/article/california-consumer-privacy-act-amendment-signed-law [https://perma.cc/6PMX-DG8C].

[24] *Id.*

[25] *See Video and Library Privacy Protection Act of 1988: Joint Hearing on H.R. 4947 and S. 2361 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary and the Subcomm. on Tech. & the Law of the S. Comm. on the*

last four years, public mistrust of social platforms has steadily risen along with a desire for the federal government to impose more regulation on advertisers.[26] Consequently, the tech industry fears a private right of action because it puts interpretation of new rules in the hands of a jury rather than a regulator.[27] The weakening of the CCPA private cause of action thus compromises the efficacy of the Act as a whole, and signals that there is reason to doubt pursuing legislative battles will significantly impact tech companies or provide additional consumer privacy protections.[28]

Given the uncertainties of whether new legislation will prove effective, proponents of civil liberties in the digital world should consider the protections of the Video Privacy Protection Act of 1988 ("VPPA"),[29] which prohibits a video company from disclosing a user's watch history without the user's consent.[30] Lawmakers who have claimed there currently exists no meaningful federal protection for consumer data[31] ignore the potential application of the VPPA to digital media.[32] American adults have shifted dramatically from watching video

Judiciary, 100th Cong. 62 (1988) [hereinafter *VPPA Joint Hearings*] (discussing the ACLU's support of the VPPA because of its civil remedy).

[26] *See* Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RES. CTR. (Mar. 27, 2018), http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns.

[27] *See* Confessore, *The Unlikely Activists*, *supra* note 15.

[28] *See* Lapowsky, *Fight Over California's Privacy*, *supra* note 19.

[29] *See The Video Privacy Protection Act as a Model Intellectual Privacy Statute*, 131 HARV. L. REV. 1766, 1786-87 (2018) [hereinafter *Model Intellectual Privacy Statute*].

[30] *See generally The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century Hearing before the Subcomm. on Privacy, Tech., & the Law of the S. Comm. on the Judiciary U.S. S.*, 112th Cong. 2 (2012) [hereinafter *Video Privacy Protection Act Hearing*] (statement of Sen. Al Franken) (explaining what the VPPA is and how it protects consumer privacy).

[31] *Consumer Data Privacy: Examining the European Union's General Data Protection Regulation and the California Consumer Privacy Act: Hearing Before Senate Comm. on Commerce., Sci., and Transp.*, 115th Cong. 2 (2018) [hereinafter *Consumer Data Privacy Hearing*] (statement of Sen. Richard Blumenthal) (discussing the need for federal protection for consumer data); *see also id.* (statement of Sen. Tammy Duckworth) (discussing the lack of federal government action relating to digital security for consumers).

[32] *Compare Examining Safeguards for Consumer Data Privacy: Hearing Before Senate Comm. on Commerce, Sci., and Transp.*, 115th Cong. 2 (2018) [hereinafter *Examining Safeguards Hearing*] (statement of Sen. John Thune, Chairman, S. Comm. on Commerce, Sci., and Transp.) (discussing privacy laws that have been enacted in the past twenty years such as the Children's Online Privacy Protection Act, the Health Insurance Portability Act, and the Gramm-Leech-Bliley Act), *with infra* Part I.E (describing legislative efforts to update the VPPA with twenty-first century consumer

content on a traditional television set to digital platforms.[33] Over a third of persons use their internet connected devices to access video content.[34] In response to that trend, social plugins — embeddable buttons and widgets that allow users to share content from a website or an app on their personal social media profiles — have become the most popular way for websites to track what content their users are watching to increase customer engagement.[35] However, data gathered via plugins is being disclosed to third parties without consumer permission.[36] Since

data privacy concerns). Congress and privacy activists have shied away from a sectoral approach to privacy regulation as taken by the VPPA. *See Consumer Data Privacy Hearing*, *supra* note 31 (statement of Nuala O'Connor, President and CEO, Ctr. for Democracy and Tech.) (stating that the United States follows a sectoral approach); Daniel Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, TEACH PRIVACY (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law [https://perma.cc/8YL4-DF45] (explaining how the U.S. regulates privacy with a sectoral approach, with laws that are directed only to specific industries, whereas the E.U. has overarching law that regulates privacy consistently across all industries); *see also Examining Safeguards Hearing*, *supra* note 32 (statement of Sen. John Thune, Chair, Commerce, Sci., and Transp. Comm.) (discussing the need for a comprehensive national data privacy law). The VPPA focuses specifically on privacy protection of the video industry. *See infra* Part I.A. However, legislators have also expressed skepticism about the possibility of passing a comprehensive federal privacy law. *See, e.g.*, *Consumer Data Privacy Hearing*, *supra* note 31 (statement of Sen. Brian Schatz) (discussing how tech companies' support for a federal privacy law will depend on the effectiveness of the CCPA).

[33] *See Time Flies: U.S. Adults Now Spend Nearly Half a Day Interacting with Media*, NIELSEN (July 31, 2018), https://www.nielsen.com/us/en/insights/article/2018/time-flies-us-adults-now-spend-nearly-half-a-day-interacting-with-media/ [https://perma.cc/F6M2-DAR9].

[34] *The Nielsen Total Audience Report: Q1 2018*, NIELSEN (July 31, 2018), https://www.nielsen.com/us/en/insights/reports/2018/q1-2018-total-audience-report.html [https://perma.cc/SC95-WUUN].

[35] *See About Social Plugins and Interactions*, GOOGLE: ANALYTICS HELP, https://support.google.com/analytics/answer/6209874?hl=en (last visited Aug. 22, 2019) [https://perma.cc/GG56-TXAN]; Allen St. John, *How Facebook Tracks You, Even When You're Not on Facebook*, CONSUMER REP. (Apr. 11, 2018), https://www.consumerreports.org/privacy/how-facebook-tracks-you-even-when-youre-not-on-facebook [https://perma.cc/67UP-8LRP]; *infra* Part I.D; *see also* Michael Guta, *WordPress Powers 30 Percent of the Top 10 Million Sites, How About Yours?* SMALL BUS. TRENDS (Mar. 8, 2018), https://smallbiztrends.com/2018/03/wordpress-powers-30-percent-of-websites.html [https://perma.cc/2JDZ-MJG6] (discussing how WordPress is now used on 30 percent of the top 10 million sites); *What is WordPress?*, ITHEMES, https://ithemes.com/tutorials/what-is-wordpress (last visited Jan. 4, 2019) [https://perma.cc/K97U-5U65] (explaining that Wordpress is a software used by many Fortune 500 companies to customize their websites, including the installation of social media plugins).

[36] *See* GEORGIOS KONTAXIS ET AL., PRIVACY-PRESERVING SOCIAL PLUGINS (2012), http://web5.cs.columbia.edu/~angelos/Papers/2012/safebutton.pdf; KATHERINE MCKINLEY,

the VPPA was drafted to restrict disclosure of the sort of video content now widely viewed online, it represents a viable option for providing immediate protection to consumer data.[37]

The current bipartisan concern for consumer privacy and demand for federal legislation[38] is akin to the public sentiment which produced the VPPA.[39] Furthermore, lawmakers behind the VPPA considered the implications of rapidly advancing technology[40] just as today's Congress considers the privacy dangers of the information age.[41] Despite these parallels, big tech lobbying efforts reduce the likelihood that the CCPA will live up to its potential.[42] Even more disconcerting is that the VPPA's ability to strengthen consumer privacy protection is not being stifled by Silicon Valley but rather the judicial system, as illustrated by three of the dispositions in *In re Hulu Privacy Litigation* ("*Hulu*"), a case from the United States District Court for the Northern District of California.[43] Courts must recognize that a significant amount of digital content fits within the scope of the VPPA in light of the technological processes underlying its delivery.[44]

The VPPA provides privacy protection for an individual's video viewing histories from disclosure to others without the individual's consent.[45] To state a claim under the VPPA, a plaintiff must prove (1) a "video tape service provider" (2) *knowingly* disclosed (3) "personally identifiable information" (4) concerning one of its consumers (5) to a

CLEANING UP AFTER COOKIES VERSION 1.0, at 2 (2008), https://www.nccgroup.trust/globalassets/our-research/us/whitepapers/isec_cleaning_up_after_cookies.pdf.

[37] *See infra* Part I.C.

[38] *See Examining Safeguards Hearing*, *supra* note 32 (statement of Sen. John Thune, Chairman, S. Comm. on Commerce, Sci., and Transp.) (stating that there is bipartisan support for a national consumer data privacy law).

[39] *See VPPA Joint Hearings*, *supra* note 25, at 18-19 (mentioning the strong bipartisan response to Judge Bork's video rental history which gave rise to the call for legislation).

[40] *See* 134 CONG. REC. S6,312 (daily ed. Oct. 14, 1988) (statement of Sen. Patrick Leahy) (acknowledging that records from public transactions can be compiled to form a personal dossier).

[41] *See Consumer Data Privacy Hearing*, *supra* note 31 (statement of Sen. Maria Cantwell) (acknowledging the privacy implications of internet technology).

[42] *See supra* notes 21–24 (discussing lobbying efforts to weaken the CCPA private cause of action).

[43] *In re* Hulu Privacy Litig. (*In re Hulu III*), 86 F. Supp. 3d 1090 (N.D. Cal. 2015); *In re* Hulu Privacy Litig. (*In re Hulu II*), No. C 11-03764 LB, 2014 WL 1724344 (N.D. Cal. Apr. 28, 2014); *In re* Hulu Privacy Litig. (*In re Hulu I*), No. C 11-03764 LB, 2012 WL 3282960 (N.D. Cal. Aug. 10, 2012); *see also infra* Part II.

[44] *See infra* Part III.

[45] 134 CONG. REC. S5397-01, at 7 (1988) (statement of Sen. Patrick Leahy) (explaining the intent of the bill is to prohibit the disclosure of video rental records).

third party.[46] Understanding how online video streaming technology is applicable to a VPPA claim requires an examination of the three dispositions from *Hulu*, which include a 2012 order denying a motion to dismiss the class action complaint ("*In re Hulu I*"),[47] an order granting in part and denying in part a summary judgment motion ("*In re Hulu II*"),[48] and an order granting a summary judgment motion ("*In re Hulu III*").[49] *Hulu* was the first case to consider whether online video streaming platforms fit within the scope of the VPPA.[50] The court determined that the VPPA applied to online streaming services because Hulu constituted a "video tape service provider."[51] Additionally, *Hulu* was the first case to address the knowledge element of the VPPA, ruling that a plaintiff must prove that the video service provider knew it was disclosing information connecting a certain user to certain videos or that a third party would actually link information it had with other information conveyed and become aware that a particular person had in fact viewed a particular video.[52] No cases have challenged this definition of the knowledge requirement under the VPPA.[53]

This Note analyzes how judicial interpretation of the knowledge element of the VPPA has incorrectly made the statute inapplicable to digital media and, as a result, failed to provide adequate privacy protection for consumers' online video viewing histories. Specifically, courts have analyzed the knowledge requirement without appropriate consideration of the technology underlying the delivery of digital media. This Note argues that courts should construe an internet platform's use of social plugins as actual knowledge of the disclosure of personally identifiable information under the VPPA.

---

[46] *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 279 (3rd Cir. 2016); *see* Mollett v. Netflix, Inc., 795 F.3d 1062, 1066 (9th Cir. 2015).

[47] *In re Hulu I*, 2012 WL 3282960.

[48] *In re Hulu II*, 2014 WL 1724344.

[49] *In re Hulu III*, 86 F. Supp. 3d 1090.

[50] *In re Hulu I*, 2012 WL 3282960, at *5-6; *Model Intellectual Privacy Statute*, *supra* note 29, at 1770.

[51] *In re Hulu I*, 2012 WL 3282960, at *5-6.

[52] *In re Hulu III*, 86 F. Supp. 3d at 1095 ("[T]he term "knowingly" connotes actual knowledge."); *In re Hulu II*, 2014 WL 1724344, at *15 ("No case has construed the word "knowingly" as it appears in the VPPA."); *see also* Chris King, *Three Years of Change: Recent Court Cases Under the Video Privacy Protection Act*, 26 DEPAUL J. ART, TECH. & INTELL. PROP. L. 135, 142 (2016).

[53] *See, e.g.*, Bernardino v. Barnes & Noble Booksellers, Inc., 17-CV-04570, 2017 WL 3727230, at *9 (S.D.N.Y. 2017) (referencing how the court in *Hulu* addressed the knowledge element of a VPPA violation); Robinson v. Disney Online, 152 F. Supp. 3d 176, 182 (S.D.N.Y. 2015) (describing how the court in *Hulu* addressed contextual information about whether disclosure was done knowingly).

Part I provides background on the circumstances that led to the enactment of the VPPA, the emergence of the internet advertising industry and related technologies, and the statutory language of the VPPA as developed through case law and statutory amendment. Part II argues that the United States District Court for the Northern District of California's significant characterization of code in transmitting data in *Hulu* is flawed and wrongly renders the VPPA inapplicable to digital media. Part III argues that the court in *Hulu* misapplied the Electronic Communications Privacy Act's definition of the term "knowingly." Part IV argues that the use of social plugins should constitute actual knowledge under the VPPA. Finally, Part V proposes a judicial solution given the difficulties presented by legislation.

I. BACKGROUND OF THE VPPA

A. Statute and Statutory Language

The VPPA prohibits video service providers from disclosing personally identifiable information ("PII") except in certain, limited circumstances.[54] The VPPA "reflects the central principle of the Privacy Act of 1974: that information collected for one purpose may not be used for a different purpose without the individual's consent."[55] The VPPA's broad, technology-neutral language, has made it generally resilient to technological and doctrinal changes.[56]

The VPPA 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 for the relief . . . ."[57] Under the statute, a consumer is defined as "any renter, purchaser, or subscriber of goods or services from a video tape service provider."[58] "Personally identifiable information" means "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."[59] A video tape service provider is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials

[54] S. REP. NO. 100-599, pt. 3, at 5 (1988).
[55] *Id.* at 7.
[56] *Model Intellectual Privacy Statute*, *supra* note 29, at 1768-69.
[57] 18 U.S.C. § 2710(b)(1) (2019).
[58] *Id.* § 2710(a)(1).
[59] *Id.* § 2710(a)(3).

