Stepping in for the FCC: Extending the Video Privacy Protection Act to Internet Service Providers

*Claire O'Rourke**

Introduction

During then-D.C. Federal District Court Judge Robert Bork's confirmation hearing for the United States Supreme Court, the *Washington City Paper* published an article based on a list of his family's video rental history, provided by the judge's local video store.[1] Congress, outraged at this invasion of the judge's privacy, passed the Video Privacy Protection Act (VPPA) in 1988, which holds video service providers liable if they knowingly disclose data that personally identifies consumers.[2]

Since the VPPA became law, the video store era has faded into the past and online video streaming is the new normal. Although there was little court action on the VPPA in the immediate aftermath of its passage, the modern video era has led several federal circuit courts to assess whether the VPPA applies to data generated through online video streaming, either via websites or apps.[3] However, no clear judicial consensus has formed across the circuits on how to apply the statute, and the Supreme Court has declined to review the issue.[4]

Inconsistent judicial rulings reflect a broader problem of patchwork privacy laws for all online data collection. Several alphabets worth of agencies oversee some aspect of data privacy; but in October

* Antonin Scalia Law School, J.D. expected, 2020.

1 *See* Andrea Peterson, *How Washington's Last Remaining Video Rental Store Changed the Course of Privacy Law*, Wash. Post (Apr. 28, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/04/28/how-washingtons-last-remaining-video-rental-store-changed-the-course-of-privacy-law.

2 18 U.S.C.A. § 2710 (West 2013); Peterson, *supra* note 1.

3 *See* Eichenberger v. ESPN, Inc., 876 F.3d 979, 984 (9th Cir. 2017); *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 267 (3d Cir. 2016); Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 484 (1st Cir. 2016); Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1255-57 (11th Cir. 2015).

4 *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 273 (3d Cir. 2016), *cert. denied* sub nom. C. A. F. v. Viacom Inc., 137 S. Ct. 624 (2017).

2016, the Federal Communications Commission (FCC) issued a wide-sweeping privacy rule on internet service providers' (ISPs) use of consumer data, the most significant action taken by a regulator on data privacy in decades.[5] This rule was quickly undone, however, just a few months later in April 2017, through the Congressional Review Act (CRA), and no additional regulations or legislation have replaced it since.[6] The combination of agency and congressional silence on clear data use privacy requirements by ISPs leaves consumers with significant gaps in their online data privacy. Despite the vacuum left without congressional action or clear regulations, consumers' data privacy rights must be protected.

This Comment argues that courts should apply the VPPA to ISPs' data collection practices to provide a strong base of online data protection for consumers. First, this Comment analyzes the history and content of the VPPA, as well as recent court rulings based on the statute. Next, it assesses how ISPs use consumers' data and the recently rescinded FCC ISPs privacy rule. Finally, it argues that courts can appropriately apply the VPPA to ISPs, rather than just to specific apps or websites that stream videos. This VPPA application will provide a good first step in protecting consumer data privacy with ISPs, regardless of when Congress or various government agencies move again to formally address this topic.

I. BACKGROUND

A. *The VPPA's History and Substance*

Decades later, Robert Bork's Supreme Court nomination is best remembered for how its vote ended—in defeat.[7] Commentators reference his nomination as forever changing the landscape for judicial nominees because of the "scorched earth" tactics now employed over

---

[5] *See* Brian Fung and Craig Timberg, *The FCC Just Passed Sweeping New Rules to Protect Your Online Privacy*, WASH. POST (Oct. 27, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/10/27/the-fcc-just-passed-sweeping-new-rules-to-protect-your-online-privacy/?tid=a_inl&utm_term=.f3eac5ad2bb8., *What to Expect Now that Internet Providers Can Collect and Sell Your Web Browser History*, WASH. POST (Mar. 29, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/03/29/what-to-expect-now-that-internet-providers-can-collect-and-sell-your-web-browser-history.

[6] S.J. Res. 34, 115th § 1 (as passed by House, Mar. 28, 2017).

[7] *Senate's Roll-Call On the Bork Vote*, N.Y. TIMES (Oct. 24, 1987), http://www.nytimes.com/1987/10/24/us/senate-s-roll-call-on-the-bork-vote.html.

ideological differences during Supreme Court nominations.[8] Nevertheless, there was an additional outcome that is rarely discussed in modern tellings of the Bork saga: the "Bork Bill."[9] When a local Washington, D.C. paper acquired the Bork family's two-year video rental history and printed a summary of that list as part of its nomination coverage, many members of the House and Senate denounced this release.[10] Although not impactful on the nomination itself, the rental list disclosure became the catalyst for the enactment of the VPPA in 1988.[11]

The Senate released a committee report to accompany the VPPA's congressional consideration.[12] It characterizes the VPPA as an attempt "to give meaning to, and thus enhance, the concept of privacy for individuals in their daily lives."[13] Although Judge Bork's rental history was the impetus, the discussion in the report takes on a more general tone to drive home the point that "information collected for one purpose may not be used for a different purpose without the individual's consent."[14] Senator Patrick Leahy, one of the lead cosponsors of the bill, declared:

> In an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone. I think that is wrong. I think that really is Big Brother, and I think it is something that we have to guard against.[15]

Another cosponsor, Senator Alan Simpson, stated when the bill was introduced, "The advent of the computer means not only that we can be more efficient than ever before, but that we have the ability to

---

[8] Nina Totenburg, *Robert Bork's Supreme Court Nomination 'Changed Everything, Maybe Forever*,' NPR (Dec. 19, 2012), http://www.npr.org/sections/itsallpolitics/2012/12/19/167645600/robert-borks-supreme-court-nomination-changed-everything-maybe-forever.

[9] *See* Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689, 694 (2013).

[10] S. REP. NO. 100-599, at 5 (1988), *as reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4342–5.

[11] *See id.* at 9, *as reprinted* at 4342–8.

[12] S. REP. NO. 100-599 (1988), *as reprinted in* 1988 U.S.C.C.A.N. 4342-1.

[13] *Id.* at 5, *as reprinted* at 4342–5.

[14] *Id.* at 8, *as reprinted* at 4342–8.

