Uncertainty Surrounding the Repeal of the Internet Privacy Rules

ISHA SRIVASTAVA *

I. INTRODUCTION

The concept of personal privacy is a fundamental right that dates back to the beginning of common law. During a time when technology was being newly integrated into society, Samuel Warren and Louis Brandeis recognized the basic right, "to be let alone."[1]

A newer technology, the Internet, is a critical tool for consumers because it provides society with access to endless amounts of information by serving as an online conduit for commerce, communication, education, and entertainment.[2] But with the incessant desire to connect online, how does one retain the ability to preserve one's online anonymity? In an age where everyone is constantly concerned about whether they can connect to Wi-Fi, the ability for individuals to preserve a certain amount of online anonymity is an essential dimension to logging online. With every mouse click that a web user makes online, a digital footprint that contains valuable personal information is left unsecured for corporations or third-parties to use for virtually unrestricted purposes.

Thus, the broadband service providers which charge subscribers to connect them to the virtual realm, acquire more than just consumer business in the process. Service providers obtain an exclusive behind-the-scenes peek into a user's web traffic history, which allows them to paint a picture of the consumer and have access to personal information that edge providers, such as Google or Facebook, do not have.

A consumer's service provider already has access to personal information, including one's name, address, and other type of personally identifiable information simply obtained through the process of signing up to get online.[3] It knows which websites one visits and records the time spent on the

* Isha Srivastava graduated with a Biomedical Engineering degree from the University of the Pacific in 2013 and earned her law degree, with an Intellectual Property & Technology Law Certificate, from the University of San Francisco School of Law in 2018. Isha would like to thank her parents for their continuous love and support, and she would like to pass her heartfelt gratitude to Dean Susan Freiwald for the guidance and encouragement provided in researching and writing this article.

1. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

2. *See* Protecting and Promoting the Open Internet, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601, 5603 (Mar. 12, 2015), https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf [https://perma.cc/4FA5-72FV].

3. Kieren McCarthy, *Your Internet History On Sale to Highest Bidder: U.S. Congress Votes To Shred ISP Privacy Rules*, THE REGISTER (Mar. 28, 2017), https://www.theregister.co.uk/2017/03/28/congress_approves_sale_of_internet_histories/ [https://perma.cc/WN58-DJDU].

website.[4] Over time, service providers are able to collect an abundance of a user's online information that third parties, such as advertisers are eager to acquire.[5] As a result, service providers monetize personal information while third parties capitalize on it.

In a 2016 effort to safeguard online user history, the Federal Communications Commission ("FCC"), under a Democratic administration, drafted Internet Privacy Rules that would have required service providers to offer their consumers the fundamental privacy protections of transparency, choice, and security.[6] These Internet Privacy Rules required broadband providers to obtain user consent and inform users about the privacy policies that were scheduled to take effect in December 2017.

However, the 2016 election changed the fate of consumer privacy. Previously, democratic President Barack Obama had appointed a member of the Democratic Party to head the FCC, which recognized the basic need for online user privacy and ultimately adopted the Internet Privacy Rules.[7]

However, the FCC's priorities drastically changed when President Donald Trump took office and nominated a Republican as the new chairman of the FCC. Further, a new controlling party within the FCC whose priorities often times differed from the commission's previous concerns emerged. The newly Republican-controlled FCC dismantled the 2016 privacy rules within months, ultimately permitting service providers to dive deep into the pockets of consumer online histories once again.

This paper will explore the history of federal Internet Privacy Rules from its original intentions to its controversial demise. The first section of this paper will examine the privacy rules in detail by analyzing the history of administrative authority over regulation of the Internet. The second section will study the repeal of the 2016 drafted privacy rules and what impact the 2016 election had on privacy protection. Finally, the departing section will explore privacy protection mechanisms moving forward that can achieve similar effects to those the 2016 Internet Privacy Rules would have accomplished.

4. *Id.*

5. Kari Paul, *Your Browser History Can Now Be Sold To Advertisers Without Your Consent*, MARKETWATCH (Apr. 2, 2017), https://www.marketwatch.com/story/your-browser-history-could-soon-be-sold-to-advertisers-without-your-consent-2017-03-28 [https://perma.cc/D9MB-PMEP].

6. *See* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, Notice of Proposed Rulemaking, 31 FCC Rcd. 2500 (Apr. 1, 2016).

7. Brooks Boliek, Alex Byers, and Bill Duryea, *The FCC Chair's Internet Pivot*, POLITICO PRO (Feb. 2, 2015), https://www.politico.com/story/2015/02/tom-wheeler-net-neutrality-114785 [https://perma.cc/N96P-TPQ9].