. . . ."[60] Finally, the statute does not define the mens rea element,[61] and no opinion prior to *In re Hulu II* in 2014 construed the word "knowingly" as it appears in the VPPA.[62]

B. Enactment of the VPPA in Response to the Debate on the Right to Privacy

A review of the origins of the VPPA helps to illustrate that it is relevant in important respects to privacy concerns in the digital age. The VPPA was drafted as a measure to ensure the titles of the movies people watched would be protected against disclosure without their consent.[63] The legislative motivation to pass the bill came after a newspaper in Washington published an article listing the titles of over one hundred films Judge Robert H. Bork's family had rented from a video store.[64] The story broke while the Senate Judiciary Committee was holding hearings on Judge Bork's nomination to the Supreme Court in 1987.[65] Apart from concerns about Judge Bork's privacy,[66] lawmakers asserted that a person's right to privacy protects the choice of movies he or she watches because they reflect that person's individuality.[67] During a joint hearing, Senator Pat Leahy, a drafter of the VPPA and Chairman of the Senate Judiciary Committee's Subcommittee on Technology and the Law, stated:

> If we are going to tell people . . . who want to be in any form of public life . . . we are going to go all the way back and find out what . . . you took out on videos or what you watch at night on television programs, then we are in a sorry state.[68]

Senator Leahy's statement generated consensus among members of the Senate Judiciary Committee's Subcommittee on Technology and the Law and the House Judiciary Committee's Subcommittee on Courts,

---

[60] *Id.* § 2710(a)(4).

[61] *See id.* § 2710.

[62] *In re Hulu II*, No. C 11-03764 LB, 2014 WL 1724344, at *15 (N.D. Cal. Apr. 28, 2014).

[63] 134 CONG. REC. S5397-01, *supra* note 45, at 6 (statement of Sen. Patrick Leahy) (explaining the intent of the VPPA).

[64] S. REP. NO. 100-599, pt. 3, at 5 (1988).

[65] *Id.*

[66] *See* 134 CONG. REC. S5397-01, *supra* note 45, at 6 (statement of Sen. Leahy).

[67] *Id.*

[68] *VPPA Joint Hearings*, *supra* note 25, at 19.

Civil Liberties, and the Administration of Justice on the importance of intellectual privacy.[69]

C. Technological Advancement

Additionally, the VPPA was drafted in response to privacy concerns related to technological advancements in information collection via computers.[70] Specifically, lawmakers expressed concerns about the "subtlety of th[e] problem"[71] of transactional data: the trail of information generated by every monetary transaction in an individual's daily life that is recorded and stored in sophisticated recordkeeping systems.[72] Congress worried that transaction information would enable private entities to generate dossiers on individual activity.[73] One member of the House of Representatives described the privacy protection of a consumer's video viewing history as a chain-link fence in need of a brick wall (the VPPA) because, at that point, the consumer's right to privacy was based solely on the discretion of a merchant.[74]

The American Civil Liberties Union substantiated this concern in testimony to Congress during a joint session.[75] It exposed American Express, which used new technology to track cardholders' charges and provided that transaction data to third parties for targeted advertising.[76] Consequently, Congress[77] implemented civil remedies to ensure that the VPPA would be enforced by individuals who suffer as a result of

---

[69] *See Model Intellectual Privacy Statute*, *supra* note 29, at 1766-67; *see VPPA Joint Hearings*, *supra* note 25, at 18-19 (discussing bipartisan support for the bill). Intellectual privacy refers to the notion that every individual has the right to engage with content without the threat of surveillance. *See* Evan Selinger, *What is Intellectual Privacy, and How Yours is Being Violated*, CHRISTIAN SCI. MONITOR (Feb. 25, 2015), https://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0225/What-is-intellectual-privacy-and-how-yours-is-being-violated; *Model Intellectual Privacy Statute*, *supra* note 29, at 1766-67; *VPPA Joint Hearings*, *supra* note 25, at 67 (discussing the constitutional right to privacy); *see also* S. REP. NO. 100-599, *supra* note 64, at 7 (discussing the importance of privacy as it relates to learning).

[70] *See* 134 CONG. REC. S5397-01, *supra* note 45, at 6.

[71] *Id.* at 7.

[72] *Id.* ("[T]he trail of information generated by every transaction that is now recorded and stored in sophisticated recordkeeping systems.").

[73] *VPPA Joint Hearings*, *supra* note 25, at 55.

[74] *Id.* at 30.

[75] *See id.* at 57-74.

[76] *Id.* at 56.

[77] *See VPPA Joint Hearings*, *supra* note 25, at 24 (statement of Mr. Moorhead) (crediting members of the Senate and House of Representatives for sponsoring the bill).

unauthorized disclosures.[78] Furthermore, the legislation included a federal cause of action for unauthorized disclosures of consumer viewing histories to ensure that individuals would maintain control over their personal information when renting or purchasing a movie.[79]

The moviegoer of 1988, the year the VPPA was enacted,[80] has been replaced by its information-age analogue — the binge watcher of digital content on Netflix.[81] This has raised questions about whether the VPPA is outdated and ill-suited for protecting consumers' online viewing histories.[82] Consumer demand for digital video content is ever-increasing as more online entertainment platforms emerge and offer original programming, making the VPPA's applicability to streaming services significant for consumer privacy.[83]

But the drafters of the VPPA were concerned with the possibility that technological innovation would present new "Big Brother" types of surveillance.[84] The surveillance threats predicted by Congress have come to fruition by way of "surveillance capitalism" that is now prevalent.[85] By simply engaging with online platforms (e.g., using social network services and search engines), users automatically provide their demographic data for free to online companies.[86] The direct relationship between the user and online platform that an individual opts in to when

[78] S. REP. NO. 100-599, *supra* note 64, at 8 (explaining the "civil remedies section puts teeth into the legislation").

[79] 134 CONG. REC. S5397-01, *supra* note 45, at 13 (statement of Mr. Simon) (stating the bill ensures consumer control over personal information relating to video viewing history).

[80] Video Privacy Protection Act, 18 U.S.C. § 2710 (2019).

[81] *Netflix Declares Binge Watching is the New Normal,* CISION PR NEWSWIRE (Dec. 13, 2013), https://www.prnewswire.com/news-releases/netflix-declares-binge-watching-is-the-new-normal-235713431.html.

[82] *Video Privacy Protection Act Hearing*, *supra* note 30, at 2 (statement of Sen. Al Franken) (acknowledging that some individuals consider the VPPA outdated).

[83] *See* Juan Pablo Manterola, *Online Streaming is the Future of Sports Broadcasting: It's Not 'If' You'll Cut Cable, but 'When*,' FORBES (Apr. 14, 2017, 9:00 AM), https://www.forbes.com/sites/forbesagencycouncil/2017/04/14/online-streaming-is-the-future-of-sports-broadcasting-its-not-if-youll-cut-cable-but-when/#60183f893bbc (discussing the emergence of the digital experience via social media platforms, a seemingly infinite number of hours of live-streaming network and cable content, and the original programming of video streaming services such as Hulu and Amazon).

[84] S. REP. NO. 100-599, *supra* note 64, at 5-7 (discussing the threats to individual privacy because of emerging technologies).

[85] *See* John Laidler, *High Tech is Watching You*, HARV. GAZETTE: BUS. & ECON. (Mar. 4, 2019), https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy.

[86] *See id.*

signing up for an online platform, such as Gmail[87] or Facebook,[88] provides for the sale of information to advertisers.[89] Because the technical aspects of data collection practices are challenging to understand,[90] a brief overview of the generation and transmission of a user's data while the user browses the internet follows. These details help inform a later discussion of the factual circumstances necessary for a video service provider to be deemed to have *knowingly* disclosed a consumer's viewing history to a third party without their consent under the VPPA.[91]

D. Cookies, Pixels, and Similar Technologies

Internet users surf the web by using a browser such as Safari, Internet Explorer, or Firefox.[92] A user's browser choice depends in large part on the features offered by each browser.[93] Whether it is reliability, organizational tools, or relative simplicity, user preferences are driven by customizability.[94] With that in mind, when a user visits a website, the site places a cookie, a small text string,[95] on the user's web browser. This allows the website to recognize the user's computer, keep track of the user's activities on the site, and enhance the user experience.[96]

---

87 *See* KONTAXIS ET AL., *supra* note 36.

88 *See* García Martínez, *supra* note 8.

89 *See* Paul Blumenthal, *Facebook And Google's Surveillance Capitalism Model is in Trouble*, HUFFPOST (Jan. 29, 2018), https://www.huffingtonpost.com/entry/facebook-google-privacy-antitrust_us_5a625023e4b0dc592a088f6c.

90 *See generally* Nicholas Confessore, *Demystifying Online Privacy, Through the Story of the Man Who Took on Silicon Valley*, N.Y. TIMES (Aug. 18, 2018), https://www.nytimes.com/2018/08/18/insider/online-privacy-facebook-data-google.html.

91 *See In re Hulu III*, 86 F. Supp. 3d 1090, 1097 (N.D. Cal. 2015).

92 Scott Gilbertson, *The Curious Case of Web Browser Names*, WIRED (Jan. 13, 2012, 1:03 PM), https://www.wired.com/2012/01/the-curious-case-of-web-browser-names.

93 *See* Jim Martin, *The Best Web Browsers for 2019*, TECH ADVISOR (Aug. 6, 2019), https://www.techadvisor.co.uk/test-centre/software/best-web-browsers-3635255 (analyzing the best web browsers based on performance, security, and features).

94 *See id.* (discussing how Microsoft is rebuilding its Edge browser to include additional features such as extensions, themes, and other useful tools).

95 Lynette I. Millett et al., *Cookies and Web Browser Design: Toward Realizing Informed Consent Online*, 3 TRANSACTIONS ON COMPUTER-HUM. INTERACTION 46, 46 (2001).

96 *See Internet Cookies*, FED. TRADE COMM'N, https://www.ftc.gov/site-information/privacy-policy/internet-cookies (last updated Mar. 2018) [hereinafter *Internet Cookies*].

However, "different types of cookies keep track of different activities."[97] Session cookies are used only when a user is actively navigating a website and are then deleted once the user leaves the site.[98] These cookies make it possible for the site to keep track of the items in a consumer's digital shopping cart until checkout[99] and store consumer's login credentials for future use.[100] By comparison, persistent cookies remain on a user's computer and record information every time they visit the site.[101] As a result, the site is able to keep track of a consumer's preferences[102] with an aim of customizing the browsing experience and providing personalized features.[103] Taken together, all of these features are only available as a result of user tracking: the cookie exchange that occurs between the user and site[104] for every "click" request while browsing the site.[105]

Concerns about user tracking arise when a third party — an entity other than the site the user is visiting — is allowed to place cookies on the user's browser.[106] These so-called third-party cookies[107] are used when a user visits a webpage and content from another site is referenced, such as an advertisement[108] or a social media plugin.[109] Third-party cookies come in the form of tracking pixels, a barely perceptible dot that is purposely hidden in the background of a web page.[110] Businesses choose to install an advertising platform's pixels on

[97] *What are Cookies?*, NORTON, https://us.norton.com/internetsecurity-how-to-what-are-cookies.html (last visited Oct. 19, 2019).

[98] *Id.*

[99] MCKINLEY, *supra* note 36, at 2.

[100] Jessica Davies, *Know Your Cookies: A Guide to Internet Ad Trackers*, DIGIDAY (Nov. 1, 2017), https://digiday.com/media/know-cookies-guide-internet-ad-trackers.

[101] *Internet Cookies*, *supra* note 96.

[102] *See id.*

[103] *Id.*; MCKINLEY, *supra* note 36, at 2; *see also* Millett et al., *supra* note 95, at 46.

[104] *See Online Tracking*, FED. TRADE COMM'N, https://www.consumer.ftc.gov/articles/0042-online-tracking (last updated June 2016) [hereinafter *Online Tracking*] ("First-party cookies are placed by the site that you visit. They can make your experience on the web more efficient.").

[105] *See* MCKINLEY, *supra* note 36, at 2 (explaining how cookies "can be used to track a user's activity").

[106] *Id.*

[107] *Online Tracking*, *supra* note 104.

[108] MCKINLEY, *supra* note 36, at 2.

[109] *See* Allen St. John, *How Facebook Tracks You, Even When You're Not on Facebook*, CONSUMER REP. (Apr. 11, 2018), https://www.consumerreports.org/privacy/how-facebook-tracks-you-even-when-youre-not-on-facebook/.

[110] *See, e.g.*, Hamdan Azhar, *Politicians Don't Trust Facebook–Unless They're Campaigning*, WIRED (June 26, 2019, 8:03 PM), https://www.wired.com/story/facebook-

their website as an analytics tool to improve the effectiveness of their advertising by understanding the actions people take on their website.[111] Pixels work as follows.

A business installs the pixel onto its website and then tracks actions people are taking on its website.[112] This level of customization allows businesses to attract website visitors back in a cost-efficient way known as retargeting.[113] For example, a company may include the Facebook pixel on their site.[114] When a user leaves an item in their shopping cart without completing the purchase, the company can target those users through highly targeted ads on Facebook reminding them to buy the product.[115] As a result, companies are able to reach people who have visited a specific page or taken a particular action on its website and target people who are more likely to make a purchase.[116] However, this increased ability to advertise to a desired audience[117] comes at a cost to consumer privacy.[118]

The tracking data from pixels placed on websites allows advertising platforms to tie the data collected to the individual users.[119] Although

privacy-candidates-pixel-campaigning (describing how Facebook pixel technology is embedded on political campaign websites in order to increase the candidate's reach to constituents); Brian Barrett *A Clever Way to Tell Which of Your Emails are Being Tracked*, WIRED (March 20, 2015, 8:00 AM) https://www.wired.com/2015/03/ugly-mail/ (discussing how the sender of an email utilizes pixel technology by "insert[ing] a transparent 1x1 image" into an email to track when a recipient has opened that email).

111 *See About Facebook Pixel*, FACEBOOK, https://www.facebook.com/business/help/742478679120153?helpref=faq_content (last updated July 18, 2019) [hereinafter *About Facebook Pixel*].

112 *See Use Facebook Pixel*, FACEBOOK, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited December 18, 2019) (explaining that users' actions that are desirable to track include "Add to cart," "Add to wishlist," "Schedule," "Start trial," "Subscribe").

113 Brett Farmiloe, *Five Effective Types of Retargeting Ads That Work on a Small Budget*, FORBES (Dec. 4, 2017, 7:00 AM), https://www.forbes.com/sites/forbesagencycouncil/2017/12/04/five-effective-types-of-retargeting-ads-that-work-on-a-small-budget/#193c086e5e3d.

114 St. John, *supra* note 109.

115 *Id.*

116 *See About Facebook Pixel*, *supra* note 111.

117 *See* Who *Took the Cookie? The Science Behind Targeted Advertising*, Herosmyth (Feb. 2, 1018), https://www.herosmyth.com/article/who-took-cookie-science-behind-targeted-advertising; Cameron Fitchett, *Reach and Reach Efficiency in Digital Advertising*, GIMBAL (Apr. 14, 2015), https://gimbal.com/reach-and-reach-efficiency-in-digital-advertising (describing the concept of "reach efficiency" as a way of measuring how efficiently an ad campaign reaches its target audience).

118 *See* St. John, *supra* note 109.