[15] *Id.* at 5-6, *as reprinted* at 4342–5, 6.

be more intrusive than ever before."[16] He continued, "Every day Americans are forced to provide to businesses and others personal information without having any control over where that information goes."[17] As a result of this challenge, Senator Simpson believed the VPPA was necessary to "protect time honored values . . . particularly our right to privacy."[18] Against this discussion and backdrop, the VPPA passed both chambers of Congress with so little controversy that it was done by voice vote.[19]

The VPPA—which now includes a modification from 2012[20]—creates liability for any "video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider."[21] It also provides several exceptions to this blanket liability.[22] If a consumer signs a written consent, a video service provider is permitted to share some of her personally identifiable information.[23] This consent can be electronic, but in all cases it must be in a "distinct and separate" form from other customer obligations.[24] Consent may be given either "at the time the disclosure is sought" or in advance for up to two years.[25] For any form of consent, the video service provider must provide the consumer a "clear and conspicuous" opportunity to withdraw, either case-by-case or at any point prior to the advance consent's natural expiration.[26] A video service provider is also permitted to share data with law enforcement officers who produce a warrant.[27] Additionally, a video service provider may furnish "solely . . . the names and addresses of consumers" to any third party, provided that the consumer has had the "clear and conspicuous" ability to prohibit this type of disclosure.[28] However, this disclosure cannot include any details such as "the title, description

16 *Id.* at 6, *as reprinted* at 4342–6, 7.

17 S. REP. NO. 100-599, at 6-7 (1988), *as reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4342–6, 7.

18 *Id.*

19 S.J. Res. 34, 115th § 1 (as passed by House, Mar. 28, 2017), Roll Call Vote available at http://clerk.house.gov/evs/2017/roll202.xml; William McGeveran, *The Law of Friction*, 2013 U. CHI. LEGAL F. 15, 23 (2013).

20 Public Law No: 112-258; H.R. 6671, 112th Cong. (2012).

21 18 U.S.C.A. § 2710(b)(1) (West 2013).

22 18 U.S.C.A. § 2710(b)(2) (West 2013).

23 18 U.S.C.A. § 2710(b)(2)(B) (West 2013).

24 *Id.*

25 *Id.*

26 *Id.*

27 18 U.S.C.A. § 2710(b)(2)(C) (West 2013).

28 18 U.S.C.A. § 2710(b)(2)(D) (West 2013).

or subject matter" of the viewed videos.[29] Furthermore, there is an exception that does allow subject matter disclosure if its purpose is only to market "directly to the consumer."[30] Finally, the statute sets a limit to the length of time for which video service providers may keep a consumer's personally identifiable information.[31] For video service providers who violate the VPPA, the damages include actual damages not less than $2,500, as well as the possibility of punitive damages, fees, or other relief.[32]

The definitions section of the VPPA, on its face, seems to be very broad.[33] The statute defines a "consumer" as "any renter, purchaser, or subscriber of goods or services from a video tape service provider."[34] "Personally identifiable information" (PII) covers information "which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."[35] Finally, the video tape service provider itself is defined beyond video tapes.[36] A "video tape service provider" is "any person, engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials."[37] It is this definitional aspect, more than anything else, that has catapulted the VPPA into the modern age.[38]

B. *Modern Litigation Surrounding the VPPA*

After the VPPA sailed through Congress, it sat on the books with minimal activity surrounding it for several years.[39] Even so, as video consumption transformed with the rapid growth of the internet, the

---

[29] *Id.*

[30] 18 U.S.C.A. § 2710(b)(2)(D)(ii) (West 2013).

[31] 18 U.S.C.A. § 2710(e) (West 2013).

[32] 18 U.S.C.A. § 2710(c) (West 2013).

[33] 18 U.S.C.A. § 2710(a) (West 2013).

[34] 18 U.S.C.A. § 2710(a)(1) (West 2013).

[35] 18 U.S.C.A. § 2710(a)(3) (West 2013).

[36] *See* 18 U.S.C.A. § 2710(a)(4) (West 2013).

[37] *Id.*

[38] *See, e.g.*, Eichenberger v. ESPN, Inc., 876 F.3d 979, 981 (9th Cir. 2017); *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 268, 281 (3d Cir. 2016); Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 486 (1st Cir. 2016); Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1253 n.1 (11th Cir. 2015); *In re* Hulu Privacy Litig., No. C 11-03764 LB, 2012 WL 3282960, at *4-6 (N.D. Cal. Aug. 10, 2012).

[39] *See* Gregory M. Huffman, *Video-Streaming Records and the Video Privacy Protection Act: Broadening the Scope of Personally Identifiable Information to Include Unique Device Identifiers Disclosed with Video Titles*, 91 CHI.-KENT L. REV. 737, 738 (2016).

VPPA began to find new life.[40] Both the breadth of the definitions and the strength of the damages in the VPPA have led to a series of class action lawsuits filed in the last decade around mobile apps and video streaming websites.

In 2012, *In re Hulu Privacy Litigation* laid the initial groundwork to extend the VPPA to internet video companies.[41] In *Hulu*, the United States District Court for the Northern District of California held that the definition of a "video tape service provider" extended to those that provide videos generally, regardless of whether the videos are in the form of physical tapes and discs or in the form of digital transmissions.[42] The court also established that an individual does not need to pay for a service to be considered a "subscriber" under the VPPA's "consumer" definition.[43] This ruling left a lot of gray area—merely establishing that for someone to be protected, she needs to do more than visit a website but she could do less than pay for its services.[44]

After *Hulu*, a series of other VPPA online video cases popped up across the United States. Within a single nine-month period, three separate decisions led to a circuit split on interpretation of the VPPA's definitions.

1. The Eleventh Circuit

In 2015, the United States Court of Appeals for the Eleventh Circuit was the first to delve more deeply into the VPPA definitions in *Ellis v. Cartoon Network*.[45] Ellis was a class action member of those who downloaded Cartoon Network's free CN app on an Android mobile device.[46] He proceeded to watch various video clips on the app, though he never registered or created an account within the app.[47] Unbeknownst to him, Cartoon Network could—and did—track his viewing habits through his device's Android ID number.[48]

---

40 *See id.*

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

42 *See id.* at *6.

43 *Id.* at *8.

44 *See id.* at *7-8.

45 803 F.3d 1251 (11th Cir. 2015).

46 Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1253-54 (11th Cir. 2015).

47 *See id.* at 1254.