II. THE HISTORY OF THE FEDERAL INTERNET PRIVACY RULES

A. THE EVOLUTION OF FCC AUTHORITY OVER REGULATION OF DATA PRIVACY LAWS

Over the decades, the Internet has evolved from an unknown terrain into the key means individuals use to connect with one another in our high-tech society. As technology continues to be easily accessible to users, regulation becomes necessary to protect consumers, who unknowingly offer personal information with every mouse-click. Currently, the FCC has jurisdiction over broadband service providers, and will continue to have jurisdiction unless Internet Service Providers ("ISPs") are considered to be outside the agency's jurisdiction.[8]

The Radio Act of 1912 ("1912 Radio Act") allowed the United States Department of Commerce and Labor to regulate communications so that groups, including the military, emergency responders, police, and entertainment companies, could transfer signals to their targeted audiences through public or commercial airwaves.[9] The purpose of the 1912 Radio Act was to minimize radio frequency interference in order for the government to receive potential distress signals and to maintain clear pathways for signals that communicated important messages to the government.[10] The Act made it illegal for anyone to transmit radio frequencies for broadcasting purposes without a government-approved license. The appellate court in *Hoover v. Intercity Radio Co., Inc.* determined that Commerce Secretary, Herbert Hoover, could not refuse to renew a company's license if all the requirements for obtaining a radio license were satisfied.[11] The Secretary of Commerce was essentially obliged to issue radio licenses to citizens who met the Act's requirements. Consequently, almost all radio licenses were issued, causing congested airways that essentially prevented the development of commercial broadcasting.[12]

The Secretary of Commerce's federal powers were further limited when the Supreme Court, in *United States v. Zenith Radio Corporation,* found that the Secretary of Commerce also lacked the authority to specify the terms of a broadcasting license.[13] The U.S. had charged *Zenith* with violating Section 1 of the 1912 Radio Act, asserting that *Zenith* was functioning outside the parameters outlined in its license when it remained on-air at the same time as

8. Jon Brodkin, *FCC Explains How Net Neutrality Will Be Protected Without Net Neutrality Rules*, ARSTECHNICA (Dec. 11, 2017), https://arstechnica.com/tech-policy/2017/12/voluntary-net-neutrality-will-protect-consumers-after-repeal-fcc-claims/ [https://perma.cc/FQ2E-6H7Q].

9. Radio Act of 1912, Pub. L. No. 62-264, 37 Stat. 302 (1912) (repealed 1927) (providing licensing of private radio operators but not provisions for regulating them).

10. Carl Zollmann, *Recent Federal Legislation: Radio Act of 1927*, 11 MARQ. L. REV. 121, 122 (1927).

11. Hoover v. Intercity Radio Co., 286 F. 1003 (D.C. Cir. 1923).

12. *"The Public Interest Standard in Television Broadcasting,"* CURRENT (Dec. 18, 1998), https://current.org/1998/12/the-public-interest-standard-in-television-broadcasting/ [https://perma.cc/3BEX-FKSW].

13. *See* United States v. Zenith Radio Corp., 12 F.2d 614 (N.D. Ill. 1926).

another station. However, Section 2 of the Act did not stipulate how the Secretary of Commerce was to determine the hours of operation for the two competing stations.[14] The combination of the ambiguous statutory language and the inability to exercise discretion for regulating licenses left the Secretary of Commerce with little authoritative power.[15]

With broadcasters left unregulated with limited number of available radio frequencies, the 1912 Radio Act did not accommodate for the growing telecommunications industry. Also, free speech advocates argued that all broadcasters should be allowed to buy airtime, and in an attempt to compromise with the public, Congress passed the Radio Act of 1927.[16] Sections 9 and 11 of the 1927 Radio Act permitted the Federal Radio Commission ("FRC") to verify that licensees served a "public interest, convenience, or necessity" when granting broadcasting licenses.[17] Since the statutory text did not clarify what requirements met the "public interest" definition, the FRC determined whether individual stations met the standard on a case-by-case basis.[18] Non-licensees were stripped of their free speech rights except for those who satisfied the subjective "public interest" requirements.[19] As a result, the few broadcasters on air held a monopoly over the scarce resource of radio frequencies.

Additionally, telephone companies lacked proper regulation since the Interstate Commerce Commission ("ICC") had little regulatory jurisdiction over interstate telephone companies and mainly focused its attention on the railroad industry.[20]

In order to have a single agency regulate interstate and foreign commerce by wire and non-wire communications, Congress passed the Communications Act of 1934 ("1934 Act") and transferred the FRC's responsibilities to the FCC, a new agency.[21] The 1934 Act was meant to preserve the government's commitment to providing the public with access to local telephone services at affordable rates.[22] The FCC was responsible for regulating all media technologies such as "telephone, telegraph, and radio communications."[23] The new regulations "established regulatory standards for various types of communications, including Title I services, which are subject to

14. *Id.*

15. *Id.*

16. Stuart N. Brotman, *Revisiting The Broadcast Public Interest Standard In Communications Law and Regulation*, BROOKINGS (Mar. 23, 2017), https://www.brookings.edu/research/revisiting-the-broadcast-public-interest-standard-in-communications-law-and-regulation/ [https://perma.cc/UMR3-K7EU].

17. The Radio Act of 1927, Pub. L. No. 69-632, 44 Stat. 1162 (repealed 1934).

18. *See* Brotman, *supra* note 16.

19. *Id.*

20. *See* Daniel F. Spulber and Christopher S. Yoo, *Toward a Unified Theory of Access to Local Telephone Networks*, 61 FED. COMM. L.J. 41 (2008).

21. *Communications Act of 1934*, ROOSEVELT INSTITUTE (Sept. 1, 2010), http://rooseveltinstitute.org/communications-act-1934/ [https://perma.cc/5XVJ-6XKS].

22. Ev Ehrich, *A Brief History of Internet Regulation*, PROGRESSIVE POLICY (March 2014), http://www.progressivepolicy.org/wp-content/uploads/2014/03/2014.03-Ehrlich_A-Brief-History-of-Internet-Regulation1.pdf [https://perma.cc/GK7G-DJHP].