119 Derek Belt, *Why Facebook Pixels Are Not Allowed On Our Website*, GOVLOOP (Mar. 23, 2016), https://www.govloop.com/community/blog/facebook-pixels-not-allowed-

there is a lack of consensus regarding how to define PII on the internet,[120] the broad availability of data heightens the ability to turn non-PII into PII.[121] The process involves aggregating and combining various pieces of data to link de-identified data with those already identified.[122] This is made easier by corporate practices that involve gathering large amounts and various kinds of information from users' online activities.[123] For example, researchers examined a publicly released dataset from Netflix containing 100,480,507 movie ratings from its subscribers.[124] The company claimed that all customer identifying information had been removed.[125] Yet the researchers were able to identify Netflix subscribers from the dataset by measuring similarities in user movie ratings on the Internet Movie Database ("IMDB").[126] With the technological capabilities of combining data[127] and the dominance of Google and Facebook,[128] which control eighty-seven percent of digital advertising,[129] it is evident that internet users

website/ (explaining how advertising platforms such as Facebook can tie the data collected to individual users via pixels, often by name); s*ee* Blumenthal, *supra* note 89 (discussing personal information people share for free on social media); Jennifer Senior, *Review: 'The Attention Merchants' Dissects the Battle for Clicks and Eyeballs*, N.Y. TIMES (Nov. 2, 2016), https://www.nytimes.com/2016/11/03/books/review-attention-merchants-tim-wu.html.

120 Paul M. Schwartz & David J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1835 (2011) (describing the debate in the United States about how to determine whether certain data are identifiable to a person for purposes of privacy law and regulation).

121 *Id.* at 1842.

122 *Id.* Deidentified data refers to records that have had enough PII removed such that the remaining information does not identify an individual. Erika McCallister et al., *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, NAT'L INST. OF STANDARDS & TECH. ES-3 (Apr. 2010), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf. Information such as a zip code, birth date, and gender of person by itself constitutes deidentified data. Schwartz & Solove, *supra* note 120, at 1842.

123 *See* Schwartz & Solove, *supra* note 120, at 1846-47.

124 ARVIND NARAYANAN & VITALY SHMATIKOV, ROBUST DE-ANONYMIZATION OF LARGE DATASETS (HOW TO BREAK ANONYMITY OF THE NETFLIX PRIZE DATASET) 10 (2008), https://arxiv.org/pdf/cs/0610105.pdf.

125 *Id.*

126 *Id.* at 1.

127 Schwartz & Solove, *supra* note 120, at 1842.

128 *See* Blumenthal, *supra* note 89.

129 Mark Bergen & Sarah Frier, *Facebook's Data Crackdown Has Two Winners: Facebook and Google*, BLOOMBERG (Apr. 6, 2018, 2:00 AM), https://www.bloomberg.com/news/articles/2018-04-06/facebook-s-data-crackdown-has-two-winners-facebook-and-google?mod=article_inline.

gave away their PII a long time ago with the rise of social and live streaming platforms.[130]

E. The VPPA's 2012 Amendment

The VPPA was amended in 2012 to clarify that a video tape service provider may obtain a consumer's informed, written consent to share PII on an ongoing basis.[131] It also allowed consent to be obtained through the internet.[132] Specifically, it allowed the consumer to consent once before a service provider shared their movie or TV show preferences with a third party.[133] Netflix launched a public campaign in support of the amendment.[134] Citing strong consumer interest in the opportunity to share and discover movies with their friends through Facebook,[135] Netflix argued that obtaining opt-in consent every time a viewer's movie choices get forwarded to a third party would hinder social video innovation.[136]

Opponents of the amendment argued that it would undo users' ability to give case-by-case permission to a video company on what it can disclose to third parties.[137] Consequently, the opponents contended, consumers acquiescing to a one-time blanket consent to cover future video choices would not constitute meaningful consent.[138] With regard to Netflix's support for the bill, legislators referred to the company's two prior failed attempts to integrate Facebook into its platform.[139] These attempts were presented as evidence that the bill's singular focus was on facilitating wide-scale disclosure rather than protecting users' personal information.[140] Additionally, opponents of the amendment asserted that its failure to update the damages provision to adequately discourage violations indicated the sole motivation for passing the bill

130 *See generally* Lee Rainie & Janna Anderson, *Trust Will Not Grow, But Technology Usage Will Continue to Rise as A 'New Normal' Sets In*, PEW RES. CTR. INTERNET & TECH. (Aug. 10, 2017), http://www.pewinternet.org/2017/08/10/theme-3-trust-will-not-grow-but-technology-usage-will-continue-to-rise-as-a-new-normal-sets-in (discussing the growing distrust between consumers and tech companies).

131 158 CONG. REC. H6828-03 (daily ed. Dec. 17, 2012).

132 *Id.*

133 158 CONG. REC. H6849-01 (daily ed. Dec. 18, 2012).

134 *See* H.R. REP. NO. 112-312, at 10 (2011).

135 *Video Privacy Protection Act Hearing*, *supra* note 30, at 10.

136 *See id.* at 11.

137 *Id.* at 3.

138 *Id.* at 14.

139 H.R. REP. NO. 112-312, *supra* note 134, at 9-11.

140 *Id.* at 11.

was to facilitate disclosure, not protect consumer interests.[141] This was significant given that online video streaming platforms were already earning billions of dollars.[142]

In essence, the question presented by the amendment was whether lawmakers should err on the side of protecting privacy or promoting commerce.[143] Lawmakers emphasized the need for genuine consent in regulating the collection and use of PII in the digital world[144] — that is, that a consumer's choice to post personal information online is an intentional act.[145] As a result, legislative efforts were made to ensure a clear way to withdraw that consent later if a user decided that they did not want a particular movie they watched to be shared with friends or to cancel the previous authorization all together.[146] Nevertheless, the 2012 amendment to the VPPA serves as an example of the successful lobbying efforts of a tech company chipping away at consumer privacy protections by apparently "equating technological expediency with consumer preferences."[147]

II. THE *HULU* COURT'S INTERPRETATION OF CODE IN TRANSMITTING DATA IS FLAWED AND RENDERS THE VPPA INAPPLICABLE TO DIGITAL MEDIA

The VPPA does not define "knowingly,"[148] and prior to 2014, no case had addressed its meaning.[149] At long last, the Northern District of California in *Hulu* determined the term "knowingly" means "consciousness of transmitting private information," not the mere transmission of code.[150] This implies that the knowledge requirement is only satisfied by knowing that *what is transmitted* will produce PII rather than *how* the transmission occurs.[151] The court reasoned that its

141 *See id.* at 12.

142 *Id.*

143 *See Video Privacy Protection Act Hearing*, *supra* note 30, at 20 (statement of Christopher Wolf, Director, Privacy and Info. Mgmt. Grp., Hogan Lovells LLP).

144 *See id.* at 19.

145 *See id.*

146 *Id.* at 25-26.

147 *See id.* at 33.

148 *See* 18 U.S.C. § 2710(b) (2019).

149 *In re Hulu II*, No. C 11-03764 LB, 2014 WL 1724344, at *15 (N.D. Cal. Apr. 28, 2014).

150 *In re Hulu III*, 86 F. Supp. 3d 1090, 1095 (N.D. Cal. 2015).

151 *See In re Hulu II*, 2014 WL 1724344, at *14-15. (explaining that transmitting data amounts to an actionable VPPA disclosure only if the data is the equivalent of "a list of videos" that can be read by the recipient).

definition was consistent with another privacy statute, the Electronic Communications Privacy Act of 1986 ("ECPA"), on which the VPPA was modeled.[152]

Significantly, the *Hulu* court relied on the ECPA because it doubted the VPPA's applicability to internet-streaming cases altogether.[153] This doubt is consistent with a potentially flawed judicial understanding of what is properly considered PII in the context of streaming video platforms.[154] The federal circuit courts have defined PII as only that which directly identifies individuals, rather than data which might make someone identifiable.[155] Debate on this issue has resulted in a circuit split regarding the statutory definition of PII under the VPPA in today's digital world.[156] Furthermore, in 2017 the Supreme Court denied certiorari to a Third Circuit case that has contributed to the current split.[157]

Hulu involved a class action against Hulu, a digital media and streaming company, for allegedly disclosing user identifying information and customers' video viewing selections to third parties.[158] Because the disclosures were made without consent of Hulu's users, the plaintiffs alleged that Hulu violated the VPPA.[159] The case was the first to consider the applicability of the VPPA to online streaming platforms.[160] The case was widely followed because the third parties involved in the litigation were heavyweights in the media advertising

---

[152] *In re Hulu III*, 86 F. Supp. 3d at 1095.

[153] *See id.* at 1095-97 (discussing how the passing of information between humans in a natural language rather than disclosure of video or user data is what prompted the VPPA).

[154] *See Model Intellectual Privacy Statute*, *supra* note 29, at 1782.

[155] *See* Schwartz & Solove, *supra* note 120, at 1873.

[156] *Model Intellectual Privacy Statute*, *supra* note 29, at 1768, 1777; Schooner Sonntag, *A Square Peg in a Round Hole: The Current State of the Video Privacy Protection Act for Videos and the Need for Updated, Legislation*, 37 LOY. L.A. ENT. L. REV. 237, 263 (2016-17); *see* Wendy Beylik, Comment, *Enjoying Your "Free" App? The First Circuit's Approach to an Outdated Law in* Yershov v. Gannet Satellite Information Network, Inc., 58 B.C. L. REV. E-SUPP. 60, 62, 68-72 (2017).

[157] Ani Gevorkian, *U.S. Supreme Court Denies Cert in Video Privacy Protection Act Case*, NAT'L L. REV. (Jan. 10, 2017), https://www.natlawreview.com/article/us-supreme-court-denies-cert-video-privacy-protection-act-case.

[158] *In re Hulu I*, No. C 11-03764 LB, 2012 WL 3282960, at *1-2 (N.D. Cal. Aug. 10, 2012) (listing the third parties).

[159] *Id.*

[160] *See* Kathryn Elizabeth McCabe, *Just You and Me and Netflix Makes Three: Implications for Allowing "Frictionless Sharing" of Personally Identifiable Information Under the Video Privacy Protection Act*, 20 J. INTELL. PROP. L. 413, 430 (2013) (identifying Hulu as impacting the applicability of the VPPA to digital streaming services).

community, including Facebook, Google, and DoubleClick.[161] Ultimately, the court dismissed all of the VPPA claims against Hulu except for the disclosures to Facebook via its "Like" button, which was included on each page of Hulu's website with video content.[162] However, before the court addressed Hulu's interaction with Facebook,[163] Hulu moved to dismiss the VPPA claims on ground that the plaintiffs lacked standing and failed to state a claim.[164] The court denied this motion.[165]

In denying the motion to dismiss for failure to state a claim, the court provided elaboration about the elements of a claim under the VPPA. In this ruling, the court failed to recognize the limits of its own understanding of technology.[166] As a result, the opinion in *Hulu* did not recognize the significance of programming code used for social plugins in that the code used to implement the Facebook Like social plugin on Hulu's website indicates how Hulu intended its users' viewing history data to be used by Facebook.[167] The court's ruling on the motion to dismiss has been credited with modernizing the VPPA because it clarified the meaning of various statutory terms.[168] In reality, the reasoning in the ruling has only made asserting a VPPA claim unduly difficult because it created unclear guidelines for identifying evidence sufficient to meet the knowledge requirement.[169]

---

[161] *See In re Hulu I*, 2012 WL 3282960, at *1-2; *These Companies are the World's Heavyweights in Media Advertising Revenues*, MARKETING CHARTS (May 5, 2017), https://www.marketingcharts.com/industries/media-and-entertainment-76947.

[162] *In re Hulu II*, No. C 11–03764 LB, 2014 WL 1724344, at *5, *17 (N.D. Cal. Apr. 28, 2014).

[163] *In re Hulu III*, 86 F. Supp. 3d 1090, 1091 (N.D. Cal. 2015) (holding Hulu did not know Facebook might combine data identifying Hulu users with separate information specifying which video that user was watching).

[164] *In re Hulu I*, 2012 WL 3282960, at *1.

[165] *Id.*

[166] *See generally* Leonid Rozenblit & Frank Keil, *The Misunderstood Limits of Folk Science: An Illusion of Explanatory Depth*, 26 COGNITIVE SCI. 521, 523 (2002) (explaining how an individual's general understanding of how a device functions can lead them to falsely assume they hold a more in-depth knowledge about the device's operation than they actually do).

[167] *See In re Hulu III*, 86 F. Supp. 3d at 1102-04 (explaining that evidence of Hulu's internal emails about data sharing and Hulu's transmission of cookies via the Like button was too general to determine what information was sent to Facebook and combined).

[168] *See* King, *supra* note 52, at 138-40 (discussing how *Hulu* provided guidance on how to plead a VPPA claim); McCabe, *supra* note 160, at 430-31 (identifying *Hulu* as impacting the applicability of the VPPA to digital streaming services).

[169] The court failed to grant adequate weight to circumstantial evidence as proof of Hulu's knowledge. *Compare In re Hulu II*, No. C 11–03764 LB, 2014 WL 1724344, at

This failure to understand the implications of the use of programming code might be explained by what is known as the Illusion of Explanatory Depth ("IOED").[170] Professors Leonid Rozenblit and Frank Keil, who developed the theory, conducted studies in which participants were asked to rate their understanding of how devices worked (e.g., how a can opener works).[171] Later, they were asked to write a "step-by-step causal explanation" of how each worked and to then rerate their understanding of the items.[172] The results showed a decrease in self-rated understanding after being asked to provide a real explanation.[173] Thus, IOED occurs when people feel they understand complex phenomena with far greater precision, coherence, and depth than they really do.[174] This powerful but inaccurate feeling of knowing is most apparent in individuals' confidence in explaining how devices work, particularly when the device's operation is easy to visualize.[175]

The court's analytical framework appears to rely on a distinction between visible and non-visible aspects of technology as the basis for weighing evidence.[176] In other words, the court focused on whether data transmitted via the Like plugin yielded information equivalent to a list

*15 (N.D. Cal. Apr. 28, 2014) (recognizing that Facebook simultaneously received Hulu user information and the titles of videos watched but that that did not constitute disclosure unless Hulu knew such data would be read together), *and id.* at *11 (discussing how context could render a "unique anonymized id . . . not anonymous" and thus an actionable VPPA disclosure), *with In re Hulu III*, 86 F. Supp. 3d at 1102-04 (explaining that evidence of Hulu's internal emails and use of source code was at best circumstantial proof of Hulu's knowledge for purposes of the VPPA claim), *and* Daniel L. Macioce, Jr., *PII In Context: Video Privacy and a Factor-Based Test for Assessing Personal Information*, 45 PEPP. L. REV. 331, 367 (2018) (arguing that *Hulu* has been misinterpreted as prohibiting contextual evidence to show PII has been disclosed to a third party).