48 *See id.*

This number is randomly generated when an Android device is first activated and remains its unique ID through the device's lifetime.[49] When Ellis or any other Android user opened the CN app, Cartoon Network kept a log of every video watched on each device according to its Android ID number.[50] Each time Ellis closed the app, Cartoon Network sent that log, including the link between the videos and Ellis' Android ID number, to a third-party analytics company, Bango.[51] Bango "specializes in tracking individual behaviors" both in general internet browsing and via mobile device apps.[52] It took the Android ID viewing information from CN and linked it to a specific individual, based on other information from a myriad of websites across the internet.[53] All of this occurred without any disclosure from CN that Ellis' information was shared with any third party.[54]

Ellis sued Cartoon Network for violations of the VPPA—on behalf of a larger class requesting monetary and injunctive damages—claiming that he fell under its protection because he was a "subscriber" under the statute, one of its classifications of "consumer."[55] Ellis alleged that Cartoon Network had violated his VPPA rights because his Android ID number and viewing history was PII as defined by the VPPA, and Cartoon Network shared his PII without his consent to third party Bango.[56] The Eleventh Circuit held that Ellis was not a VPPA-defined consumer because he was a "mere user" of the CN app, and not a subscriber.[57] He did not pay, log in, or create an account on the app, he did not sign up for information, and he did not "make any commitment or establish any relationship that would allow him to have access to exclusive or restricted content."[58] By "downloading an app for free and using it to view content at no cost," Ellis did not meet the VPPA's threshold to be a subscriber, and thus a consumer.[59] Because Ellis was not a consumer under the VPPA, he

---

[49] *Id.*

[50] *See id.*

[51] *See id.*

[52] Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1254 (11th Cir. 2015) (internal quotation marks omitted).

[53] *Id.*

[54] *See id.*

[55] *Id.*

[56] *See id.*

[57] *Id.* at 1257.

[58] Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1257 (11th Cir. 2015).

[59] *Id.*

was not entitled to its protections.[60] Therefore, the court did not even address whether the Android ID and video viewing history were considered PII.[61]

2. The First Circuit

Sixth months after *Ellis*, the United States Court of Appeals for the First Circuit issued its own opinion on the VPPA's applicability to mobile apps in *Yershov v. Gannett Satellite Information Network, Inc*.[62] Similar to Ellis, Yershov downloaded a free app onto his phone, this time from Gannett's USA Today newspaper.[63] Again, this app did not alert users, or request their consent, to send information to a third party; yet it also shared user data.[64] Each time a user viewed a video through the app, Gannett sent a third-party analytics firm the unique user ID information—such as the Android ID used in *Ellis*—the video title, and the GPS coordinates of where the video was viewed.[65] Adobe Analytics, the third party in this case, took the information from the app and compiled it with information from other sources to create a profile of each app user's personal information.[66] This information allowed Adobe and clients such as Gannett to better understand their users' tastes and preferences, as well as helped target ads.[67]

Yershov sued Gannett under the VPPA, alleging that he was a subscriber—and thus a consumer—under the statute, and that Gannett had shared his PII with Adobe Analytics.[68] The First Circuit held that by downloading the app, Yershov *was* a subscriber under the VPPA's "consumer" definition.[69] Even without submitting payment or creating an account, by putting the app on his phone, Yershov created a "materially different" relationship with USA Today than if he had just visited the website.[70] In addition, Yershov provided informa-

60 *See id.* at 1257-58.
61 *See id.*
62 Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 484 (1st Cir. 2016).
63 *See id.* at 485.
64 *See id.*
65 *See id.*
66 *Id.* at 484-85.
67 *See id.*
68 *See* Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 485 (1st Cir. 2016).
69 *Id.* at 487.
70 *Id.* at 489.

tion to Gannett through the app, even though that process occurred without his consent.[71] This interpretation of the VPPA's consumer definition is inconsistent with the Eleventh Circuit's holding in *Ellis* that downloading an app does not make a user a subscriber.[72]

The First Circuit also held in *Yershov* that Yershov's information shared with Adobe Analytics did constitute PII.[73] The court characterized the information as "effectively revealing the name of the video viewer."[74] It cautioned that there may be situations with other data where linking the information to a particular person is too tenuous to be PII; but here the link was "both firm and readily foreseeable to Gannett."[75]

3. The Third Circuit

Finally, the United States Court of Appeals for the Third Circuit decided a VPPA case in June 2016.[76] *In re Nickelodeon Consumer Privacy Litigation* continued the push on VPPA class actions suits, this time by children against Viacom for unlawful collection of their data through the Nickelodeon website, Nick.com.[77] Viacom transmitted to Google—or Google itself collected through an electronic "cookie" that Viacom installed on its behalf—eleven different data points on the children.[78] The data points included information such as the children's browser and operating system histories, IP addresses, and unique user IDs generated by the cookie.[79] The Third Circuit held that only "the kind of information that would readily permit an ordinary person to identify a specific individual[ ]" should be considered PII under the VPPA.[80] Therefore, it reasoned, "the kinds of disclosures at issue here, involving digital identifiers like IP addresses, fall outside the Act's protections."[81] During this discussion, the court noted that its characterization of PII is consistent with the PII defini-

71 *See id.*
72 *See id.*; Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1257 (11th Cir. 2015).
73 *See Yershov*, 820 F.3d at 486.
74 *Id.*
75 *Id.*
76 *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262 (3d Cir. 2016).
77 *Id.* at 267.
78 *See id.* at 269.
79 *See id.*
80 *Id.* at 290.
81 *Id.* at 267.

tion articulated in *Yershov* because this data at issue fell under the tenuous links to a particular person that the First Circuit had warned would be outside the PII definition it provided.[82]

With various and confusing definitions of "consumer" and PII floating between circuits, the Supreme Court had the opportunity to resolve the scope and definitions of the VPPA when review was requested in *Nickelodeon*. However, the Court denied certiorari in January 2017, leaving the vague and inconsistent interpretations of the VPPA definitions in place for the foreseeable future.[83]

This uncertainty only expanded in late 2017, when the United States Court of Appeals for the Ninth Circuit issued its own VPPA ruling in *Eichenberger v. ESPN, Inc.*[84] There, the court added another voice to the Third Circuit's interpretation of PII.[85] Pointing to the *Nickelodeon* holding, the Ninth Circuit held that transmission of data from a Roku device to a third-party analytics firm did not constitute disclosure of VPPA-defined PII because the shared data would not allow an ordinary person to identify the individual behind it.[86] As the debate on VPPA interpretation plays out in federal circuit courts across the country, consumers are left wondering what, if anything, is protecting their online data.

C. *Internet Service Providers (ISPs)*

Internet Service Provider (ISP) is the blanket term for a company that provides internet to a mobile device or a home.[87] Examples include AT&T, Comcast, and Verizon.[88] ISPs have a "treasure trove of user data" that "is similar to, if not larger than, that of the NSA, yet it is almost entirely unregulated."[89] This data about customers includes names, locations, places to which they travel, and every web-

---

[82] *See In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 289 (3d Cir. 2016).