23. The Communications Act of 1934, 47 U.S.C. §151, et seq. (1934).

looser restrictions, and Title II services, which fall under more rigorous 'common carrier' rules and intend to protect equal access to these networks."[24]

To ensure the laws stayed current with technological advancements, the Telecommunications Act of 1996 ("Telecommunications Act") was passed during the Clinton administration to restructure the electronic communications market.[25] The Telecommunications Act codified telephone systems as telecommunication services, while broadband systems were classified as information services.[26] The Act ultimately covered five major areas of telecommunication markets: (1) telephone services; (2) telecommunications equipment manufacturing; (3) cable television; (4) radio and television broadcasting; and (5) Internet and online computer services. When the Telecommunications Act was passed, telecommunications services were considered to primarily be telephone systems according to the 1934 Communications Act.[27] Also at the time, "information services" were considered to include cable and broadband services because companies intended to use dial-up services for private data networks to link computer systems to one another.[28] Broadband, otherwise known as "high-speed" Internet access, allowed users to connect to the worldwide web by using satellite technologies that send and receive data at high volumes and speeds.[29] Broadband services were treated as an information service because of their ability to store, transform, retrieve, and utilize information through telecommunications, as defined in the Telecommunications Act. Unlike traditional telecommunications, which operated under tougher regulations, "information services" were excluded from common carrier regulations.

In essence, the Telecommunications Act was enacted under the Clinton administration to foster fair competition within the telephone industry and the Internet separately because the two fields were not anticipated to merge into one industry at that point in time.[30] However, as technology continued to advance, the telephone service sector and the Internet access sector eventually became interwoven industries causing inconsistencies for how each component was governed under the Telecommunications Act.[31] The line drawn between information services and telecommunications carriers was a blurred one, and ISPs were still considered to be a deregulated information services.[32] In 2015, the FCC reclassified broadband Internet access as a "telecommunications service," which held ISPs to standards under Title II of the

24. *See* United States v. Zenith Radio Corp., 12 F.2d 614 (N.D. Ill. 1926).

25. David Mccabe, *Bill Clinton's Telecom Law: Twenty Years Later*, THE HILL (Feb. 7, 2016), http://thehill.com/policy/technology/268459-bill-clintons-telecom-law-twenty-years-later [https://perma.cc/RC62-XERT].

26. *See* Ehrich, *supra* note 22.

27. *Id.*

28. *See* Ehrich, *supra* note 22.

29. ANGELE A. GILROY AND LENNARD G. KRUGER, CONG. RESEARCH SERV., RL33542, BROADBAND INTERNET REGULATION AND ACCESS: BACKGROUND AND ISSUES 2 (2008).

30. *Id.* at 5.

31. *Id.* at 7.

32. *Id.*

Telecommunications Act that would essentially protect customers against "unjust or unreasonable" practices.[33] Title II was initially intended for the regulation of telephone service companies, which extended to wireless carriers and furnished the FCC with authorization to regulate broadband Internet access service as a common carrier as a result of the 2015 Open Internet Order (the Order).[34] Previously, the Federal Trade Commission ("FTC") was in charge of regulating service providers until the reclassification of ISPs as common carriers.[35]

Since this reclassification of ISPs as a telecommunication service, there has been much debate over which agency should regulate online privacy issues.[36] Traditionally, the FTC has held enforcement authority over the entire consumer market place with the exception of common carriers, which are treated as public utilities.[37] Supporters of the repeal of the privacy rules argue that the FTC should regain jurisdiction over ISP privacy because the FTC is the nation's expert agency in privacy and has particularized experience in dealing with data security practices.[38] Section 5 of the Federal Trade Commission Act ("FTCA") allows the FTC to regulate persons who engage in "unfair or deceptive acts or practices in or affecting commerce," which grants the FTC a conditional general jurisdiction over ISPs.[39] The FTC cannot directly regulate ISPs unless their practices are unfair, deceptive, or fraudulent. Section 5(n) of the FTCA acts as an additional barrier to determining whether an act is "unfair" because public policy considerations for whether a practice causes substantial injury to consumers, which is not reasonably avoidable by consumers themselves, cannot be the only reason for deeming a practice unfair.[40]

However, the historical development of regulation over telecommunications demonstrates Congress's intent to have the FCC govern communication infrastructures that serve as common carriers. The FCC will continue to have jurisdiction over broadband service providers as long as ISPs are categorized as common carriers under Title II of the 1996 Act.

33. Stan Adams, *Un-Title II-ed: What Reclassification Means*, CDT (May 5, 2017), https://cdt.org/blog/un-title-ii-ed-what-reclassification-means/ [https://perma.cc/3HM7-SGUR].

34. *Summary of the FCC's Open Internet Order*, Subsentio, http://www.subsentio.com/summary-of-the-fccs-open-internet-order/ [https://perma.cc/J9LJ-SSA5] (last visited Sept. 18, 2019).

35. Amir Nasr, *Roles of FTC, FCC Are Front and Center in a Privacy Debate*, MORNING CONSULT (Sept. 27, 2016), https://morningconsult.com/2016/09/27/roles-ftc-fcc-front-center-privacy-debate/ [https://perma.cc/M8JP-AYMB].