170 *See* ANDREW S. ZEVENEY & JESSECAE K. MARSH, THE ILLUSION OF EXPLANATORY DEPTH IN A MISUNDERSTOOD FIELD: THE IOED IN MENTAL DISORDERS 1020 (2016), https://mindmodeling.org/cogsci2016/papers/0185/paper0185.pdf.

171 Rozenblit & Keil, *supra* note 166, at 526-27, 559-60.

172 *Id.*

173 *See id.* at 529-32.

174 *See id.* at 521.

175 *See id.* at 554 (discussing high levels of overconfidence with devices and natural phenomena based on the ratio of visible to hidden parts).

176 *See In re Hulu II*, No. C 11–03764 LB, 2014 WL 1724344, at *14 (N.D. Cal. Apr. 28, 2014) (explaining that the "disclosure of information on traffic tickets in public view or *providing a list of videos is different than transmission of cookies tied to a watch page*") (emphasis added); *id.* at 522-23 (explaining how an individual may be overconfident in their ability to explain how a device works based on the ease with which they can visualize its working parts).

of videos.[177] However, the court failed to appreciate that the method used to transmit data is indicative of how a third party intends to use that information.[178] Because the act of transmission is not easily visualized, the court discounted Hulu's use of the Like plugin as evidence of knowledge under the VPPA.[179]

As an example of the court's technological analysis, at the motion to dismiss stage, Hulu argued it was not a video service provider under the VPPA.[180] Accordingly, Hulu asserted that the statute only regulates businesses that sell or rent actual video tapes and not businesses that transmit digital content over the internet.[181] The court conceded that ordinarily the mechanism of delivery would not be a consideration in protecting the confidentiality of video viewing preferences.[182] Instead, the court asserted that such a privacy statute would focus solely on the video content and not how the content was delivered.[183] This demonstrates that the court was predisposed to assigning greater weight to evidence that bore a resemblance to actual video materials (visible) compared to evidence offered to explain the transmission of data (non-visible).[184] The court's partiality to evidence that bore a resemblance to

177 *See In re Hulu II*, 2014 WL 1724344, at *14 (explaining that the transmission of data results in an actionable VPPA disclosure only when the recipient can read the data such that it is the equivalent a "list of videos").

178 *See id.* Had the court considered code to be a purposeful set of instructions meant to convey information in an intelligible way, it would have deemed the use of social plugins as evidence sufficient to meet the knowledge requirement. *See Implementation*, FACEBOOK FOR DEVELOPERS, https://developers.facebook.com/docs/facebook-pixel/implementation (last visited Jan. 4, 2019) (discussing how downloading Facebook JavaScript code enables Facebook combine cookies such as match website visitors to their respective Facebook User accounts); *Like Button for the Web*, FACEBOOK FOR DEVELOPERS, https://developers.facebook.com/docs/plugins/like-button#configurator (last visited Jan. 4, 2019) (instructing web developers on how to "copy and paste" Facebook code to include the "Like button" on their website). *See generally* Paul Ford, *What is Code?* BLOOMBERG (June 11, 2015) https://www.bloomberg.com/graphics/2015-paul-ford-what-is-code.

179 *See infra* notes 190–198 and accompanying text (discussing how code, as the pathway upon which information such as cookies is transferred, is given less evidentiary weight because it lacks salient mental representation).

180 *In re Hulu I*, No. C 11-03764 LB, 2012 WL 3282960, at *4 (N.D. Cal. Aug. 10, 2012).

181 *Id.*

182 *Id.* at *5 ("To this reader, a plain reading of a statute that covers videotapes and 'similar audio visual materials' is about the video content, not about how that content was delivered (e.g. via the Internet or a bricks-and-mortar store).").

183 *Id.* at *5-6.

184 *See* Rozenblit & Keil, *supra* note 166, at 554 (explaining that a critical factor behind the IOED is the ratio of visible to hidden parts). The court's focus on the contents being transmitted versus the means of transmission is evident in its

actual video materials is consistent with Rozenblit and Keil's contention that an individual's confidence in explaining how devices work is greater when the device's operation is easy to visualize. Specifically, Rozenblit and Keil described such overconfidence through the following example:

> When you imagine a can-opener cutting through the lid of a can, that mentally animated image feels a lot more like perception than like propositional reasoning or informal inference. Thus, it would be easy to assume that you can derive the same kind of representational support from the mental movie that you could from observing a real phenomenon. Of course, the mental movie is much more like Hollywood than it is like real life — it fails to respect reality constraints. When we try to lean on the seductively glossy surface we find the façades of our mental films are hollow card-board.[185]

The court was thus apparently influenced by its familiarity with VHS as a format and physical object, making it less complicated to equate with digital content.

The court acknowledged that the full statutory language of the VPPA covers the delivery of video cassette tapes or similar audio visual materials.[186] However, it defined the phrase "audio visual materials" as "text or images in printed or electronic form," referring to a dictionary definition and vague legislative history.[187] Such statutory interpretation was proper,[188] but it illustrates the court's preference for evidence that provides a visual representation of a video cassette tape.[189] For example, the court referred to the dictionary definition of "material" as opposed

explanation of what a triable claim under the VPPA looks like in the digital realm. *See In re Hulu III*, 86 F. Supp. 3d 1090, 1096-97 (N.D. Cal. 2015) (analogizing the transmission of data to "an encrypted list of video rentals" and that there must be proof that the recipient can read the "encrypted list" to yield a VPPA-actionable "disclosure").

185 Rozenblit & Keil, *supra* note 166, at 554-55.

186 18 U.S.C. § 2710(a) (2019) ("[T]he term 'video tape service provider' means any person, engaged in the business . . . of rental, sale, or *delivery* of prerecorded video cassette tapes or similar audio visual materials.") (emphasis added); *In re Hulu I*, 2012 WL 3282960, at *5.

187 *See In re Hulu I*, 2012 WL 3282960, at *5 (referring to the Oxford dictionary's definition of "material" as "text or images printed in electronic form" and that it comports with the court's ordinary sense of the definition of "audio visual materials"); *id.* at *6 (discussing that the statutory phrase "similar audio video materials" suggests Congress's intent to cover emerging technologies).

188 *See id.* at *5 (explaining statutory interpretation and the use of legislative history when statutory language is ambiguous).

189 *See infra* notes 190–195 and accompanying text.

to the plural "materials" used in the VPPA.[190] It did so because the plural form, defined as "equipment necessary for a particular activity," did not bring to mind the video content's form.[191] The court reasoned that the notion of "audio visual materials" as "equipment" necessary for watching a movie is more akin to a viewing process than tangible video content.[192] Thus, it is unlikely to invoke representational support for the mentally animated image of a video cassette tape because the mechanics of streaming digital content do not depict the sale or rental of actual video tapes at a brick and mortar store as originally conceived under the VPPA.[193] For that reason, the court asserted that its accepted definition of "material"[194] comported with an ordinary definition of "audio visual materials."[195] Consequently, the court's "ordinary" sensibilities[196] narrowed relevant technological evidence to that which yielded intelligible information[197] without concern for the process of transmission.[198]

As a result, the court neglected to include in its ruling any discussion of how delivery of video content in the digital context might be covered

[190] *In re Hulu I*, 2012 WL 3282960, at *5; *see* Rozenblit & Keil, *supra* note 166, at 554 (explaining that the ease with which a device can be visualized may influence one's confidence in explaining how it works).

[191] *See In re Hulu I*, 2012 WL 3282960, at *5 (explaining that "a plain reading of a statute that covers videotapes and 'similar audio visual materials' is about the video content, not about how that content was delivered" and that the dictionary definition of "material" aligns with that understanding).

[192] *See id.* (explaining the concept of "audio visual materials" as "the online streaming mechanism" to deliver video content). *Equipment*, DICTIONARY.COM, https://www.dictionary.com/browse/equipment (last updated 2012) (defining the term equipment as "(1) anything kept, furnished, or provided for a specific purpose, (2) the act of equipping a person or thing, (3) the state of being equipped"); Rozenblit & Keil, *supra* note 166, at 538 ("Causally complex systems, on the average, may also have more perceptually salient components than *procedures* . . . .") (emphasis added).

[193] *See In re Hulu III*, 86 F. Supp. 3d 1090, 1096 (N.D. Cal. 2015) (describing an actionable claim under the VPPA by way of a hypothetical scenario involving a video-store clerk); *In re Hulu I*, 2012 WL 3282960, at *5 (explaining the court's preference for the dictionary definition of "material" because it comports with the court's ordinary sense of the definition of "audio visual materials"); Rozenblit & Keil, *supra* note 166, at 557 (describing how people have a drive for coherence that can create a bias for certain features of an object or process in which they may confuse that sense of coherence with a more detailed understanding of a causal chain than they actually possess).

[194] *See In re Hulu I*, 2012 WL 3282960, at *5.

[195] *Id*; *see* Rozenblit & Keil, *supra* note 166, at 538.

[196] *See* Rozenblit & Keil, *supra* note 166, at 538 (indicating that explanations about how a device works can be misleading based on an understanding of *what* something does versus *how* it does it).

[197] *See infra* notes 233–40.

[198] *See supra* notes 167; *infra* notes 200–201 and accompanying text.

by the VPPA in light of the technological processes involved in its transmission.[199] Instead, the court reasoned that digital distribution was covered because of general consumer privacy policy concerns in the statute's legislative history.[200] Namely, the court made the broad assertion that evolving media formats in electronic form are to be protected by the VPPA without considering the technical aspects of how streaming services transmit data to third parties might impact the legal analysis of a VPPA claim.[201]

Taken as a whole, this analysis suggests that the court was only comfortable taking one inferential step in assessing a digital VPPA claim.[202] That is, digital content is equivalent to a list of video cassette tapes purchased or rented.[203] In effect, the court focused its analysis on what it called "analogies in a paper world" in which, for example, a video service provider would violate the VPPA by throwing away a video watch list in a recycle bin so long as it knew third parties would later retrieve it for their own use.[204] The court likely did so because streaming videos are the discrete, easy-to-imagine parts of online streaming services.[205] The ease of visualizing streaming videos as a list of video cassette tapes provided a way to characterize a digital disclosure.[206]

---

[199] *See In re Hulu I*, 2012 WL 3282960, at *6 (addressing the question of whether video distribution via digital streaming is suitable for a VPPA claim by referring to "Congress's concern with protecting consumers' privacy in an evolving technological world," rather than analyzing the technological processes of digital content distribution).

[200] *Id.*

[201] *See id.*

[202] *See supra* notes 176–198 (discussing the court's assignment of evidentiary weight to actual video materials (visible) compared to evidence offered to explain the transmission of data (non-visible)).

[203] *In re Hulu II*, No. C 11-03764 LB, 2014 WL 1724344, at *14 (N.D. Cal. Apr. 28, 2014) (equating the transmission to Facebook of Hulu video viewing histories and Facebook user cookies as a disclosure in violation under the VPPA with throwing Judge Bork's video watch list in the recycle bin knowing that the Washington Post searches your bin every evening for intelligence about local luminaries might be).

[204] *Id.*

[205] *See In re Hulu I*, 2012 WL 3282960, at *5 (explaining the court's preference for the dictionary definition of "material" because it is analogous to video content); Rozenblit & Keil, *supra* note 166, at 523, 554 (describing how components of a mechanical device that are easy to visualize and mentally animate, may cause a false sense of knowing the details of how the components interact such that one may be inclined to attribute deep causal knowledge of a system to oneself).

[206] Transmitting digital content is akin to a list of video cassette tapes that a consumer has rented. *See In re Hulu III*, 86 F. Supp. 3d 1090, 1096-97 (N.D. Cal. 2015) (explaining that the transmission of code requires proof of a mutual understanding

Unfortunately, the analysis of this approach was essentially limited to the typical scenario that prompted the VPPA (i.e., the disclosure of a list of videos that a consumer has watched to a third party).[207] The court thus did not address how the transmission of digital content factors into an actionable VPPA disclosure.[208] Evidently confused by an internal process that is difficult to mentally animate,[209] the court did not appreciate how the transmission of digital content is significant to the act of disclosure.[210] As a result, the court established an analytical framework for a VPPA claim that focuses on whether data transmission results in a "tangible disclosure."[211] The court explained that such a tangible disclosure occurs when "the connection between a specific user and the material that he 'requested or obtained' is obvious. If [an individual] were to hand [a third party] a slip of paper with John Doe's name above a list of recently rented videotapes, the connection between the two will generally be apparent."[212] Under that framework, a transmission of data must trigger a mental image analogous to the classic video store clerk-customer exchange in order to fall within the scope of the VPPA.[213]

For purposes of the knowledge requirement, the court's visual approach to analyzing a VPPA claim is reflected in its explanation of

between the sender and recipient that there has been a disclosure of a person's video viewing history because numerical data is not as intelligible as natural language).

[207] *Id.* at 1096 ("The paradigmatic case, the case that prompted the VPPA, involved a video store's giving a Washington Post reporter *a list of the videos* that Circuit Judge Robert Bork had rented.") (emphasis added).

[208] The court's "throwing it in the bin" analogy pinpoints the major flaw in its analysis of the knowledge requirement. *See In re Hulu II*, 2014 WL 1724344, at *14. The act of throwing away a customer's video list knowing someone searches the trash bin is the purpose behind using social plugins to transmit data. Had the court given proper consideration to the use of code, *see infra* notes 248–253, then it may have recognized that Hulu's use of the Like button fits its analogy. *See In re Hulu II*, 2014 WL 1724344, at *14.

[209] *See* Rozenblit & Keil, *supra* note 166, at 524-25, 554-54 (explaining how an individual's overconfidence about how something works is based on the ease with which they visualize the object and its functional parts).

[210] *See infra* notes 223–240.

[211] *See In re Hulu III*, 86 F. Supp. 3d 1090, 1096 (N.D. Cal. 2015); Rozenblit & Keil, *supra* note 166, at 554; *see infra* notes 268–275 and accompanying text.

[212] *In re Hulu III*, 86 F. Supp. 3d at 1096.

[213] *See id.* (explaining that the connection between a specific online user and the video content requested is apparent when it is equivalent to a video store clerk handing a piece of paper with a customer's video rental list to a third party); Rozenblit & Keil, *supra* note 166, at 521-62 (explaining that objects that are easy to mentally animate trigger an illusion of understanding); *see infra* notes 268–275 and accompanying text.

source code as a language.[214] To this end, the court identified code as the cookie information that was transmitted and the act of transmission itself.[215] Because the court recognized code, in both forms, as a series of characters (e.g., the string of letters and numbers which constitute the Facebook User ID and the JavaScript code on Hulu's website sending cookies to third parties),[216] the visual cue prompted an analysis to determine which type of code warranted greater evidentiary weight.[217] Specifically, the court observed that because Hulu wrote the code that transmitted identifying information without user permission, a VPPA violation might exist if it could be shown that Hulu and Facebook negotiated the exchange of cookies so that Facebook could track information (including watched videos) about its users on Hulu's platform when the Like button loaded, or if Hulu knew that it was transmitting Facebook ID cookies and video watch pages.[218]

First, the court described code as "a garbled collection of alphanumeric strings,"[219] that must be decrypted for it to have any evidentiary value in an actionable disclosure.[220] This interpretation focused on cookie information as code and considered whether Hulu and Facebook *both recognized* that they were using mutually intelligible code such that it would amount to a "list" of a user's video rental

---

[214] *See In re Hulu II*, 2014 WL 1724344, at *14.