[83] *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262 (3d Cir. 2016), *cert. denied sub nom.* C.A.F. v. Viacom Inc., 137 S. Ct. 624 (2017).

[84] Eichenberger v. ESPN, Inc., 876 F.3d 979 (9th Cir. 2017).

[85] *See id.* at 985-86.

[86] *See id.*

[87] *See* Jeff Dunn, *Trump Just Killed Obama's Internet-Privacy Rules — Here's What That Means for You*, BUS. INSIDER (Apr. 4, 2017, 10:55 AM), http://www.businessinsider.com/trump-fcc-privacy-rules-repeal-explained-2017-4/#how-did-all-of-this-get-started-1.

[88] *Id.*

[89] Dunn, *supra* note 87; Alice E. Marwick, *How Your Data Are Being Deeply Mined*, N.Y. REV. BOOKS (Jan. 9, 2014), http://www.nybooks.com/articles/archives/2014/jan/09/how-your-data-are-being-deeply-mined.

site that customers visit on the internet.[90] Each device a customer has is assigned an ID number by the ISP, called an IP address.[91] When an ISP connects the customer online to the web address she seeks, the ISP can see what device she is using and what websites she visits, and it can save that data.[92] The majority of traffic on ISPs are to and from websites dedicated solely to streaming online videos.[93] Netflix, YouTube, and Amazon Video alone make up almost 57 percent of downstream internet traffic in North America during peak hours.[94] By 2021, it is estimated that video-related traffic will make up 82 percent of all internet traffic.[95]

The huge swaths of data collected by an ISP as it facilitates internet access are used to produce targeted marketing on its customers, either by the ISP itself or by a third-party vendor to whom the data is sent.[96] ISPs in the past have been known to engage in practices that customers may be unaware of and likely do not appreciate.[97] These practices include selling customers' data to marketers, adding targeting data to devices based on browsing history, sending customers marketing firm results for internet searches—instead of standard search result lists—and adding electronic cookies that customers cannot delete to track their online activity.[98]

Beyond the privacy implications of ISPs and third parties storing and using customer data, there are also security risks to customers.[99]

---

[90] *See* Dunn, *supra* note 87.

[91] *See* Brian X. Chen, *What the Repeal of Online Privacy Protections Means for You*, N.Y. TIMES (Mar. 29, 2017), https://www.nytimes.com/2017/03/29/technology/personaltech/what-the-repeal-of-online-privacy-protections-means-for-you.html.

[92] *See id.*

[93] *See* Todd Spangler, *Netflix Chews Up Less Bandwidth, as Amazon Video Streaming Surges*, VARIETY, (June 22, 2016, 4:08 AM) http://variety.com/2016/digital/news/netflix-bandwidth-share-2016-1201801064/.

[94] *See id.*

[95] Rani Molla, *An Explosion of Online Video Could Triple Bandwidth Consumption Again in the Next Five Years*, RECODE, (June 8, 2017, 8:00 AM), https://www.recode.net/2017/6/8/15757594/future-internet-traffic-watch-live-video-facebook-google-netflix.

[96] *See* Aaron Pressman, *What Really Happens When the FCC's Online Privacy Rules Are Cancelled*, FORTUNE (Apr. 3, 2017), http://fortune.com/2017/04/03/fcc-online-privacy-faq/.

[97] *See* Jeremy Gillula, *Five Creepy Things Your ISP Could Do if Congress Repeals the FCC's Privacy Protections*, DEEPLINKS BLOG (Mar. 19, 2017), https://www.eff.org/deeplinks/2017/03/five-creepy-things-your-isp-could-do-if-congress-repeals-fccs-privacy-protections.

[98] *Id.*

[99] *See* Jeremy Gillula and Peter Eckersley, *Five Ways Cybersecurity Will Suffer If Congress Repeals the FCC Privacy Rules*, DEEPLINKS BLOG (Mar. 26, 2017), https://www.eff.org/deeplinks/2017/03/five-ways-cybersecurity-will-suffer-if-congress-repeals-fcc-privacy-rules.

The ads and tracking patches that marketing leaves on devices can create security vulnerabilities for hackers to exploit.[100] The mere existence of these batches of data themselves is also of interest to hackers because of the sheer volume of details contained on hundreds of thousands of individuals, which is continually growing to include many other people and data points.[101] In 2016, digital ads represented 37 percent of United States media ad spending, totaling $72 billion and thousands of data points on online browsing.[102] The size of this $72 billion market also creates more incentive for ISPs to sell data to the highest bidder, potentially at the expense of consumer privacy.[103] The more data ISPs can sell to participants in this market, the more they are incentivized to create even bigger databases, which continually increases the databases' appeal to hackers.[104]

D. *The FCC's 2016 Privacy Order*

As the circuit courts wrestled with online consumer privacy, regulatory agencies entered into the mix as well, but with an eye directly towards ISPs—not the apps or websites that courts were reviewing. In April 2016, the FCC released a Notice of Proposed Rulemaking on applying privacy requirements from the Communications Act of 1934 to ISPs, which garnered more than 275,000 responses.[105] In November 2016, the FCC released the Order, close to 400 pages long, adopting online data privacy requirements for ISPs.[106]

When presenting the rule, the FCC grouped its content into themes representing the "three foundations of privacy."[107] First, it discussed transparency.[108] In the interest of transparency, ISPs must

---

100 *See* Pressman, *supra* note 96.

101 *See id.*

102 *US Digital Ad Spending to Surpass TV this Year*, eMARKETER (Sept. 13, 2016), https://www.emarketer.com/Article/US-Digital-Ad-Spending-Surpass-TV-this-Year/1014469.

103 *See* Pressman, *supra* note 96; Brian Fung, *Republicans Voted to Roll Back Landmark FCC Privacy Rules. Here's What You Need to Know*, WASH. POST (Mar. 28, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/republicans-are-poised-to-roll-back-landmark-fcc-privacy-rules-heres-what-you-need-to-know/?utm_term=.c4288e54dd58.

104 *See* Pressman, *supra* note 96.

105 *In re* Protecting the Privacy of Customers of Broadband & Other Telecomms. Servs., 31 FCC Rcd. 2500, 13913 (2016).

106 *In re* Protecting the Privacy of Customers of Broadband & Other Telecomms. Servs., 31 FCC Rcd. 13911, 13913, 13914 (2016).

107 *Id.* at 13914.