36. *Id.*

37. Jedidiah Bracy, *FTC Officials Concerned About Jurisdiction After FCC Net Neutrality Order*, IAPP THE PRIVACY ADVISOR (Mar. 10, 2015), https://iapp.org/news/a/ftc-officials-concerned-about-jurisdiction-after-fcc-net-neutrality-order/ [https://perma.cc/4ESX-GRKE].

38. Kate Kaye, *FTC Could Regain Privacy Oversight, But It Won't Be Easy*, ADAGE (Mar. 30, 2017), http://adage.com/article/privacy-and-regulation/ftc-regain-isp-privacy-oversight-easy/308487/ [https://perma.cc/2REP-A86S].

39. 15 U.S.C §45 (1970).

40. Harold Feld, *No, The FTC Cannot Have A Ban On All ISP Blocking*, PUBLIC KNOWLEDGE (Dec. 12, 2017), https://www.publicknowledge.org/news-blog/blogs/no-the-ftc-cannot-have-a-ban-on-all-isp-blocking [https://perma.cc/H9TZ-F6FZ].

B. BACKGROUND OF THE PRIVACY RULES AND A BREAKDOWN OF THEIR REPEAL

Whether US laws were not caught up to technology due to the agency reclassification regarding the regulation of the Internet or due to the accelerated development of the Internet, ISPs were mainly left unregulated. The next subsection will discuss the primary motive for the 2016 Internet Privacy Rules, and the subsequent subsection will delve into what the privacy rules would have accomplished had the repeal not occurred. The final subsection will dissect the repeal procedurally.

1. Need for and Purpose of the FCC's Privacy Rules

ISPs such as Verizon, Comcast, and AT&T serve as a consumer's "on-ramp" to the Internet and handle all of the consumer's network traffic.[41] Accordingly, ISPs have access to sensitive consumer information such as browser history, app usage, geo-locations, health information, social security number, and miscellaneous financial information. An overwhelming 85% of popular websites with topics varying from health, news, and shopping do not encrypt browsing by default.[42] As a result, consumers' search inquiries, which range from health ailments to personal product searches, are left exposed to ISPs who can view both the full website Universal Resource Locator ("URL") as well as the specific browsing content on each individual webpage.[43]

Websites and service providers are able to capitalize on consumer browsing history through different mechanisms. Even if the user data is not sold to third parties, companies may utilize online consumer profiles to advance their own interests. For example, representatives from AT&T, Comcast, and Verizon may use or distribute personal data for their own purposes to advance their respective businesses.[44] In light of the repeal of the rules, Comcast has assured its customers that it will not sell individual web browsing history.[45] Nevertheless, this does not mean that Comcast will abstain from conveying personalized ads based on its customers' browsing history. Moreover, the current practice of refraining from selling personal user data could be changed at a company's will, which leaves consumers at the mercy of their providers.

41. Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, Rules and Regulations, 47 CFR 87274 (Dec. 2, 2016).

42. Aaron Rieke, David Robinson and Harlan Yu, *What ISPs Can See*, UPTURN (March 2016), https://www.teamupturn.org/reports/2016/what-isps-can-see [https://perma.cc/XBN3-29TQ] ("This report is designed to provide technical grounding for policymakers and other interested parties, regarding the extent of ISP visibility into the activities of their subscribers." This was supported by the Media Democracy Fund.).

43. *Id.*

44. *Can ISPs Sell Your Data?*, LE VPN BLOG (Nov. 6, 2017), https://www.le-vpn.com/can-isps-sell-data/#respond [https://perma.cc/MH27-QW68].

45. Jon Brodkin, *Comcast: We Won't Sell Browser History, And You Can Opt Out Of Targeted Ads*, ARSTECHNICA (Mar. 31, 2017), https://arstechnica.com/tech-policy/2017/03/comcast-we-wont-sell-browser-history-and-you-can-opt-out-of-targeted-ads/ [https://perma.cc/SCE5-LPYF].

ISPs sell consumer information to third parties such as advertisers, who then target consumers with personalized advertisements that are based on previous searches that were thought to be private.[46] ISPs are able to gather sensitive information regardless of whether websites use encryption by Hyper Text Transfer Protocol Secure ("HTTPS") or use unencrypted Hyper Text Transfer Protocol ("HTTP").[47] Unencrypted websites show all the data transferred between the user and the website in plaintext.[48] The encrypted HTTPS page uses Transport Layer Security ("TLS") to establish a "meeting of the minds" between the user and the website to exchange encryption keys, and assures a protected connection.[49] When a website uses HTTPS to send data between the browser and the website, the ISP cannot see the URL or the content on the page.[50] This means that ISPs have limited access to detailed search information but can still see the domain names of the URL. Searches through the Domain Name System ("DNS") are usually not encrypted and are translated into a corresponding Internet Protocol ("IP") address, which the user's computer requests from the website.[51] Consequently, the user's computer sends a DNS request about the specific domain name, which can be equivalent to revealing the name of a city rather than a specific home address within that city.

However, encryption does not act as a privacy silver bullet. ISPs can indirectly use the encrypted Internet traffic to examine the size, timing, and destination of the encrypted information to narrow the possibilities of information exchanged and possibly the websites visited.[52] Even though the actual website content is shielded from ISPs, the domain name and the time spent on the website are enough to create a user profile. For example, if an ISP monitors a user who is logging onto self-help healthcare websites and food blogs, the ISP may categorize this consumer as health conscious and create a general profile based on those findings. Long-term online use allows ISPs to infer the hidden content of the webpage, which is intrusive and a threat to user privacy.