[215] *Compare In re Hulu III*, 86 F. Supp. 3d at 1100 (discussing how the only proof of how Hulu implemented the Facebook Like button feature lies in Hulu's source code) *and In re Hulu II*, 2014 WL 1724344 at *16 (discussing how email evidence suggests that Hulu knew that using beacon technology to disclose user data could result in identification of actual users, and it recognized the VPPA implications), *with In re Hulu III*, 86 F. Supp. 3d at 1097 (explaining that an actionable VPPA claim requires proof that a third party knows that a website has used a code and they have the capacity to decode and read the contents) *and In re Hulu II*, 2014 WL 1724344 at *14 ("Code is a language, and languages contain names, and the string is the Facebook user name."). *See* Ford, *supra* note 178 (discussing how data comes from everywhere and that code serves as a set of instructions to manage the data).

[216] *See In re Hulu II*, 2014 WL 1724344, at *14 (describing the Facebook User ID as a string of numbers and letters that personally identifies a Facebook user); *id.* at *14-15 (describing JavaScript code on Hulu's website that that transfers information through cookies to third parties).

[217] *See id.* at *14 (explaining that a "Facebook User ID is more than a unique, anonymous identifier" but that the transmission of cookies requires proof that Hulu knew Facebook would combine video titles and Facebook user IDs "in a manner akin to the disclosure of Judge Bork's videos").

[218] *Id.* at *55-56.

[219] *In re Hulu III*, 86 F. Supp. 3d at 1096.

[220] *Id.* at 1096-97 ("For a disclosure to arise . . . there generally must be proof of further action by the recipient; they must know that I have used a code and they must at least have the capacity to decode and read the contents.").

history, not an encrypted video rental history.[221] Second, the court asserted that code acts as the pathway upon which information such as cookies are transferred between parties on the internet, indicating the act of transmission.[222]

With regard to code as the act of transmission, the court utilized the word "execute" to describe code as an automated mechanism.[223] The court observed that when a user's browser visited Hulu's website, it *executed* code in which the browser sent a request to Facebook to load the Like button on the webpage.[224] In effect, the court likened code to an internet user's browser pushing an automated mathematical button.[225] While code appears to be an arbitrary set of symbols generated by a computer, in reality, a programmer has translated human language into a numerical sequence in order to execute certain operations to certain degrees of precision, otherwise known as an algorithm.[226]

Thus, the court's understanding of code is erroneous because it does not grant sufficient evidentiary weight to code as the means of transmission. Specifically, the court observed that Hulu user data was transmitted "automatically using Hulu's code to load the Facebook Like button,"[227] but then questioned whether such data sharing amounted to a negotiated exchange between Hulu and Facebook.[228] This uncertainty about whether Hulu's use of code to transmit user data without their permission was sufficient to show an agreed-upon exchange between

---

[221] *See id.* at 1096 (noting that it would be a violation of the VPPA to pass someone an encrypted list of a user's video rentals if the recipient and video service provider both understood that they were using a mutually intelligible code).

[222] *See In re Hulu II*, 2014 WL 1724344 at *13-16 ("Hulu sent code *and* information to load the Facebook Like button . . . . Hulu wrote and installed the code that integrated the Like button on the watch pages, and it transmitted the Facebook ID cookies when it sent the request to Facebook to load the Like button.") (emphasis added).

[223] *In re Hulu III*, 86 F. Supp. 3d at 1093-94 ("When the user's browser *executed* this code, the browser sent the request to Facebook to load the Like button on the watch page . . . . Hulu did not send Facebook the Hulu User ID or the Hulu user's name when the user's browser *executed* the code to load the Like button.") (emphasis added).

[224] *Id.*

[225] *See In re Hulu II*, 2014 WL 1724344 at *16-17 (describing code as the act of transmission as a "*request* [sent] to Facebook to load the Like button") (emphasis added); *see also* Ford, *supra* note 178.

[226] Ford, *supra* note 178.

[227] *In re Hulu II*, 2014 WL 1724344 at *13.

[228] *See id.* at *16 (explaining that loading the Like button was an automated mechanism for transferring certain data points without the user's permission but that it only *might* be evidence of an agreement to share user identifying data between Hulu and Facebook) (emphasis added).

Hulu and Facebook demonstrates the lack of evidentiary weight given to the Like button because a website's use of code indicates how it intends data to be managed and shared.[229] Moreover, though the court acknowledged there were "fact issues about Hulu's knowledge,"[230] it also stated that denying Hulu's motion for summary judgment was in part to allow for the completion of discovery involving source code.[231] This further demonstrates that the court underestimated the evidentiary weight of code as the act of transmission because it implicitly suggests that the court did not consider Hulu's use of the Like button by itself to be sufficient evidence of a negotiated exchange of data between Hulu and Facebook.[232] At most, the court regarded Hulu's transmission of user data as evidence of the "purposefulness" behind utilizing social plugins for sharing data with third parties but not sufficient to show Hulu had knowledge that it was transmitting both an identifier and the person's video watching information.[233]

To borrow the court's approach of using a dictionary in its legal analysis,[234] the term "execute" has both a legal and technological definition.[235] Under the legal definition, "execute" means "to transact or carry through (a contract, mortgage, etc.) in the manner prescribed by law."[236] By comparison, the technological meaning of "execute" is "to run (a program or routine) or to carry out (an instruction in a program)."[237] In view of that, the court utilized the legal definition of the term "execute" to focus on whether the information amounted to a

[229] *See* Ford, *supra* note 178 (explaining that code as the act of transmission "is the most important signaling behavior that a technology company can engage in" because the programming language used to write the code is indicative of how data is intended to be managed and shared); *About Facebook Pixel*, *supra* note 111 ("When you set up the Facebook pixel, we will start to receive information from your website. This information allows us to better target your ads and optimize your ads for conversions.").

[230] *In re Hulu II*, 2014 WL 1724344 at *16.

[231] *Id.* at *17.

[232] *Id.* at *16 (surmising that there might be a VPPA violation "[i]f Hulu and Facebook negotiated the exchange of cookies").

[233] *Id.* at *16 (recognizing that the transmission of cookies to load the Like button was intentional); *id.* at *1 (holding there was insufficient evidence to determine as a matter of law whether Hulu knowingly disclosed data in violation of the VPPA).

[234] *See supra* notes 186–195 and accompanying text (discussing how the court used the Oxford dictionary's definition of "material" as "text or images printed in electronic form" because it followed the court's ordinary sense of the definition of "audio visual materials").

[235] *Execute*, DICTIONARY.COM, https://www.dictionary.com/browse/execute (last updated 2013).

[236] *Id.*

[237] *See id.*

video list (a transaction) that could be read by a third party after transmission.[238] This detracted from considering the act of transmission itself because it focused on whether the cookies yielded PII after transmission to Facebook without proper regard for the act of transmission as an indicator of whether that combination is likely to occur at all.[239] Further consideration of whether the act of transmission (i.e., social plugins on a website) influences the likelihood that cookies are combined by a third party to produce PII for purposes of a triable VPPA claim would have shown that Hulu and Facebook negotiated the exchange of cookies so that Facebook could track information (including watched videos) about its users on Hulu's platform when the Like button loaded.

Thus, the court essentially reduced code to a device within a computer rather than an affirmative act aimed at solving a problem.[240] The "problem" refers to the particular activity that a programmer seeks to accomplish with data being collected. In short, the way in which data is sought to be organized (i.e., "the problem") is reflected by the specific code language employed.[241] Another name for code as an affirmative act is software.[242] Software selection indicates how an individual wants to

[238] *See In re Hulu II*, No. C 11-03764 LB, 2014 WL 1724344, at *36 (N.D. Cal. Apr. 28, 2014) (explaining that a VPPA claim "require[s] the identification of a specific person tied to a specific *transaction*" with a video tape service provider) (emphasis added); *see also id.* at *50 ("The court's view is that if Hulu never knew that Facebook *might* read the videos and the Facebook ID cookies together in a manner akin to the disclosure of Judge Bork's videos, then there is not a VPPA violation.") (emphasis added) (internal quotations omitted).

[239] *See In re Hulu III*, 86 F. Supp. 3d 1090, 1104 (N.D. Cal. 2015) (stating that internal emails at Hulu describing the privacy implications of data sharing with third parties via beacon technology are not circumstantial proof of what Hulu knew about its disclosures to Facebook).

[240] *See* Ford, *supra* note 178 (describing code as "an explicit list of instructions" for transmitting data as quickly and efficiently as possible depending on the task at hand given that "users do things (searches, status updates, tweets) an extraordinary number of times").

[241] *See, e.g.*, *id.* (explaining that Java is an object-oriented language that is like a physical filing cabinet because it provides "programmers a great way to name things [data]").

[242] *See Software*, TECHOPEDIA, https://www.techopedia.com/definition/4356/software [https://perma.cc/NB49-2F4W] ("Software, in its most general sense, is a set of instructions or programs instructing a computer to do specific tasks.") (last visited Nov. 1, 2019); *cf.* Marc Andreessen, *Why Software is Eating the World*, WALL ST. J. (Aug. 20, 2011), https://www.wsj.com/articles/SB10001424053111903480904576512250915629460 (discussing how software is transforming industries that are viewed as primarily existing in the physical world because of the ability to "do" things without new infrastructure and train new employees.

organize, manage, and share data.[243] Accordingly, the code language used to develop software for a website reflects an agenda as to how it intends to use its data.[244] Consequently, Hulu's use of the Like button reflects a willingness to exchange data for detailed analytics that achieve its specific business goals.[245] Moreover, Facebook's ability to deliver such reports was based on its promise to combine user data obtained from its social plugins on third party websites.[246] Given software's role as an executor of a business agenda, the court neglected how code is often utilized to achieve the business goal of efficient data management.[247]

In sum, the court's visual system, distinguishing between visible and non-visible aspects of technology for purposes of evaluating technology-related evidence, focused on what the outcome of the disclosure looked like rather than how the contents were transmitted.[248] In order to fall within the scope of the VPPA, the court's system of evaluation required that the transmission of data (cookies as code) via the Facebook Like button trigger a mental image analogous to the classic video store clerk-customer exchange such that third party receives a "list" of a customer's video rental history, not an encrypted video rental history.[249] While the question of which cookies are disclosed is important for determining the existence of PII,[250] the means

[243] *See* Ford, *supra* note 178 ("Code is inert. How do you make it ert? You run software that transforms it into machine language . . . . A language is software for making software . . . . Languages have agendas . . . . Data management is the problem that programming is supposed to solve . . . . That's how we ended up with 'big data.'").

[244] *See id.*

[245] *See, e.g.*, *About Facebook Pixel*, *supra* note 111 (explaining that Facebook Pixel allows a company to see what actions its customers take on its website in order to reach those customers again through future Facebook ads); *see also Specifications for Facebook Pixel Standard Events*, FACEBOOK, https://www.facebook.com/business/help/402791146561655 (last updated Aug. 27, 2019) (listing different customer actions a website can track).

[246] *See* Caroline McCarthy, *Facebook F8: One Graph to Rule Them All*, CNET (Apr. 21, 2010, 10:25 AM), https://www.cnet.com/news/facebook-f8-one-graph-to-rule-them-all (introducing the Like button at the company's F8 developer summit in 2010 as a way to gain more information faster about its individual users).

[247] *See In re Hulu III*, 86 F. Supp. 3d 1090, 1103 (N.D. Cal. 2015) (asserting that internal emails at Hulu addressing the business benefits of data analytics do not raise a genuine issue of material fact on the VPPA claims); Ford, *supra* note 178 (explaining that "data management is the problem that programming is supposed to solve" because user-created data such as tweets, emails, and Facebook posts necessitate a way for internet companies to organize and share these data points).

[248] *See supra* notes 188–200 and accompanying text.

[249] *See supra* notes 206–213 and accompanying text.

[250] *See supra* Part I.D.

by which they are transmitted is also significant.[251] Namely, the code language a website uses to transfer data indicates how it wants the information to be used.[252] Thus, the court's analysis falls short by failing to identify that the use of social plugins, by itself, is sufficient evidence of actual knowledge for purposes of the VPPA knowledge requirement.[253]

III. THE *HULU* COURT MISAPPLIED THE ECPA'S DEFINITION OF THE TERM "KNOWINGLY"

The Northern District of California dismissed all of the VPPA claims against Hulu except for the disclosures to Facebook.[254] Specifically, the court dismissed the VPPA claim against comScore, a metrics company that analyzed Hulu's viewing audience and provided reports that Hulu used to obtain media content and sell advertising, because there was a lack of evidence showing comScore combined "watch page" URL web addresses containing the video name and the Hulu users' seven-digit Hulu User ID to identify persons to the videos they watched.[255] By comparison, the court denied Hulu's motion for summary judgment for its disclosures to Facebook because there was a genuine dispute as to material issues of fact about whether the user data Hulu transmitted to Facebook via the Like button was a prohibited disclosure under the VPPA.[256] Consequently, Facebook's Like button was the only remaining issue.[257]

---

[251] *See supra* notes 234–240 and accompanying text and *infra* Part IV.

[252] *See supra* notes 242–247; *In re Hulu II*, No. C 11-03764 LB, 2014 WL 1724344, at *14-15 (N.D. Cal. Apr. 28, 2014) ("Hulu hosts its vendors' JavaScript code on Hulu's domain so that when Hulu's web pages execute the vendor code, a vendor such as comScore obtains information through cookies that are set by hulu.com."); Ford, supra note 175 (explaining that programming languages vary because of the way they "instruct the computer to process data"); *see, e.g.*, *You Never Learned to Code? Start Here.*, MASHABLE https://mashable.com/2015/12/05/learning-to-code/#rAXr3bnS8Sqd (last visited Jan. 4, 2019) [https://perma.cc/ZT3Y-BV6C].

[253] *See In re Hulu III*, 86 F. Supp. 3d 1090, 1100-01 (N.D. Cal. 2015) (stating that the code used in the act of transmission (i.e., the "show_faces" attribute of the Like button) did not provide evidence that Hulu must have known Facebook could identify Hulu users and their video viewing histories through the Like button). *But see In re Hulu II*, 2014 WL 1724344, at *53-55 (observing that internal emails at Hulu indicated that it knew that cookies with identifying information were sent and that third parties could use it with other data to build user profiles).