108 *Id.*

have provided clear, accurate privacy notices, prominently displayed.[109] In addition, they must have provided customers—at the point of sale—information about what data was collected, how it was shared, and the types of entities the information was shared with.[110] Customers must have received advanced notice on material changes to privacy policies, and these privacy policies must have been available on websites and apps persistently in a clear and conspicuous manner.[111] The policies must also have stated whether customers could opt-in or opt-out of various aspects of the privacy protections.[112]

The second foundation of privacy, according to the FCC, was choice.[113] The Commission declared that "customers must be empowered to decide how broadband providers may use and share their data."[114] To further this, it created three tiers of data, each of which required a different level of consumer approval for collection and sharing.[115] First, regarding any sensitive data or material retroactive changes to data sharing policies, a customer must have opted-in to allow an ISP to share their data.[116] Sensitive data included information that most consumers traditionally think of as sensitive, such as health and medical data; but the Commission also included internet and app-use history in this category.[117] At the next level, customers had the option to opt-out of data sharing regarding non-sensitive data, such as the type of broadband service plan a customer had.[118] Finally, the Commission allowed the disclosure of basic data use that ISPs needed to continue providing service to customers.[119]

The third foundation of privacy the FCC rule covered was security.[120] The rule required ISPs to take reasonable measures to protect customer data.[121] ISPs could share data about a customer that fell

---

109 *Id.*

110 *Id.*

111 *See id.* at 13968.

112 *See In re* Protecting the Privacy of Customers of Broadband & Other Telecomms. Servs., 31 FCC Rcd. 13911, 13914 (2016).

113 *See id.*

114 *Id.*

115 *See id.* at 13914-15.

116 *See id.* at 13915.

117 *See id.* at 13914-15.

118 *See In re* Protecting the Privacy of Customers of Broadband & Other Telecomms. Servs., 31 FCC Rcd. 13911, 13915 (2016).

119 *See id.*

120 *See id.*

121 *Id.*

outside the scope of these rules, but even that data must have been de-identified, and the third party receiving it must have been contractually prohibited from re-identifying the information.[122] Furthermore, in the event that there was still a data breach, ISPs had a customer and government notification requirement that they must have satisfied within a narrow window of time.[123]

Apart from these three foundational themes, the FCC rule also addressed several other important privacy measures.[124] First, it forbid ISPs from refusing service if customers did not share their data beyond the minimal amount necessary to allow the ISP to operate (such as where to send communications from the provider to the customer).[125] It also created extensive restrictions on financial incentives that ISPs could offer customers in exchange for sharing their data.[126] Violating any terms of this rule was considered a violation of the Communications Act of 1934.[127] In the past, FCC enforcement measures against violators of the Communications Act have included civil penalties and mandatory compliance plans to force the bad actors into compliant behavior.[128]

When released, the FCC privacy rule was hailed as creating "landmark protections for internet users."[129] One privacy advocate with the Center for Digital Democracy stated the day it was released "was probably the best day we've had on . . . commercial Internet privacy—maybe ever."[130] In contrast, the Association of National Advertisers described the regulation as "unprecedented, misguided, counterproductive, and potentially extremely harmful."[131]

---

122 *See id.* at 13914, 13957-58.

123 *See id.* at 13915.

124 *See In re* Protecting the Privacy of Customers of Broadband & Other Telecomms. Servs., 31 FCC Rcd. 13911, 13915 (2016).

125 *See id.*

126 *See id.*

127 *See id.* at 13912.

128 *See e.g., AT&T Consent Decree*, 30 FCC Rcd 2808 (2015); *Cox Consent Decree*, 30 FCC Rcd 12302 (2015).

129 Cecilia Kang, *Broadband Providers Will Need Permission to Collect Private Data*, N.Y. TIMES (Oct. 27, 2016), https://www.nytimes.com/2016/10/28/technology/fcc-tightens-privacy-rules-for-broadband-providers.html.

130 Brian Fung & Craig Timberg, *The FCC Just Passed Sweeping New Rules to Protect Your Online Privacy*, WASH. POST (Oct. 27, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/10/27/the-fcc-just-passed-sweeping-new-rules-to-protect-your-online-privacy.

131 Kang, *supra* note 129.

This strong reaction from many industries did not go unnoticed by Congress. Telecom and tech industries approached the Hill immediately to lobby Congress to overturn the regulation.[132] Although not a power always available to Congress, the Congressional Review Act (CRA) allows Congress to repeal regulations reported to Congress within the previous sixty days of legislative session.[133] Because the FCC privacy regulation was released in the final days of the Obama Administration, while Congress was in session for very few days, the CRA was an optional tool.[134]

On March 23, 2017, the Senate voted to disapprove the FCC's privacy regulation in a 50-48 vote that split precisely down party lines, with Republicans voting in favor of the repeal and Democrats voting against it.[135] The House quickly followed suit in a 215-205 vote, and the President signed the repeal into law.[136] The text of the CRA provides that Congress "disapproves" of the FCC regulation and, as a result, the "rule shall have no force or effect."[137] By revoking the FCC rule, Congress effectively ensured that there cannot be regulatory action to manage ISP data sharing, as the CRA does not allow rules to be reissued in substantially similar forms.[138] Because of this limitation on future rulemakings, the CRA has been described as "a sledgehammer."[139] The FCC still has the power to sue individual telecom companies that it believes overstep the bounds of the privacy regulations and laws that remain on the books.[140] Still, it is now unable to preemptively regulate consumer privacy matters with ISPs.[141] Without this tool, the only option left for comprehensive consumer privacy pol-

132 *See* Alex Byers, *How a Telecom-Tech Alliance Wiped Out FCC's Privacy Rules*, POLITICO (Mar. 31, 2017), http://www.politico.com/story/2017/03/broadband-data-victory-republicans-236760.

133 *See* Brian Naylor, *Republicans Are Using An Obscure Law To Repeal Some Obama-Era Regulations*, NPR (Apr. 9, 2017), http://www.npr.org/2017/04/09/523064408/republicans-are-using-an-obscure-law-to-repeal-some-obama-era-regulations.

134 *See id.*

135 S.J. Res. 34, 115th Cong. § 1 (as passed by House, Mar. 28, 2017), Roll Call Vote available at http://clerk.house.gov/evs/2017/roll202.xml.

136 *Id.*

137 S.J. Res. 34, 115th § 1 (as passed by House, Mar. 28, 2017).

138 *See* 5 U.S.C.A. § 801(b)(2) (West 2018).

139 Michael Grunwald, *Trump's Secret Weapon Against Obama's Legacy*, POLITICO MAGAZINE (Apr.10, 2017), http://www.politico.com/magazine/story/2017/04/donald-trump-obama-legacy-215009.

140 *See* Fung, *supra* note 130.