Moreover, consumers who use their mobile devices to go online do not evade detection by ISPs. As more consumers rely on their mobile devices to connect to the Internet, ISPs may use the cellular website interactions to generate innovative consumer profiles that are still beneficial to third parties.[53]

46. Olivia Solon, *Your Browsing History May Be Up For Sale Soon. Here's What You Need To Know*, THE GUARDIAN (Mar. 28, 2017), https://www.theguardian.com/technology/2017/mar/28/internet-service-providers-sell-browsing-history-house-vote [https://perma.cc/SD5A-9FJ3].

47. Aazean, *What Exactly Can Your ISP See When You Surf The Web*, BOLEHVPN (July 22, 2017), https://blog.bolehvpn.net/what-exactly-can-your-isp-see-when-you-surf-the-web/ [https://perma.cc/9EHH-NSFC].

48. *Id.*

49. *Id.*

50. *See* Bracy, *supra* note 37.

51. *Id.*

52. *Id.*

53. *Id.*

ISPs, thus, have access to user information from the moment users log on to the moment they log off. In the process, ISPs gain insight into users' online browsing habits and may choose to sell the information to third parties who can exploit consumers through targeted advertisements. With private consumer history left unprotected and accessible to ISPs, consumers need to be able to make informed decisions about their online privacy.

2. What Would the Privacy Rules Have Accomplished Had They Not Been Repealed?

After the reclassification of ISPs as common carriers in the 2015 Open Internet Order, the FCC recommended that traditional privacy laws be applicable to the regulation of "broadband Internet access services" ("BIAS").[54] When using the Notice of Proposed Rulemaking to draft regulations for BIAS, the FCC heavily relied on the FTC's best practices and the Consumer Privacy Bill of Rights ("CPBR").[55] In 2016, the FCC issued a final Report and Order promoting the rules for ISP regulation. The following section will explore the distinct online forms of personal information the privacy rules were meant to protect in addition to the effects on consumer privacy had the privacy rules been implemented.

a. Protected Information Under Section 222 of the Telecommunications Act

Section 222(a) of the Telecommunications Act stipulates that every telecommunication carrier has a duty to protect the confidential proprietary information of its customers.[56] The privacy rules aim to protect Customer Proprietary Information ("CPI") under Section 222, which is composed of three types of information that telecommunications carriers have access to such as: (1) individually identifiable Customer Proprietary Network Information ("CPNI"); (2) personally identifiable information ("PII"); and (3) communication content.[57]

The first type of CPI is CPNI in the broadband context from Section 222(h)(1) and refers to information that "relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier" as a result of a "carrier-customer relationship."[58] CPNI may include information that relates to unique identifier headers ("UIDH") as long as the information reveals technical configuration, type, destination, and amount of use of a telecommunications service.[59] In the final Report and Order of

54. Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, Notice of Proposed Rulemaking, 31 FCC Rcd. 2500, 2502 (Apr. 1, 2016).

55. *Id.*

56. 47 U.S.C. §222(a) (2008).

57. *See* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, Report and Order, 31 FCC Rcd. 13911, 13913 (Nov. 2, 2016).

58. *See* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, Notice of Proposed Rulemaking, 31 FCC Rcd. 2500, 2514 (Apr. 1, 2016).

59. *See* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, Report and Order, 31 FCC Rcd. 13911, 13930 (Nov. 2, 2016).

2016, the FCC identified a non-exhaustive list of protected information considered to be CPNI which includes: broadband service plans, geo-location, Media Access Control ("MAC") addresses and other device identifiers, IP addresses and domain name information, traffic statistics, port information, application headers, application usage information, application payload, and customer premise equipment and device information.[60] Accordingly, CPNI protection extends to the multi-step process a user takes to establish a connection to the Internet through a Transmission Control Protocol ("TCP") and Internet Protocol ("IP") system.[61]

The second type of protected CPI is PII, and refers to "any information that is linked or linkable to an individual," or "information that is reasonably linkable to an individual or device if it can be used on its own, in context, or in combination to identify an individual or device, or to logically associate with other information about a specific individual or device."[62] Examples of PII include customer contact information such as names, addresses, and phone numbers of individuals since this information is reasonably linkable to an individual or device.[63] Types of PII may also include but are not limited to social security number, date of birth, mother's maiden name, government-issued identifier, physical address, email address or other online contact information, phone number, MAC address, IP address, and unique device identifier.[64]

The third type of CPI is the communication content that refers to a nonexclusive list of "contents of emails; communications on social media; search terms; website comments; items in shopping carts; inputs on web-based forms; and consumers' documents, photos, videos, books read, [and] movies watched."[65]

An exception to protected CPI is de-identified data, which is accomplished when the service provider: (1) finds information that is not reasonably linkable to an individual or device; (2) publicly commits to maintain and use the data in a non-individually identifiable fashion or does not attempt to re-identify data; and (3) contractually ensures that any third-party entity obtaining the de-identified data does not attempt to re-identify the data.[66]

Anonymization of data is accomplished by disconnecting identifying information such as a name and a social security number; but to gain in-depth analysis of the anonymized data, the administrator may alter the identifiers

60. *Id.*

61. Chris Woodford, *The Internet*, EXPLAIN THAT STUFF (Jan. 27, 2018), http://www.explainthatstuff.com/internet.html [https://perma.cc/XGA3-QZY7].