[254] *See In re Hulu II*, 2014 WL 1724344, at *17.

[255] *See id.* at *12, 17.

[256] *See id.* at *5.

[257] *See id.* at *17.

In *Hulu*, the court held that there was no genuine issue of material fact as to whether Hulu knew Facebook might combine data transmitted by Hulu in order to link users with the videos they watched.[258] Specifically, Hulu sent Facebook the user-identifying c_user cookie (the user's Facebook ID) and the watch-page URL via the Like button.[259] Hulu did so before the Hulu user did anything other than load the watch page that included the social plugin.[260] Such data was collected whether or not the user clicked on the Like button.[261] But the court ruled that Hulu did not know Facebook might connect these two pieces of information (c_user and URL) to construct PII.[262] In effect, the court ruled that allowing third parties to place plugins on a website does not constitute actual knowledge under the VPPA.[263] As its rationale, the court restated that the purpose of the VPPA is to ban the disclosure of information connecting a certain user to certain videos, not the disclosure of user or video data.[264] However, the distinction also hinted that the court was predisposed to regarding the "videotape-era"[265] statute as ineffective in the digital realm.[266] Without extrinsic proof of an agreement, the court doubted a VPPA claim would be actionable.[267]

[258] *In re Hulu III*, 86 F. Supp. 3d 1090, 1097-98 (N.D. Cal. 2015).

[259] *Id.* at 1093-94.

[260] *Id.* ("[W]hen a Hulu watch page loaded with the Facebook Like button, the page prompted a user's web browser to transmit the watch-page address and Facebook c_user cookie to Facebook-controlled servers.").

[261] *See* St. John, *supra* note 35 ("If you're logged into Facebook with the same browser you use to surf the web, the company knows exactly who you are and the vast majority of the websites you visit . . . [e]ven if you're not logged in, the company can still associate the data with your IP address and all the websites you've been to that contain Facebook code.").

[262] *See In re Hulu III*, 86 F. Supp. 3d at 1105.

[263] *Id.*

[264] *Id.* at 1095-96 ("[T]he connection—distances this Internet-streaming case from the situations for which the VPPA was enacted.").

[265] *See id.* at 1096.

[266] *See id.*

[267] The court's doubt was due to its failure to understand how a third party might otherwise be able to decode and read cookies. *See id.* at 1096 ("If extrinsic proof shows that the reporter and video provider had agreed to separate the disclosures in place and time, so that the clerk would hand over only the renter's name, while the video titles would arrive later by a third-party courier—but that both parties understood how the name and titles were related—that would supply the connection."); *id.* at 1097 ("There must be some mutual understanding that there has been a disclosure. Moving away from natural language, in other words—as we do in this case—requires the recipient to more actively participate to yield a VPPA-actionable 'disclosure.'"); see also *supra* notes 206–213 and accompanying text.

In particular, the court questioned the viability of an actionable VPPA claim based solely on the sharing of numerical data.[268] Consistent with this viewpoint, the court articulated a narrow view of PII.[269] It required three elements which included that the connection between a specific user and the material he "requested or obtained" be obvious.[270] The court repeatedly used the term "obvious" in reference to the connection element, to support the notion that disclosure of PII is immediate.[271] Requiring immediacy was the court's way of emphasizing that a disclosure of PII should allow the third party to read the information and instantly see the connection.[272] In doing so, the court formulated a definition of PII that attempted to reflect the classic video store clerk-customer exchange where there is a mutual understanding of disclosure.[273] But the court did not apply this logic fairly when it asserted that Hulu's digital disclosure was "different" because Hulu did not connect the data points — the user's identity and that of the video material — but instead transmitted them separately (albeit simultaneously).[274] Thus, this narrow interpretation of PII disregarded the commercial purpose behind social plugins from which one could reasonably infer Hulu knew Facebook would link information together to learn the video preferences of an identified Facebook user.[275]

Arguing semantics, as the court did through its analogical reasoning,[276] demonstrates its unfamiliarity with social plugin

[268] *See In re Hulu III*, 86 F. Supp. 3d 1090, 1096 (N.D. Cal. 2015) ("No one would deny that I would violate the VPPA by passing someone an encrypted list of Judge Bork's video rentals—if my recipient and I both understood that we would use a mutually intelligible code. If, instead, I hand someone only a garbled collection of alphanumeric strings (which I alone understand to contain someone's encrypted video-rental history), there is likely no actionable disclosure.").

[269] *See* Macioce, Jr., *supra* note 169 ("In In re Hulu II's wake, the majority of courts that have applied the VPPA in an Internet video context have found support in In re Hulu II for a narrow construction of the Statute's definition of PII.").

[270] *See In re Hulu III*, 86 F. Supp. 3d at 1095-96 (A triable VPPA claim requires that a video service provider "knowingly disclos[e]: 1) a consumer's identity; 2) the identity of 'specific video materials'; and 3) the fact that the person identified 'requested or obtained' that material.").

[271] *See id.* at 1096.

[272] *See id.*

[273] *See id.* at 1096-97.

[274] *Id.* at 1096.

[275] *See infra* Part IV.

[276] Courts have shown a tendency to analogize emerging technologies to older more familiar forms of technology when they lack understanding. *See In re Hulu III*, 86 F. Supp. 3d at 1096-97 (discussing the paradigmatic older case of disclosure of PII between a video store clerk and local reporter in comparison digital case of handing someone only a garbled collection of alphanumeric strings).

technology.[277] Moreover, the court's reasoning suggests a lack of interest in acquiring such knowledge.[278] This ignorance of technological processes has and will likely continue to result in inconsistent court decisions within the realm of digital information privacy.[279] It is thus doubtful that the court relied on the ECPA's definition of the term "knowingly" solely because the VPPA was modeled after at it,[280] but rather because ECPA case law addresses situations involving older, one might argue more familiar, technology (e.g., sending a fax).[281] Additionally, ECPA cases draw upon legislative history to clarify what

[277] *See* Brown v. Entm't Merchs. Ass'n, 564 U.S. 786, 806 (2011) (Alito, J., concurring) (cautioning courts from analogizing to "familiar" technology in understanding new technology); *Model Intellectual Privacy Statute*, *supra* note 29, at 1789 (explaining that "the weaknesses in the VPPA are mostly a matter of statutory interpretation, particularly a cramped judicial notion of what information is personally identifiable"); Beylik, *supra* note 156, at 74-75 (observing that cases involving emerging technology have led to unpredictable results because they rely on the court's familiarity with technology itself); Luke M. Milligan, *Analogy Breakers: A Reality Check on Emerging Technologies*, 80 MISS. L.J. 1319, 1322 (2011) (explaining that the role of analogical reasoning in judicial decisions in the criminal procedure context involving emerging technologies has led to mixed results because courts have struggled to analogize them to older technologies); *cf.* Susan Freiwald, *First Principles of Communication Privacy*, 2007 STAN. TECH. L. REV. 3, 12, 35 (2007) (asserting that courts will experience challenges in determining what electronic communications are subject to a reasonable expectation of privacy because courts extend precedents past the point the analogy supports such as telephone communications and email correspondences).

[278] *Cf.* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 859-79 (2004) [hereinafter *Constitutional Myths*] (explaining that in many cases courts do not understand the technical facts or general technological context such that they perform guess work by establishing rules that may or may not do what the courts think they will do); Daniel J. Solove*, Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 772 (2005) ("Kerr is right that there are many times when judges are lazy and do not acquire a good understanding [of technology].").

[279] *See* Freiwald, *supra* note 277, at 8; Kerr, *Constitutional Myths*, *supra* note 278, at 859-79; Solove, *supra* note 278, at 772.

[280] *In re Hulu III*, 86 F. Supp. 3d at 1095 (stating the VPPA was modeled after the ECPA); *See* S. REP. NO. 100-599, at 3-4 (1988) (describing the ECPA as "the most advanced privacy legislation passed by the Congress" responding "to important issues concerning the use of new information, communication and computer technologies").

[281] *See, e.g.*, Freedman v. America Online, Inc., 329 F. Supp. 2d 745, 749 (E.D. Va. 2004) (holding an AOL employee knowingly disclosed the plaintiff's subscriber information when she *faxed* it the subscriber information to police) (emphasis added); Worix v. MedAssets, Inc., 857 F. Supp. 2d 699, 703 (N.D. Ill. 2012) (holding that a health care provider did not knowingly disclose patient information after a hard drive was stolen because failure to safeguard data is risky but "does not make its receipt by a third party virtually certain, unlike sending a fax, which is what occurred in Freedman").

a plaintiff must show to prove an actionable disclosure,[282] which the court utilized in formulating its knowledge requirement.[283] In sum, the court avoided the issue of actual knowledge as it pertains to data sharing because of an apparent unwillingness to recognize that the use of social plugins is extrinsic proof an agreement between the video service provider and third party.[284] It likely did so in order to maintain an established triable VPPA claim that would mirror the traditional type of situation it was originally intended to confront.[285] Consequently, the definition for the "knowingly" element in the VPPA was taken from the Stored Communications Act ("SCA"), an outdated and notoriously complex statute, better known as Title II of the ECPA.[286]

The SCA[287] was enacted as part of the ECPA in 1986.[288] The legislative purpose behind the SCA was to protect the privacy and security of communications transmitted by new computer technology.[289] Specifically, the statute prohibits a person or entity providing an electronic communication service to the public, such as an email service provider, [290] from knowingly divulging the contents of a communication while in electronic storage by that service.[291] This

[282] *See, e.g.*, *Freedman*, 329 F. Supp. 2d at 748 (E.D. Va. 2004) (describing a three-prong test to satisfy section 2702(a)(3)'s state of mind requirement); *Worix*, 857 F. Supp. 2d at 702 (N.D. Ill. 2012) (stating "knowing conduct includes willful blindness, but not recklessness or negligence").

[283] *In re Hulu III*, 86 F. Supp. 3d at 1095 (citing Freedman and Worix as ECPA cases providing the basis for its definition of knowingly).

[284] *See* supra notes 237–38, 263–64, 272. *Cf.* Jill Priluck, *How Courts Avoid Ruling on Issues of Privacy*, SLATE (Apr. 11, 2017, 5:58 PM), http://www.slate.com/articles/technology/future_tense/2017/04/how_courts_avoid_ruling_on_issues_of_technology_and_privacy.html; Michael Brick, *When the Judge Can't Really Judge*, N.Y. TIMES (Sept. 11, 2000), https://www.nytimes.com/2000/09/11/business/technology-when-the-judge-can-t-really-judge.html.

[285] *See In re Hulu III*, 86 F. Supp. 3d at 1096-98 (discussing how a VPPA claim based on information passed between humans in natural language is different to try compared to VPPA plaintiff's burden in an Internet-video case).

[286] *Cf.* Solove, *supra* note 278, at 773 (explaining how "many judicial misunderstandings stem from courts trying to fit new technologies into old statutory regimes built around old technologies . . .").

[287] 18 U.S.C. § 2701 (2019).

[288] *See Electronic Communications Privacy Act of 1986 (ECPA)*, U.S. DEP'T OF JUSTICE: JUSTICE INFO. SHARING, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 (last updated Apr. 23, 2019); S. REP. NO. 99-541, at 35 (1986).

[289] S. Rep., *supra* note 285, at 5.

[290] Jeffrey Paul DeSousa, Note, *Self-Storage Units and Cloud Computing: Conceptual and Practical Problems with the Stored Communications Act and Its Bar on ISP Disclosures to Private Litigants*, 102 GEO. L.J. 247, 250 (2013).

[291] 18 U.S.C. § 2702(a)(1) (2019).

language has confused the courts since its passage.[292] Notwithstanding the SCA's infamous reputation for its lack of clarity,[293] the court in *Hulu* relied on an SCA case, *Freedman v. America Online, Inc.*, in fashioning its definition of "knowingly."[294] *Freedman* stated that the knowledge requirement for the ECPA requires proof that the defendant knew all the factual circumstances that constitute the alleged offense.[295]

The court in *Hulu* implemented *Freedman* into its three element test for PII.[296] Specifically, the court established its definition of knowingly within its third element involving the necessary *connection* between a specific user and the video material "requested or obtained."[297] Thus, if a defendant knew that a third party would combine user identifying information with a video title, that would be equivalent to an awareness of all the factual circumstances constituting the alleged offense.[298] Accordingly, the court found that the plaintiffs offered no proof that Hulu knew Facebook might combine information to yield PII under the VPPA.[299] Furthermore, the court emphasized that proof of conduct sufficient to support the knowledge requirement cannot be supported by general assertions about how personal information moves around in the age of the internet.[300] However, a circuit split arose in 2017 regarding the term "knowingly" under the ECPA which addresses what type of conduct constitutes a violation.[301] The Sixth Circuit held that a defendant must know they are violating the statute.[302] By comparison, the Fifth Circuit stated specific intent is not required to violate the statute.[303]

---

[292] *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, And a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 (2004) [hereinafter *A User's Guide*]; Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law* 54 HASTINGS L.J. 805, 820-21 (2003) [hereinafter *Lifting the Fog*] (discussing how the federal circuit courts of appeal have struggled consider the SCA to be a confusing and uncertain area of the law).

[293] *See* Kerr, *Lifting the Fog*, *supra* note 292, at 820-21.

[294] *See In re Hulu III*, 86 F. Supp. 3d 1090, 1095 (N.D. Cal. 2015).

[295] Freedman v. Am. Online, Inc., 329 F. Supp. 2d 745, 747 (E.D. Va. 2004).

[296] *In re Hulu III*, 86 F. Supp. 3d at 1095.

[297] *Id.* at 1095-96 ("[A]n actionable VPPA violation [requires that] the video provider . . . knowingly disclose[]: 1) a consumer's identity; 2) the identity of 'specific video materials'; and 3) the fact that the person identified 'requested or obtained' that material.").

[298] *See id.*

[299] *Id.* at 1098-99.

[300] *See id.* at 1101.

[301] *See* Alexander v. Verizon Wireless Servs., LLC, 875 F.3d 243, 255 (5th Cir. 2017).