141 *See id.*

icies is legislation.[142] Given that it was congressional action that removed the FCC's 2016 privacy rule, it is unlikely that Congress will soon implement legislation with similar coverage.[143]

During the advocacy efforts for the CRA, telecom companies—via their trade associations—indicated that without the FCC privacy regulation, they would voluntarily follow privacy guidelines that the Federal Trade Commission (FTC) uses for tech companies.[144] This pledge implies that tech companies would affirmatively request that customers provide consent for sharing the customers' sensitive data, since the FTC currently requires that tech companies obtain this consent.[145] However, that FTC sensitive data definition differs in a significant respect from the FCC's regulation: it does not consider "web browsing or app usage" to be sensitive.[146] Furthermore, these actions would be voluntary, so there would be no law or regulation preventing ISPs from changing their opt-in practices.[147]

Just a month after the disapproval of the FCC regulation became law, then-Representative Marsha Blackburn introduced a bill that would provide online privacy protections for consumers substantially similar to those included in the FCC's previously promulgated rule.[148] The BROWSER Act of 2017 would put enforcement in the hands of the FTC—rather than the FCC—and affect the actions of "edge" service providers, such as Google or Facebook, in addition to those of ISPs.[149] All impacted industries strongly opposed it when it was introduced, and the bill has since made no progress towards passage.[150] Even the simple step of introducing a Senate companion to begin consideration of the issue in both chambers did not occur.[151] As a result,

142 *See* 5 U.S.C.A. § 801(b)(2) (West 2018).

143 *See* Jeff Flake, *Settling a Bureaucratic Turf War in Online Privacy Rules*, WALL ST. J., Mar. 2, 2017, https://www.wsj.com/articles/settling-a-bureaucratic-turf-war-in-online-privacy-rules-1488413165.

144 *See* Dunn, *supra* note 87.

145 *See id.*

146 *Id.*

147 *See* Pressman, *supra* note 96.

148 *See* John D. McKinnon and Brody Mullins, *Google's Washington Clout Faces a Reckoning—Populist Backlash and Reaction to Russian Meddling Shake Giant*, WALL ST. J., (Oct. 31, 2017), https://www.wsj.com/articles/googles-dominance-in-washington-faces-a-reckoning-1509379625.

149 *See* H.R. 2520, 115th Cong. § 1 (2017).

150 McKinnon, *supra* note 148.

151 *See id.*

after the CRA, there is no federal statute or regulation that explicitly protects consumers' online history privacy.

II. ANALYSIS

With the repeal of the FCC privacy regulation, the prohibition on issuance of a substantially similar regulation, and the evident intransigence of Congress, consumers are again left to fend for themselves on online privacy issues. Fortunately for consumers, the executive and legislative branches do not on their own make up the Federal Government.[152] The judicial branch has the ability to, at least partially, fill this gap in consumer privacy.[153] Applying the VPPA to ISPs is where courts can start in a modern effort to build and enforce consumer privacy rights.

This would not be the first time the judiciary has led on the issue of consumer privacy, so courts should feel confident ruling to advance consumer privacy rights.[154] In the late 1960s and the 1970s, the Supreme Court issued a series of privacy-related opinions, including *Katz v. United States*,[155] *Stanley v. Georgia*,[156] and *Whalen v. Roe*.[157] It was not until the late 1970s and the 1980s—after these Supreme Court opinions—that Congress passed a flurry of legislation on privacy in response to growing consumer awareness of the issue.[158] This era included the Privacy Protection Act of 1980,[159] the Cable Communica-

---

152 *See* U.S. CONST, Art. III.

153 *See* 18 U.S.C.A. § 2710 (West 2013).

154 *See, e.g.*, Whalen v. Roe, 429 U.S. 589, 605 (1977) (discussing the duty to protect data collected for public purposes from unwarranted disclosure "arguably has its roots in the Constitution"); Stanley v. Georgia, 394 U.S. 557, 565, 568 (1969) (holding that possessing obscene material in a private home is not a crime but rather falls under an individual's First Amendment free speech rights); Katz v. United States, 389 U.S. 347, 358-59 (1967) (holding a warrantless wiretap of a payphone was an unconstitutional search and seizure). The Roberts Court has already begun leading the way on privacy issues again through its decision in *Carpenter v. United States*, 138 S. Ct. 2206, 2219-20 (2018).

155 389 U.S. 347 (1967).

156 394 U.S. 557 (1969).

157 429 U.S. 589 (1977).

158 *See* S. REP. NO. 100-599, at 2-4 (1988), *as reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4342–1-4.

159 42 U.S.C.A. § 2000aa (West 2013).

tions Policy Act of 1984,[160] the Electronic Communications Privacy Act of 1986,[161] and, of course, the VPPA in 1988.[162]

The VPPA's statutory definitions, as well as past circuit court decisions interpreting the VPPA, show that the VPPA can logically cover data accumulated through the relationship between a customer and an ISP. The definitions of video service provider, consumer, and PII each can be applied to ISP customer data, based on the plain meaning of the statute or circuit court statutory interpretation.

In the statute, "video tape service provider" is defined as "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials."[163] Two aspects of this definition are relevant. First, the type of material covered. In *Hulu*, the United States District Court for the Northern District of California held that Hulu was a video tape service provider under the VPPA because the phrase "similar audio visual material" includes streaming digital video.[164] It noted that the legislative history demonstrated that the VPPA reflected "Congress's concern with protecting consumers' privacy in an evolving technological world," so it felt comfortable extrapolating the legislative intent to cover internet videos.[165] Since then, no other significant VPPA case has even bothered to contest that the VPPA covers internet video in general.[166] Because ISPs also allow customers to view the types of internet videos at issue in *Hulu*, material provided by ISPs can be covered by the VPPA based on the *Hulu* court's holding.

The second aspect of the video service provider definition in the VPPA that is relevant is whether an ISP engages in "rental, sale, or delivery" of videos.[167] The significant VPPA court cases have not spe-

---

160 Cable Communications Policy Act, Pub. L. No. 98-549 (codified as amended in scattered sections of 47 U.S.C.).

161 18 U.S.C.A. § 2511 (West 2013).

162 18 U.S.C.A. § 2710 (West 2013).

163 18 U.S.C.A. § 2710(a)(4) (West 2013).

164 *See In re* Hulu Privacy Litig., No. C 11-03764 LB, 2012 WL 3282960, at *6 (N.D. Cal. Aug. 10, 2012).

165 *Id.*

166 *See, e.g.*, Eichenberger v. ESPN, Inc., 876 F.3d 979 (9th Cir. 2017); *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262 (3d Cir. 2016); Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482 (1st Cir. 2016); Ellis v. Cartoon Network, Inc., 803 F.3d 1251 (11th Cir. 2015).