62. *See* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, Report and Order, 31 FCC Rcd. 13911, 13944 (Nov. 2, 2016).

63. *Id.* at 13947.

64. *Id.* at 13946.

65. *Id.* at 13950.

66. *Id.* at 13952.

rather than remove the identifiable markers.[67] This allows computer programs with the ability to develop and test algorithms at rapid speeds and to detect patterns from information not categorized as PII, to re-identify anonymous data, leaving purportedly anonymous data vulnerable to whoever makes a concerted effort to unveil the truth.

In *Northwestern Memorial Hospital v. Ashcroft*, Judge Richard Posner held that anonymity and privacy were not synonymous concepts and decided that disclosing de-identified health records was still an invasion of privacy.[68] In *Northwestern*, the government sought 45 patient's de-identified medical records in relation to an abortion case, however, Judge Posner feared that "skillful Googlers" could piece together information from privileged redacted medical records to embarrass the anonymous women.[69] Because neutral information can be manipulated to re-identify anonymous data, its de-identification should not be the only reason for permitting access to sensitive data.

b. Effects of Privacy Rules Had There Been No Change in Administration

Had the privacy rules not been repealed when the administration changed in 2016, they would have required broadband service providers to obtain customer authorization before collecting their personal browsing data. The privacy rules were derived from the three historical pillars of privacy: transparency, choice, and security.[70] The new privacy rules would have required ISPs to: (1) notify customers about what types of information the ISP collects about its customers; (2) specify how and for what purposes the ISP uses and shares the information; and (3) identify the types of entities with which the ISP shares the information.[71] Such transparency would have enabled consumers to make informed decisions when selecting an ISP. For example, ISPs would have had to notify users about their use of "opt-in" and "opt-out" alternatives, which will be discussed in detail under consumer choice.

Consumer choice dictates the type of user consent needed based on the sensitivity of the information collected by the broadband provider.[72] The emphasis shifts from how consumer information is used to what the consumer's expectations of privacy are.[73] The privacy rules would have explicitly required ISPs to obtain "opt-in" consent to use and share sensitive information

67. Paul Ohm, *Broken Promise of Privacy: Responding to the Suprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1712 (2010) (noting the techniques of anonymization known as the Release-and-Forget Model).

68. Northwestern Memorial Hospital v. Ashcroft, 362 F.3d 923, 929(7th Cir. 2004).

69. *Id.*

70. *See* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, Report and Order, 31 FCC Rcd. 13911, 13918 (Nov. 2, 2016).

71. *Fact Sheet: The FCC Adopts Order to Give Broadband Consumers Increased Choice Over Their Personal Information*, FCC (Oct. 27, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DOC-341938A1.pdf [https://perma.cc/5PH2-N3SL].

72. *See* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, Report and Order, 31 FCC Rcd. 13950 (Nov. 2, 2016).

73. *Id.*

such as: (1) precise geo-location; (2) children's information; (3) health information; (4) financial information; (5) social security numbers; (6) web browsing history; (7) app usage history; and (8) content of communication information.[74] ISPs would not have been automatically authorized to access sensitive information unless the online user went into his or her preferences and manually checked the box to opt-in. Only at that point would the ISP have had access to the information detailed above.

In contrast, transmitted material that is not characterized as sensitive information, would have been subject to opt-out consent.[75] ISPs would automatically have had access to the user's non-sensitive information unless the user manually chose to "opt-out" of the preset preference. Exceptions to the consent requirements would have included billing and collection services, protecting users from fraudulent use of the provider's network, and the use and sharing of non-sensitive information to provide services marketed with the broadband service.[76]

An unintended consequence of the opt-in feature could have been the squandered opportunity to improve social welfare from an economic perspective.[77] Online users with more technological aptitude would have evaluated opt-in services and reaped the benefits of specific ISP features while technologically-challenged users would have been gradually excluded from any ISP-made improvements moving forward. The underrepresented online group of users could potentially have been deprived of their preferences, which contradicts the purpose of providing opt-in and opt-out choices.

In addition to the regulations meant to restrict ISP access to consumer information, ISPs would have been required to strengthen their security measures. Broadband service providers would have been forced to follow the FCC R&O's guideline that lists reasonable data security practices such as: (1) implementing up-to-date and relevant industry best practices; (2) providing accountability over security practices; (3) implementing customer authentication tools; and (4) properly disposing of data consistent with FTC best practices as well as the CPBR.[78] In the event that a data breach does occur, ISPs would have been required to notify: (1) affected customers of the data breach no later than 30 days after determination of breach; (2) the FCC, the Federal Bureau of Investigation, and the U.S. Secret Service of breaches that affected more than 5,000 customers no later than 7 days after determination of breach; and (3) the FCC at the same time as the customers were notified of the breach if it affected fewer than 5,000 customers.[79]

In sum, the 2016 privacy rules prioritized online consumer privacy by protecting all three types of customer proprietary information, as defined

74. *Id.*

75. *Id.*

76. *Id.*

77. Nicklas Lundblad and Betsey Maisello, *Opt-In Dystopias*, SCRIBD (Apr. 2010), https://www.scribd.com/document/30469167/Opt-in-Dystopias [https://perma.cc/MYS6-LKN8].

78. *See* FCC Fact Sheet, *supra* note 71, at 3.

79. *Id.*

under Section 222, while still maintaining the traditional pillars of privacy in its historical context.