[302] *See id.*

[303] *See id.*

The circuit split serves as an example of the obfuscation of the ECPA's statutory language that is consistent with potential judicial misunderstanding of the ECPA as a whole.[304] In spite of that, the court in *Hulu* correctly recognized that a defendant's conduct plays a central role in determining whether she was aware of all the factual circumstances constituting a VPPA claim.[305] However, the court underestimated how the technological aspects of Hulu's conduct affected its knowledge about what Facebook might do with the data involved,[306] despite the fact that social plugins transmit data that identifies individuals with the website visited.[307] And social plugins, as a business practice, provide strong evidence for a triable VPPA claim.[308]

IV. USE OF SOCIAL PLUGINS SHOULD CONSTITUTE ACTUAL KNOWLEDGE UNDER THE VPPA

Hulu's decision to include the Facebook Like plugin on its website was a business decision to transmit private information in exchange for detailed analytics.[309] Hulu makes revenue from advertisers that pay to run commercials at periodic breaks during a user's programming.[310] Thus, Hulu has an interest in obtaining detailed information on its users and their interactions with its website.[311] Similarly, Facebook seeks to combine as many user data points as possible to serve as targetable data

304 *See* Kerr, *A User's Guide*, *supra* note 292, at 1208 ("Courts, legislators, and even legal scholars have had a very hard time making sense of the SCA."); Solove, *supra* note 278, at 772 ("Congress's electronic surveillance law is infinitely more complex than the technologies it seeks to regulate.").

305 *In re Hulu II*, No. C 11-03764 LB, 2014 WL 1724344, at *15 (N.D. Cal. Apr. 28, 2014) (discussing the factual circumstances in *Freedman v. America Online, Inc.* and *Muskovich v. Crowell*, as examples of conduct that did and did not meet the knowledge requirement under the ECPA).

306 *See In re Hulu III*, 86 F. Supp. 3d at 1099 (discussing how plaintiffs offer no proof that Hulu knew Facebook might combine data to yield PII).

307 *See What Information Does Facebook Get When I Visit a Site with the Like Button?*, FACEBOOK HELP CTR., https://m.facebook.com/help/186325668085084?helpref=related [https://perma/cc/38B2-YWQ3] [hereinafter *What Information Does Facebook Get*] (last visited Oct. 1, 2019) (explaining the data points received from the Like button includes the individual's Facebook user ID, the website being visited, and "the date and time and other browser-related info").

308 *See supra* notes 245–247.

309 *See In re Hulu III*, 86 F. Supp. 3d at 1093-94.

310 *Id.* at 1093.

311 *Cf. Data Policy*, FACEBOOK, https://www.facebook.com/full_data_use_policy#sharing-partner-information (last updated Apr. 19, 2018) (describing how Facebook provides statistics and insights to third-party partners who use Facebook to operate their services).

points for online companies' marketing purposes.[312] The commercial nature of the relationship between Hulu and Facebook illustrates a mutual understanding as required by the court's interpretation of the VPPA.[313] It demonstrates that Hulu expected its data to be readable by Facebook and in exchange to receive information about the types of people who use its service.[314] This shared purpose suggests that Hulu's use of the Like button is significant contextual evidence for the knowledge requirement.[315] Thus, the court could reasonably have inferred that Hulu knew Facebook would link information together to learn the video preferences of an identified Facebook user.[316]

The court's legal analysis of the business relationship between Hulu and Facebook was inadequate for two principal reasons. First, the court stated that the Facebook Like button does not provide proof that Hulu knew the plugin would identify a specific user had watched a specific video,[317] however, Facebook's publicly available Help Center page explains that the use of the Like button results in the user's Facebook ID and browsing data from the webpage being shared with Facebook.[318] This demonstrates how the court's unfamiliarity with privacy issues stemming from the use of social plugins prevented it from granting such evidence the weight it deserved.[319] For that reason, the court failed to

312 *See supra* notes 245–247.

313 *In re Hulu III*, 86 F. Supp. 3d at 1097; *see supra* notes 245–247.

314 *See Data Policy*, *supra* note 311 (discussing how Facebook uses data transmitted from websites its users visit for business clients' analytical reports).

315 *See In re Hulu III*, 86 F. Supp. 3d at 1096-97 ("No one would deny that I would violate the VPPA . . . if my recipient and I both understood that we would use a mutually intelligible code . . . . For a disclosure to arise . . . there generally must be proof of further action by the recipient; they must know that I have used a code and they must at least have the capacity to decode and read the contents.").

316 *See id.*

317 *Id.* at 1101 (discussing that Hulu's use of the Facebook Like button provided no proof that Hulu knew the plugin would disclose to Facebook that a specific user had watched a specific video).

318 *What Information Does Facebook Get*, *supra* note 307 ("[W]hen you go to a website with a Like button . . . the data we receive includes your user ID, the website you're visiting, the date and time and other browser-related info.") (last visited Jan. 4, 2019); *see Data Policy, supra* note 311 ("We use the information we have (including your activity off our Products, such as the websites you visit and ads you see) to help advertisers and other partners measure the effectiveness and distribution of their ads and services, and understand the types of people who use their services and how people interact with their websites, apps, and services.").

319 *See In re Hulu III*, 86 F. Supp. 3d at 1101 (discussing that Hulu's use of the Facebook Like button provided no proof that Hulu knew the plugin would disclose that a specific user had watched a specific video); *What Information Does Facebook Get*, *supra* note 307 ("[W]hen you go to a website with a Like button . . . [t]he data we receive

understand that social plugins are useful to a website because the website knows precisely what user-identifying information is transmitted during the webpage load time.[320] Specifically, the website is aware that the user ID will be combined with the URL of the visited page and sent to a Social Networking Service ("SNS") like Facebook.[321] Moreover, implementing the Like button is intended to grant Facebook permission to combine data to provide informative analytics back to Hulu.[322] As a result, the court's assertion that Hulu's use of the Like button only demonstrated its knowledge of how social plugins function was short-sighted. [323] It overlooked the purpose behind the use of social plugins in ecommerce.[324] Overlooking how social plugins transmit data

includes your user ID, the website you're visiting, the date and time and other browser-related info.") (last visited Jan. 4, 2019); *Data Policy, supra* note 311.

320 *See In re Hulu III*, 86 F. Supp. 3d at 1099 (stating there was evidence that Hulu knew that, when the Like button loaded, relevant data was sent to Facebook, however, it did not prove Hulu's knowledge that Facebook might combine the data to yield PII under the VPPA); *see also* KONTAXIS ET AL., *supra* note 36 (discussing that the transmission of user identifying information during the load time of a website with a social plugin will include the URL of the visited page and the user' social media profile that typically contain the person's name, email address, and other private information); Caitlin Dewey, *98 Personal Data Points that Facebook Uses to Target Ads to You*, WASH. POST (Aug. 19, 2016) https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/?noredirect=on&utm_term=.b463dca7459e. *But see In re Hulu II*, No. C 11-03764 LB, 2014 WL 1724344, at *16 (N.D. Cal. Apr. 28, 2014) (stating there might be a VPPA violation if Hulu and Facebook negotiated the exchange of data when the Like button loaded, or if Hulu knew that it was transmitting PII).

321 *See supra* notes 311–318; KONTAXIS ET AL., *supra* note 36 (discussing that the transmission of user identifying information during the load time of a website with a social plugin will include the URL of the visited page and the user' social media profile that typically contain the person's name, email address, and other private information); *see also* Dewey, *supra* note 320.

322 *See About Facebook Pixel*, *supra* note 111 (explaining that pixel code embedded in Facebook plugins will gather HTTP headers and Facebook profile cookies are compiled together to better target ads).

323 *See In re Hulu III*, 86 F. Supp. 3d at 1101 ("In the end, though, the show_faces [the Like button] evidence suggests at most what Hulu should have known generally about how show_faces=true worked.").

324 *See id.* (stating that the court is aware that personal information is constantly shared and connected across the Internet but that there must be specific proof about what information was sent and connected and what Hulu actually knew about these things); Will Oremus, *Facebook's Five New Reaction Buttons: Data, Data, Data, Data, and Data*, SLATE (Feb. 24, 2016, 1:06 PM), http://www.slate.com/blogs/future_tense/2016/02/24/facebook_s_5_new_reactions_buttons_are_all_about_data_data_data.html (discussing how the Like button has always been a key source of data for Facebook's business clients and how new reaction plugins provide additional data points that can be combined).

contradicted the court's statement that context matters in determining if there has been an actionable disclosure.[325]

Second, the court misconstrued the degree of certainty a defendant must have about the requisite circumstances constituting the offense to establish a knowing state of mind.[326] In particular, the court referenced *Mollett v. Netflix, Inc.*, a 2012 VPPA case which did not define the term knowingly but did address how to determine liability.[327] *Mollett* stated that plaintiffs must allege facts that give rise to a reasonable inference that a defendant knowingly disclosed PII to someone other than the consumer.[328] The plaintiffs in *Hulu* asserted the evidence presented permitted a reasonable inference that Hulu knew it was sending PII to Facebook.[329] However, the court asserted there was a lack of specific proof based on the use of the Like button.[330] This demonstrates that the court's failure to understand how data is transferred via social plugins prevented it from appreciating the specificity of the plaintiffs' alleged facts.[331]

Additionally, the Hulu court relied on ECPA cases that emphasized specific legislative history about the imposition of liability for acting knowingly.[332] The legislative history stated that there is good reason for imposing liability when he is aware "that the result is practically certain

---

[325] *See In re Hulu II*, No. C 11-03764 LB, 2014 WL 1724344, at *11 (N.D. Cal. Apr. 28, 2014) ("In sum, the statute, the legislative history, and the case law do not require a name, instead require the identification of a specific person tied to a specific transaction, and support the conclusion that a unique anonymized ID alone is not PII but context could render it not anonymous and the equivalent of the identification of a specific person.").

[326] *See In re Hulu III*, 86 F. Supp. 3d at 1095 (citing Freedman v. Am. Online, Inc., 329 F. Supp. 2d 745 (E.D. Va. 2004); Worix v. MedAssets, Inc., 857 F. Supp. 2d 699 (N.D. Ill. 2012); Mollett v. Netflix, Inc., No. 5:11-CV-01629-EJD, 2012 WL 3731542 (N.D. Cal. Aug. 17, 2012)).

[327] *See* Mollett v. Netflix, Inc., No. 5:11-CV-01629-EJD, 2012 WL 3731542, at *4 (N.D. Cal. Aug. 17, 2012).

[328] *Id.* ("Plaintiffs must still allege facts giving rise to a reasonable inference that Netflix knowingly or willfully disclosed PII to someone other than the consumer.").

[329] *In re Hulu III*, 86 F. Supp. 3d at 1101.

[330] *Id.* (explaining there was insufficient evidence to prove what Hulu knew about what was done with data sent Facebook).

[331] *See id.* at 1099 ("The plaintiffs do not cite the facts discussed below to show Hulu's knowledge that Facebook might combine these things to yield PII under the VPPA. They marshal these facts to show only that Hulu knew that, when the Like button loaded, the c_user cookie would send user-identifying information to Facebook.").

[332] Worix v. MedAssets, Inc., 857 F. Supp. 2d 699, 702 (N.D. Ill. 2012) ("[L]egislative history is not always a clear guide to the meaning of a statutory term. But *Muskovich*, *Freedman*, and the legislative history all read the statutory requirement of "knowing" conduct consistently . . . .").

to follow from his conduct, whatever his desire may be as to that result."[333] By identifying that Hulu wrote and installed the code that integrated the Like button on the watch pages,[334] the court could have reasonably concluded that Hulu knew it was transmitting Facebook ID cookies and video watch pages, and that Facebook was subsequently combining the data to create PII.[335] Indeed, this is the purpose behind the use of social plugins.[336] Furthermore, had the court appreciated the end goal of both parties,[337] it would not have been arbitrary to equate Hulu's use of social plugins with actual knowledge of disclosure.[338] Taken as a whole, the court's misunderstanding of technology[339] minimized the plaintiff's evidence to general contextual evidence.[340] More strikingly, the court failed to consider the information Facebook already had in its possession from other sources and how this information strengthens the relevance of context in pleading a triable claim.[341]

---

[333] H.R. REP. NO. 99-647, at 49 (1986) (quoting United States v. U.S. Gypsum Co., 438 U.S. 422, 445 (1978)).

[334] *In re Hulu II*, No. C 11-03764 LB, 2014 WL 1724344, at *16 (N.D. Cal. Apr. 28, 2014).

[335] *See About Facebook Pixel*, *supra* note 111 ("When you set up the Facebook pixel, we will start to receive information from your website. This information allows us to better target your ads and optimize your ads for conversions.").

[336] *See supra* notes 245–247, 318 and accompanying text.

[337] The court discusses how transmission of data results in revenue for both companies but lacks any discussion as to the quality of data (e.g., combining data to identify an individual on a website) required to make that revenue stream possible. *See In re Hulu III*, 86 F. Supp. 3d 1090, 1093 (N.D. Cal. 2015) (discussing how advertisers pay Hulu based on how many times an ad is viewed and that Facebook makes money from advertisement revenue); Keith Collins & Larry Buchanan, *How Facebook Lets Brands and Politicians Target You*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/interactive/2018/04/11/technology/facebook-sells-ads-life-details.html (discussing the growth and development of Facebook's ad-targeting platform by refining data to identify individuals and increase the accuracy of targeted advertising).

[338] *See supra* notes 309–316 and accompanying text.

[339] *See In re Hulu III*, 86 F. Supp. 3d at 1103 (discussing how even if loading the Like button is akin to beacon technology, there is no evidence of a connection to the watch-page URLs). *See generally* Paris Martineau, *Facebook is Tracking You on 8.4 Million Websites*, OUTLINE (May 18, 2018, 1:37 PM), https://theoutline.com/post/4578/facebook-is-tracking-you-on-over-8-million-websites (explaining that the Like button appears on 8.4 million websites for the purposes of tracking users' activity on each site which is added with their overall profile for retargeted advertising purposes).

[340] *See In re Hulu III*, 86 F. Supp. 3d at 1102-04 (explaining that evidence of Hulu's internal emails and use of source code was too general to determine what information was sent to Facebook and combined).

[341] *See id.* at 1093 ("Facebook collects information and processes content 'shared by its users,' and it provides that information to marketers."); *id.* at 1104 (explaining emails

Some have argued that "the knowledge element of the VPPA violation is intertwined with the definition of PII."[342] In particular, if a defendant did not think they were conveying PII, "then there could be no knowledge of the conveyance, regardless of whether they knew what the third party might do with the information."[343] This interpretation of knowingly follows from courts taking *Hulu* to mean that they are prohibited from examining the context in which information is disclosed.[344] Consequently, judges discount context such that there is no VPPA violation where the recipient of information must take "further steps" to match the identifier to a specific person.[345] Many courts consider this limitation to what constitutes PII under the VPPA to be consistent with the purpose of the statute.[346] However, this rationale suffers from the same lack of consideration of the interrelationship between technology and consumer data commerce as the opinion in *Hulu*.[347] The context in which information is disclosed and the risk of user information being exposed as a result of disclosure are factors that courts should consider, especially given that emerging technologies may cause prior conclusions about certain user information to be inadequate today.[348] Understanding that these disagreements over PII persist,[349] social plugins constituting actual

sent internally at Hulu and its privacy policy are, at best circumstantial proof of Hulu's knowledge for purposes of the VPPA claim); Macioce, Jr., *supra* note 269, at 367 ("*In re Hulu II* has been interpreted to prohibit an examination of the context in which information is disclosed. But *In re Hulu II* did not foreclose the importance of examining the context of information disclosure in determining whether it constitutes PII.").