167 18 U.S.C.A. § 2710(a)(4) (West 2013).

cifically addressed whether the mobile apps or online video streaming websites involved in litigation "deliver" the videos, but seem to have assumed that they do.[168] In the case of an ISP, it is directly in charge of delivering the video to a customer's device.[169] When a customer attempts to access a webpage, the ISP takes the device's request to go to a webpage and contacts that webpage.[170] The webpage gives the ISP the proper connection information, which the ISP then returns to the customer's device that initially requested the webpage.[171] This exchange between the ISP, the customer, and the website fits squarely into Merriam-Webster's definition of "deliver": "to take and hand over to or leave for another."[172] Therefore, through both process and content, ISPs are video service providers as defined under the VPPA.

Regarding the consumer aspect of the VPPA, the statute identifies "consumer" as "any renter, purchaser, or subscriber of goods or services from a video tape service provider."[173] "Subscriber" is the part on which courts disagree most and what impacts ISPs, as many people pay a monthly fee to an ISP to gain internet access.

Both *Yershov* and *Ellis* considered what constitutes a subscriber when reviewing free mobile app downloads and provided different analyses on what type of commitment or relationship between a customer and the app must exist in order for the customer to be deemed subscribed.[174] However, their discussions revolved around what non-monetary elements may exist.[175] Both courts indicated that, although a monetary commitment is not necessary, money plus an indication of more than a single transaction of payment would demonstrate that an individual is a subscriber, and thus a consumer, under the VPPA.[176] Because many customers pay money—normally an ongoing monthly

---

168 *See, e.g.*, Eichenberger v. ESPN, Inc., 876 F.3d 979 (9th Cir. 2017); *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262 (3d Cir. 2016); Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482 (1st Cir. 2016); Ellis v. Cartoon Network, Inc., 803 F.3d 1251 (11th Cir. 2015).

169 *See* Tim Fisher, *Internet Service Provider (ISP)*, LIFEWIRE (Aug. 4, 2017), https://www.lifewire.com/internet-service-provider-isp-2625924.

170 *See id.*

171 *See id.*

172 *Deliver*, MERRIAM-WEBSTER.COM, https://www.merriam-webster.com/dictionary/deliver (last visited Jan. 2, 2018).

173 18 U.S.C.A. § 2710(a)(1) (West 2013).

174 *See* Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 487-88 (1st Cir. 2016); Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1255-57 (11th Cir. 2015).

175 *See id.*

176 *See id.*

fee—to their ISP, ISP customers logically fall under the VPPA's definition of consumers by being subscribers under the statute.

This parallel between content streaming providers challenged under the VPPA, such as those in *Hulu*, *Ellis*, *Yershov*, and *Nickelodeon*, among others, and ISPs becomes even stronger in reviewing more of the First Circuit's reasoning in *Yershov* surrounding what constitutes a subscriber:

> Our conclusion is further informed by positing a non-electronic version of the electronic relationship between Yershov and Gannett. Imagine that Gannett had installed a hotline at Yershov's home, for free, allowing him to call Gannett and receive instant delivery of videos in exchange for his name and address, and he then used the hotline over the course of many months to order videos. We doubt that Congress would have intended that Gannett would have been free in such a scenario to publish Yershov's PII . . . .[177]

The "hotline" description that the court provided is strikingly similar to how an ISP brings videos to a device.[178]

The final relevant definition for ISPs in the VPPA is PII. In the statute, PII means "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."[179]

In *Nickelodeon*, the Third Circuit held that the "static digital identifiers" at issue in the case, including an IP address, a browser fingerprint, and a unique device identifier, were not PII under the VPPA because they could not be used by the "average person" to identify a specific individual.[180] The Ninth Circuit explicitly adopted this interpretation as well in *Eichenberger*.[181]

In contrast, the First Circuit in *Yershov* did find that PII under the VPPA was inappropriately revealed to a third party.[182] There, the app revealed a user's list of videos viewed, his GPS coordinates when the video was viewed, and the IP address of his viewing device.[183] The court held that Gannett, the app owner, had shared the information

177 *Yershov*, 820 F.3d at 489.
178 *See* Fisher, *supra* note 169.
179 18 U.S.C.A. § 2710(a)(3) (West 2013).
180 *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 281-82 (3d Cir. 2016).
181 *See* 876 F.3d 979, 985 (9th Cir. 2017).
182 *See* Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 486 (1st Cir. 2016).
183 *Id.* at 484.

with Adobe Analytics, the third-party analytics firm, knowing that Adobe Analytics could link that data to a specific individual.[184] Because of this, Gannett had shared PII as defined by the VPPA.[185]

This relationship between a video content source and a third-party data analytics firm in *Yershov* and *Nickelodeon* is the same type of relationship that ISPs can develop with third-party data analytics firms.[186] The Third and Ninth Circuits claim that their reasoning is consistent with the First Circuit's holding in *Yershov*, so PII interpretation under either holding should lead to the same results.[187] Nevertheless, these circuits would not likely find ISP-held data—such as IP address and viewing history—to be PII, as these data points are, in the courts' interpretation, beyond what a casual searcher could use to link the data to a specific person.[188] Instead of relying on this narrower interpretation of PII from the Third Circuit, courts should follow the First Circuit's reasoning in *Yershov* to find that the data that ISPs have on customers is covered under the VPPA.[189]

In *Yershov*, the First Circuit found that there was a breach of PII, but acknowledged that there are situations where the shared online data is "too uncertain" to be connected to a specific person and thus not PII under the VPPA.[190] The Third Circuit claimed that this was the situation in *Nickelodeon* because the information shared did not include GPS coordinates, unlike the shared data in *Yershov*.[191] It believed that the remaining data at issue in *Nickelodeon* did not qualify because an average person could not link the information to a specific person.[192] Despite the Third Circuit's statement on consistency with the First Circuit, this misinterprets the First Circuit's definition of PII in *Yershov*.[193] There, the court analyzed the data as PII based on whether linking the information to a specific individual was "both firm and readily foreseeable" to the party using or sharing the informa-

184 *Id.* at 486.

185 *Id.*

186 *See* Gillula, *supra* note 97.

187 *See* Eichenberger v. ESPN, Inc., 876 F.3d 979, 985-86 (9th Cir. 2017); *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 289 (3d Cir. 2016).

188 *See In re Nickelodeon*, 827 F.3d at 281-83.

189 *See Yershov*, 820 F.3d at 486.