3. Procedural Background of the Repeal of Privacy Rules

Once the Internet was reclassified as a common carrier in 2015, the FTC was not allowed to regulate Internet privacy as it previously had. In 2016, Democratic FCC chairman, Tom Wheeler, played a significant role in the passage of the Internet Privacy Rules by stressing the importance of protecting customers from broadband providers who had access to users' personal data without regulation.[80]

When President Donald Trump took office in 2017, he appointed Republican Ajit Pai as FCC chairman who lobbied for dismantling the privacy rules. Republicans, with a 3-2 majority in the FCC, combined forces with the Republican House of Representatives and Republican Senate to repeal the Internet Privacy Rules. In April of 2017, President Trump exercised his executive power to accept the proposed repeal.[81]

Congress repealed the Internet Privacy Rules using the Congressional Review Act of 1996 ("CRA"), permitting Congress to negate regulations previously approved by federal agencies. After the rule in question is delivered to Congress, the Senate has the option to exercise the procedure for up to 60 days under this Act.[82] An advantage of using the CRA is that the regulation will not be allowed to go into effect, and, further, the agency that initially issued the rule may not create a substantially similar rule without Congress passing a new law.

Prior to the repeal of the Internet Privacy Rules, Congress had used the CRA only once in 20 years under the Bush administration to overturn a regulation that the Clinton administration had approved.[83] Since the CRA forbids reissuing a rule that is substantively similar to the old rule without Congressional action, the FCC will not be able to reissue a rule that requires ISPs to obtain permission from consumers before using their personal sensitive information.

C. OVERVIEW AND MOVING FORWARD

With the FCC currently in charge of broadband service providers, it has limited power over privacy regulations as a result of the repeal. Users will

80. Jim Puzzanghera, *New Rule: Internet Providers Must Ask You Before Sharing Your Sensitive Personal Data*, LOS ANGELES TIMES (Oct. 27, 2016), https://www.latimes.com/business/la-fi-internet-privacy-fcc-20161027-story.html [https://perma.cc/D462-HMXL].

81. David Shepardson, *Trump Signs Repeal of U.S. Broadband Privacy Rules*, REUTERS (Apr. 3, 2017), https://www.reuters.com/article/us-usa-internet-trump/trump-signs-repeal-of-u-s-broadband-privacy-rules-idUSKBN1752PR [https://perma.cc/4JHJ-DDAP].

82. *See generally* RICHARD S. BETH, CONG. RESEARCH SERV., RL31160, DISAPPROVAL OF REGULATIONS BY CONGRESS: PROCEDURE UNDER THE CONGRESSIONAL REVIEW ACT (Oct. 10, 2001) (In order for both houses to "qualify for an expedited consideration, a disapproval resolution must be submitted within 60 days after Congress receives the rule, exclusive of recess periods).

83. Harper Neidig, *Trump Signs Internet Privacy Repeal*, THE HILL (Apr. 3, 2017), https://thehill.com/homenews/administration/327107-trump-signs-internet-privacy-repeal [https://perma.cc/TLX9-UY95].

have to find alternatives to safeguard their online personal data against privacy violations by ISPs, who continue to have unrestricted access to consumer data.

III. REPEAL IN PRIVACY RULES CAUSED BY THE ELECTION

The U.S. federal government operates with the collective effort of the three branches, which leaves consumer privacy protection laws to fluctuate with the current political climate.

A. SHIFT IN THE EXECUTIVE BRANCH

The president appoints five members to the FCC, who are confirmed by the Senate, and then proceed to fulfill five-year terms.[84] To prevent politicization, no more than three of the five members can originate from the same political party.[85] President Barack Obama had previously appointed Thomas Wheeler, a member of the Democratic Party, as the chairman of the FCC.[86] Wheeler shed a light on the issues surrounding online consumer privacy and unveiled privacy violations of ISPs, which ultimately led to the adoption of the Internet Privacy Rules.[87]

The shift of power in the executive branch directly led to the repeal of the previously adopted privacy rules. The FCC's priorities radically shifted when President Donald Trump took office in 2017 and nominated Ajit Pai as FCC chairman. The now predominantly Republican commission listened to critics of the privacy rules who claimed that the policies were ineffective due to the imbalanced regulation of ISPs over websites. Opponents of the privacy rules were unsatisfied with the FCC's reclassification of ISPs as telecommunication carriers because they believed the FTC had better experience with online privacy issues directly relating to advertising policies. The FTC handles cases when companies exhibit anticompetitive behavior and it polices companies who engage in unfair and deceptive practices. Opponents of the privacy rules argued that the commission's lack of experience in addition to the inconsistent rules governing service providers and website operators was ample reason for Congress to repeal the rules.[88] The impact of a Republican leader in the White House, with opposite priorities to the previous leadership, rippled as far out to the federal agencies that were fundamentally supposed to protect our online privacy rights.

84. Stephen Lovely, *What Is The FCC, And How Does It Work?*, CORDCUTTING (Oct. 13, 2016), https://cordcutting.com/what-is-the-fcc-and-how-does-it-work/ [https://perma.cc/K3H5-V3ZY].

85. *Id.*

86. *See* Boliek, *supra* note 7.