342 Bernardino v. Barnes & Noble Booksellers, Inc., No. 17-CV-04570 (LAK) (KHP), 2017 WL 3727230, at *9 (S.D.N.Y. Aug. 11, 2017).

343 *Id.*

344 Macioce, Jr., *supra* note 169, at 365-67; *see Bernardino*, 2017 WL 3727230 at *9 ("Recently, the court in *In re Hulu Privacy Litigation* addressed the knowledge element of a VPPA violation . . . . [T]he court found that a plaintiff must prove that the defendant knew that a third party would actually link information it had with other information conveyed and become aware that a particular person had in fact purchased a particular video.").

345 Macioce, Jr., *supra* note 169, at 366-67 (discussing the Eleventh Circuit's rationale in Ellis v. Cartoon Network, Inc. in adopting a narrow view of PII based on the decision in *Hulu*).

346 *Bernardino,* 2017 WL 3727230 at *9 ("Other courts have recognized that there must be limitations to what constitutes PII under the VPPA.") (citing *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 383 (3rd Cir. 2016); Robinson v. Disney Online, 152 F. Supp. 3d 176, 181 (S.D.N.Y. 2015)).

347 *See* Macioce, Jr., *supra* note 169, at 388-89.

348 *Id.*

349 *See* Gevorkian, *supra* note 154.

knowledge would reduce arbitrary decision-making for what counts as identifiable information under the VPPA.[350]

V. SOCIAL PLUGINS AS A PROPOSED LEGAL RULE

A. The Futility of a Legislative Solution

For many privacy advocates, only the passage of a detailed consumer privacy bill will suffice. [351] And perhaps proponents of such federal legislation are justified in settling for nothing less.[352] The current privacy model for websites puts the onus on the user to decide whether opt-in or opt-out policies are fair.[353] But most consumers do not have the knowledge or time to understand what types of data sharing are reasonable.[354] For that reason, consumer privacy as an inherent right has been supported by the European Union's General Data Protection Regulation ("GDPR") and CCPA to give individual users more control of their personal data.[355]

---

[350] *See* Schwartz & Solove, *supra* note 120, at 1847-48 ("[W]hether information can be re-identified depends on technology and corporate practices that permit the linking of de-identified data with already-identified data.").

[351] *See #Takectrl: Nationwide Privacy Push*, ACLU, https://www.aclu.org/issues/privacy-technology/takectrl-nationwide-privacy-push (last visited Jan. 4, 2019) [https://perma.cc/BA2K-FUCD] (discussing how various coalitions of elected officials and citizens that introduced bills in 16 states on January 20, 2016 to enhance protection of personal privacy in the digital age); *Status of Internet Privacy Legislation by State*, ACLU, https://www.aclu.org/issues/privacy-technology/internet-privacy/status-internet-privacy-legislation-state (last visited Jan. 4, 2019) [https://perma.cc/8UTE-UK4G] (listing states that have introduced privacy legislation in 2017 in response to President Trump signing a law overturning strong, commonsense privacy rules that gave consumers control over what internet service providers (ISPs) could do with their data).

[352] *See* Cameron F. Kerry, *Why Protecting Privacy is a Losing Game Today—and How to Change the Game*, BROOKINGS (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game (describing the Snowden scandal of 2013, the Equifax breach of 2017, and the Cambridge Analytica controversy during the 2016 presidential election all have issued calls for federal privacy legislation).

[353] Confessore, *The Unlikely Activists*, *supra* note 15 ("'It's like selling you coffee and making it your job to decide if the coffee has lead in it.' When it comes to privacy, he said, 'we have no baseline law that says you can't put lead in coffee.'"); *id.* ("[T]he tech industry's 'notice and choice' consent model, where companies dictated all the terms of service up front, forcing consumers to either agree or find a different app.").

[354] *Id.* ("Most consumers simply didn't have the time or experience to navigate the personal-data economy on their own.").

[355] *See id.* (explaining that CPPA allows consumers to "opt out" of data sales between companies, compared to the GDPR, which requires companies to obtain consumers' permission for collecting the information in the first place.); Keith Johnson, *What is*

Still, meaningful privacy protection is unlikely given President's Trump recent signing of legislation that repealed various consumer privacy statutes.[356] Furthermore, the tech industry has invested in lobbying efforts to combat legislation that threatens access to free user data which it depends on.[357] The impact of such efforts has already been realized with the 2012 Amendment to the VPPA.[358] However, the most compelling reason that privacy legislation is not a viable solution for consumers is that the public does not actually want it.[359]

If consumer privacy legislation is passed, social media platforms would likely become subscription-based.[360] Because social media platforms follow an advertising-supported business model, regulating it would reduce profits and force sites to make its users pay for the service.[361] Moving from a free service to paid service for social platforms is an outcome that Americans likely do not want.[362] That may change

Consumer Data Privacy, and Where is it Headed?, FORBES (July 9, 2018, 7:45 AM), https://www.forbes.com/sites/forbestechcouncil/2018/07/09/what-is-consumer-data-privacy-and-where-is-it-headed/#6b8e05941bc1 (describing consumer privacy as a right that GDPR protects by giving control over personal data to citizens).

356 Confessore, *The Unlikely Activists*, *supra* note 15 (discussing the Trump administration's meetings to set a new national privacy standard that would perhaps override California's new privacy statute); David Shepardson, *Trump Administration Working on a Consumer Data Privacy Policy*, REUTERS (July 27, 2018, 2:36 PM), https://www.reuters.com/article/us-usa-internet-privacy/trump-administration-working-on-consumer-data-privacy-policy-idUSKBN1KH2MK ("In April 2017, Trump signed legislation repealing privacy rules approved during the Obama administration requiring internet service providers to do more to protect customers' privacy than websites.").

357 Confessore, *The Unlikely Activists*, *supra* note 15.

358 *See supra* Part I.E.

359 *See* Johnson, *supra* note 355 ("[I]s it reasonable for consumers to receive a free service like Facebook in exchange for sharing their data? Ask most consumers and they will say 'it depends.' Are we talking about sharing all my photos? Who gets them? What about my posts? Does someone read them or is it a bot scanning for keywords? What are the keywords used for anyway?").

360 *See* Callum Borchers, *Would You Pay $18.75 for Ad-Free Facebook?*, WASH. POST (Apr. 14, 2018) https://www.washingtonpost.com/news/the-fix/wp/2018/04/14/would-you-pay-18-75-for-ad-free-facebook/; Sean Keach, *Paid Version of Facebook? Here's How Much it Could Cost You Each Month*, SUN (Apr. 16, 2018, 2:53 PM), https://www.thesun.co.uk/tech/6062210/facebook-paid-money-monthly-fee-how-much.

361 Borchers, *supra* note 360 (describing Facebook's advertising-supported business model); Keach, *supra* note 360 (explaining that Facebook cannot offer its services for free because then it would not make any money).

362 *See, e.g.*, Rani Molla, *How Much Would You Pay for Facebook Without Ads?*, RECODE (Apr. 11, 2018, 5:46 PM), https://www.recode.net/2018/4/11/17225328/facebook-ads-free-paid-service-mark-zuckerberg; *Would You Pay For Facebook? The Digital Economy May Be Heading That Way*, FORBES (May 3, 2018, 4:15 PM), https://www.forbes.com/sites/quora/2018/05/03/would-you-pay-for-facebook-the-digital-economy-

given the growing public mistrust of big tech companies when it comes to safeguarding user data.[363] But even then, Silicon Valley's political presence will likely thwart passage of any comprehensive privacy bill.[364] Accordingly, the courts recognizing the role social plugins play in data collection by tech companies could impact consumer privacy interests presently.[365] Because of the VPPA's private right of action, social plugins constituting actual knowledge would provide a basis for triable claims and could potentially financially impact Silicon Valley companies.[366]

B. Judicial Solution: Recognizing Social Plugins' Implications for "Knowledge"

The GDPR went into effect in the European Union in May 2018 and "regulates the processing by an individual, a company, or an organization of personal data relating to individuals in the EU."[367] A website that utilizes sponsored content, such as social plugins that track users via pixels, must get consent from visitors immediately when they visit the site.[368] If users do not consent to the use of their personal information for analytics, they should still be able to use the website in some way.[369]

may-be-heading-that-way/ ("For some reason, we seem to value digital and physical goods differently. We'll drop $5 on daily lattes from Starbucks without thinking twice, but won't spend more than 99 cents on an app.").

363 *See* Jonathan Vanian, *Facebook Is the Least Trusted Major Tech Company When It Comes to Safeguarding Personal Data, Poll Finds*, FORTUNE (Nov. 8, 2018), http://fortune.com/2018/11/08/mark-zuckerberg-facebook-reputation.

364 Alvaro M. Bedoya, *Why Silicon Valley Lobbyists Love Big, Broad Privacy Bills*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/opinion/silicon-valley-lobbyists-privacy.html ("We cannot underestimate the tech sector's power in Congress and in state legislatures. If the United States tries to pass broad rules for personal data, that effort may well be co-opted by Silicon Valley, and we'll miss our best shot at meaningful privacy protections.").

365 *See supra* Part IV.

366 *See* Confessore, *The Unlikely Activists*, *supra* note 15 (discussing how a private right of action in privacy legislation poses a real threat to Silicon Valley's data collection practices).

367 *What Does the General Data Protection Regulation (GDPR) Govern?*, EUROPEAN COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en (last visited Jan. 4, 2019) [https://perma.cc/JVA2-XCKM].

368 *See GDPR Key Changes*, EU GDPR, https://eugdpr.org/the-regulation (last visited Jan. 4, 2019); Luke Irwin, *How the GDPR Affects Cookie Policies*, IT GOVERNANCE (Sept. 15, 2017), https://www.itgovernance.eu/blog/en/how-the-gdpr-affects-cookie-policies.

369 *How Are My Cookies?,* PRIVSECREPORT (Sept. 13, 2017), https://gdpr.report/news/2017/09/13/how-are-my-cookies [https://perma.cc/F2NP-WQ5Z].

Pursuing similar legislation at the federal level in the United States is desirable, but unlikely.[370] This is due to big tech's lobbying efforts,[371] President Trump's stance on privacy,[372] and Congress's skepticism regarding the passage of a comprehensive federal privacy law.[373] Thus, courts should adopt a legal rule that states the use of social plugins on a website satisfies the knowledge requirement under the VPPA unless meaningful consent has been obtained by the user.[374] This would be effective in application across cases with different factual circumstances because of the widespread use and development of plugins as a means of collecting consumer data.[375] Moreover, such a rule would clarify what type of conduct constitutes awareness of the factual circumstances constituting a violation of the VPPA.[376] Most importantly, from a pleading standpoint, it would address the court's requirement in *Hulu* of providing affirmative proof that a defendant knows the third party is combining data to recreate PII.[377] Overall, a rule that states placing third-party social plugins on a website constitutes actual knowledge under the VPPA would make for an actionable claim.[378] Additionally, it would still adequately protect the interests of parties involved on all sides of the business of online video streaming.[379]

370 *See* Sonntag, *supra* note 156, at 268 (discussing the need for new digital privacy legislation to include a strict consent provision informing precisely what data is being combined); Cecilia Kang, *Tech Industry Pursues a Federal Privacy Law, on Its Own Terms*, N.Y. TIMES (Aug. 26, 2018), https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html.

371 *See supra* text accompanying notes 18–23 and note 364.

372 *See supra* note 356 and accompanying text.

373 *See supra* note 32 and accompanying text.

374 *See* Kathleen M. Sullivan, *The Justices of Rules and Standards*, 106 HARV. L. REV. 22, 62 (1992) ("[Legal rules] force the decisionmaker to treat differently cases that are actually substantively alike in terms of the underlying principle or policy, and to treat similarly cases that are different. A decision favoring rules thus reflects the judgment that the danger of unfairness from official arbitrariness or bias is greater than the danger of unfairness from the arbitrariness that flows from the grossness of rules."); *How Are My Cookies?, supra* note 369 (explaining that Recital 32 of the GDPR requires that consent involve a "clear affirmative act" such as ticking a box on a website).

375 Jack Marshall, *Facebook Wants to Help Sell Every Ad on the Web*, WALL ST. J. (May 27, 2016, 12:00 AM), https://www.wsj.com/articles/facebook-wants-to-help-sell-every-ad-on-the-web-1464321603; St. John, *supra* note 35.

376 *See supra* Part IV.

377 *See In re Hulu III*, 86 F. Supp. 3d 1090, 1097-98 (N.D. Cal. 2015); King, *supra* note 52, at 142.

378 *See* Sonntag, *supra* note 156, at 270.

379 *See id.* at 270.

CONCLUSION

The crux of digital privacy concerns today is that consumers fear a lack of control over their personal information more than ongoing internet surveillance.[380] Today's digital lifestyle is based on sending and receiving "likes" that show an individual is engaged in their community.[381] The VPPA was enacted with the understanding that digital interactions would change social discourse.[382] For that reason, the VPPA focused on protecting transactional information, specifically extending privacy protection to those transactions involving the purchase or rental of video tapes.[383] The disclosure of a consumer's video list in the twenty-first century is accomplished by way of social plugins.[384] While such a transaction is difficult to visualize, it does exist and should be subject to protection under the VPPA.[385] Furthermore, the business context surrounding this data transmission indicates that tech companies expect third parties to identify individuals with each transaction.[386] Therefore, the courts should construe an internet platform's use of social plugins as actual knowledge under the VPPA since legislation is not viable and consumer protection is needed.

---

380 Susan Scutti, *The Psychology of Privacy in the Era of the Internet of Things*, CNN (Mar. 22, 2017, 5:01 AM), https://www.cnn.com/2017/03/22/health/psychology-privacy-wikileaks-internet-of-things/index.html (describing findings from a privacy experiment that when people are informed "in an easily digestible form" how, when and who will be collecting data when they buy a smart item, it could alleviate the potential downside of smart living).

381 *See* Delfina Forstmann, *The Age of the Attention Economy Fueled by Social Media Addiction*, MEDIUM (Mar. 19, 2018), https://medium.com/@goboldfish/the-age-of-the-attention-economy-fueled-by-social-media-addiction-9c8b8150cbf6 [https://perma.cc/6YC3-ZREJ] ("Perhaps the 'like' button is an inoffensive way to show that you are paying attention. . . . This form of attention expression has become a new form of currency. People can count 'likes' on their posts and then may be driven to act a certain way to generate more engagement.").

382 *See* S. REP. NO. 100-599, at 5-6 (1988).

383 *Id.* at 12.

384 *See supra* Part IV.

385 *See supra* Part II.

386 *See supra* Part IV.