190 *Id.*

191 *See In re Nickelodeon*, 827 F.3d at 289.

192 *See id.*

193 *See Yershov*, 820 F.3d at 486.

tion.[194] That was the case in both *Yershov* and *Nickelodeon*, as linking data with individuals was the entire purpose of sharing the data with the third-party analytics company.[195] That linking is also the reason that an ISP would share customer data with a third-party analytics company.[196] Therefore, the First Circuit's understanding of PII in *Yershov* would also cover data shared by ISPs.

Congressional intent also firmly aligns with extending the VPPA to ISPs. The goal of the VPPA was to protect any list of private viewing habits away from public consumption.[197] As Representative Al McCandless stated during a hearing on the VPPA, "[Congress has] a gut feeling that people ought to be able to read books and watch films without the whole world knowing."[198] During the congressional debate on the VPPA, Senator Patrick Leahy warned, as computers became more prevalent: "it would be relatively easy at some point to give a profile of a person . . . I think that is wrong . . . and I think it is something that we have to guard against."[199] Later, Senator Leahy added that "the trail of information generated by every transaction" is a "more subtle and pervasive form of surveillance."[200] Senator Chuck Grassley believed that the VPPA would "give specific meaning to the right of privacy, as it affects individuals in their daily lives."[201]

In light of this legislative history, the VPPA's statutory language, and previous VPPA court interpretation, courts should extend the VPPA to cover customers' data privacy with ISPs. Although extending the VPPA to ISPs cannot take the place of the FCC's 300 plus page regulation, it can bring back some baseline protections that the regulation tried to institute.[202] First, the VPPA can require ISPs to obtain customer consent for data disclosures—including IP address and browsing history—in a clear, separate form from the rest of the terms and conditions that ISPs set forth.[203] This is not as extensive as

---

194 *Id.*

195 *See In re Nickelodeon*, 827 F.3d at 269-70; *Yershov*, 820 F.3d at 484-85.

196 *See* Gillula, *supra* note 97.

197 *See* S. REP. NO. 100-599, at 5-6 (1988), *as reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4342-5-6.

198 *Id.* at 7, *as reprinted* at 4342-7.

199 *Id.* at 5-6, *as reprinted* at 4342-5-6.

200 *Id.* at 6, *as reprinted* at 4342–7.

201 *Id.*

202 *See* 18 U.S.C.A. § 2710 (West 2013); *In re* Protecting the Privacy of Customers of Broadband & Other Telecomms. Servs., 31 FCC Rcd. 13911, 13914-5 (2016).

203 *See* 18 U.S.C.A. § 2710(b)(2) (West 2013).

the opt-in/opt-out policies under the former FCC rule, but it does provide a mandatory minimum of consent.[204]

Next, there are several time-related restrictions on data disclosure through the VPPA.[205] It ensures that data-sharing consent cannot be given forever, but must expire at least every two years, so that consumers must again be made aware that they are consenting to data disclosure.[206] Additionally, the VPPA also gives consumers the right to withdraw from consent to ISP data sharing at any time.[207] By applying the VPPA to ISPs, there will also be a limit on the length of time the ISPs can keep customer data before destroying it, helping to decrease the security risk to customers if a hacker gains access to the data trove.[208]

Finally, the VPPA provides real consequences for ISP violations, particularly if a class action is brought under the VPPA.[209] There are actual damages of at least $2,500 and possible punitive damages, plus fees and other costs that a plaintiff can win in a lawsuit.[210] This motivation may encourage ISPs to both respect and protect customer data, as a hack could easily lead to much larger actual damages. Although nowhere near perfect, by applying the VPPA to ISPs, courts can make some progress towards protecting consumer data on the internet.

CONCLUSION

The VPPA came about after a reporter tracked down Judge Bork's video rental history.[211] The reporter did this because, even in 1987, consumer privacy was an actively discussed issue during the Supreme Court confirmation, as "Bork was a strict constitutionalist and generally did not believe that individuals were guaranteed privacy protections beyond those specifically outlined in legislation."[212] In the modern technology era, there is a gap in consumer privacy rights. After the FCC's privacy rule was overturned by the CRA, it seemed

204 *See* 18 U.S.C.A. § 2710 (West 2013)(b)(2)(B); *In re* Protecting the Privacy of Customers of Broadband & Other Telecomms. Servs., 31 FCC Rcd. 13911, 13914 (2016).

205 *See* 18 U.S.C.A. § 2710(b)(2)(B), (e) (West 2013).

206 *See* 18 U.S.C.A. § 2710(b)(2)(B)(ii)(II) (West 2013).

207 *See* 18 U.S.C.A. § 2710(b)(2)(B)(iii) (West 2013).

208 *See* 18 U.S.C.A. § 2710(e) (West 2013).

209 *See* 18 U.S.C.A. § 2710(c) (West 2013).

210 *Id.*

211 *See* S. REP. NO. 100-599, at 5 (1988), *as reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4342-5.

212 Peterson, *supra* note 1.

as though there were minimal online data consumer privacy rights.[213] Fortunately, this Comment's analysis shows that courts can plausibly and should hold that the VPPA covers customer data collected by ISPs, ensconcing consumer online privacy rights in already-existing legislation. The statute's plain meaning reflects that the process by which an ISP provides a video to a customer makes the ISP a "video tape service provider." The content that an ISP provides also qualifies it as a "video tape service provider," based on the prior court interpretation of this phrase in *Hulu*.[214] Additionally, applying the legal analysis of a VPPA "consumer" put forth in *Yershov* and *Ellis* demonstrates that an ISP user is a subscriber, and thus a consumer, under the VPPA.[215] Finally, the First Circuit's interpretation of PII under the VPPA in *Yershov* could apply to the data that ISPs store and share with third parties.[216] The VPPA is by no means a perfect substitute for regulations such as the FCC's 2016 rule to protect privacy. However, it can provide a foundation of online browsing data privacy until Congress or regulators act in this space again. Although they did not impact his Supreme Court nomination, Judge Bork's video viewing habits can still have an impact for millions of Americans today.

---

213 *See In re* Protecting the Privacy of Customers of Broadband & Other Telecomms. Servs., 31 FCC Rcd. 13911 (2016); Pub. L. No. 115-22, 131 Stat 88.

214 *See In re* Hulu Privacy Litig., No. C 11-03764 LB, 2012 WL 3282960, at *6 (N.D. Cal. Aug. 10, 2012).

215 *See* Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 487-88 (1st Cir. 2016); Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1255-57 (11th Cir. 2015).

216 *See Yershov*, 820 F.3d at 486.