87. *Id.*

88. *See* Glenn G. Lammi, *The Nullification of FCC's Broadband Privacy Rules: What It Really Means For Consumers*, FORBES (Apr. 12, 2017), https://www.forbes.com/sites/wlf/2017/04/12/the-nullification-of-fccs-broadband-privacy-rules-what-it-really-means-for-consumers/#37b6def479ba [https://perma.cc/4UX9-EWY8].

B. SHIFT IN THE CONGRESSIONAL BRANCH

Congress's support laid the foundation for the repeal to take place. Congressional Republicans covertly scheduled a vote to roll back privacy protections when the nation was distracted by the House's battle to repeal the Affordable Care Act.[89] Although the president held the power to veto, he acted under the CRA and signed the bill to repeal the privacy rules into law as of April of 2017, ultimately depriving consumers of their online privacy rights.[90]

IV. PRIVACY PROTECTION MECHANISMS MOVING FORWARD

A. HOPE FOR THE NEW FCC?

The change within the government created a new controlling party within the FCC whose priorities differ from the previous commission's concerns. The new FCC has rejected the previous view that broadband providers are "the most important and extensive conduits of consumer information."[91] The new Republican commissioners contend broadband service providers and website operators should be held to the same standards, instead of the two being regulated under different agencies with different rules.[92] Specifically, corporations concur that the new Internet rules would just leave consumers confused by separate sets of rules governing each online service, which could potentially inhibit competition and lead to antitrust violations. Since ISPs' users would have to opt-in and users of all other types of website services would continue to use opt-out, data accumulated through "big data" analytics would be used unfairly among corporations, and ultimately lead to increased transactional costs for all parties involved. Consequently, advocates of the repeal agree that the privacy rules would "create confusion" because the FCC and the FTC would monitor different parts of the "Internet ecosystem."[93]

Regardless of the reason, the repeal of the privacy rules has left all consumers unprotected while corporations continue to benefit from consumer vulnerability online. Proponents of the privacy rules are convinced that the

89. Kimberly Kindy, *How Congress Dismantled Federal Internet Privacy Rules*, THE WASHINGTON POST (May 30, 2017), https://www.washingtonpost.com/politics/how-congress-dismantled-federal-internet-privacy-rules/2017/05/29/7ad06e14-2f5b-11e7-8674-437ddb6e813e_story.html?noredirect=on&utm_term=.445576bf546d [https://perma.cc/G229-DT5S].

90. *Id.*

91. Larry Downes, *The Downside of the FCC's New Internet Privacy Rules*, HARVARD BUSINESS REVIEW (May 27, 2016), https://hbr.org/2016/05/the-downside-of-the-fccs-new-internet-privacy-rules [https://perma.cc/23QT-4H5L].

92. Larry Downes, *Why Congress's Rejection Of Proposed FCC Data Rules Will Not Affect Your Privacy In The Slightest*, FORBES (Mar. 30, 2017), https://www.forbes.com/sites/larrydownes/2017/03/30/why-congresss-rejection-of-proposed-fcc-data-rules-will-not-affect-your-privacy-in-the-slightest/#3e9d2f1e8b14 [https://perma.cc/2G33-DU5E].

93. Jeff Flake, *Settling a Bureaucratic Turf War in Online Privacy Rules,* WSJ (Mar. 1, 2017), https://www.wsj.com/articles/settling-a-bureaucratic-turf-war-in-online-privacy-rules-1488413165 [https://perma.cc/E5M6-9QWM].

call for uniform rules for service providers and website operators is a tactical diversion to allow all corporations access to personal consumer data.[94]

B. WILL THE FCC TRY TO REGAIN AUTHORITY?

Although a majority of Republicans view the FTC as the most competent agency to regulate ISPs because of its prior history of handling online privacy, the FTC does not have jurisdiction over common carriers. It is highly unlikely that the FTC will be able to synchronize standards for ISPs and websites without major interference from the FCC.

Even if the FCC allows the FTC authority over broadband service providers, there would be other barriers that the FTC would have to overcome. In October 2014, the FTC sued AT&T for deceiving customers by proposing unlimited data plans and adjusting speeds once customers hit specific usage limits.[95] AT&T claimed that the FTC had no authority since the company was regarded as a common carrier. However, in 2014, AT&T was regarded as a common carrier for landline, mobile phone and voice services, but was not regarded as a common carrier for mobile Internet access. The FTC contended that it could punish AT&T for wrongdoings related to its non-common carrier services. The case went all the way to the Ninth Circuit, which determined that AT&T's status as a common carrier under the Communications Act protects it from liability under Section 5 of the FTC Act. During this process the Ninth Circuit did not cover in-depth whether the common carrier status would be applicable to an ISP if only a fraction of its business involved common carrier services. The court noted that AT&T is a common carrier "for a substantial part of its activity."[96] This leaves a slim chance that the FTC will gain authority over a type of provider that is not considered a common carrier for "a substantial part of its activity." As long as common carriers are under FCC jurisdiction, the FTC will not have authority.

C. STATE-LEVEL PROTECTION

Many states have started to seek within their borders for solutions regarding Internet privacy matters. As such, after Congress dismantled the privacy rules, California decided to protect its own residents by creating state consumer privacy laws. Assemblymember Ed Chau (D-Monterey Park) introduced The California Broadband Internet Privacy Act ("CBIPA").[97] As of June 2018, CBIPA passed and provided California residents an assortment of new online privacy rights such as the right to: (1) be informed about the type of personal data companies collect; (2) request deletion of personal information; (3) opt out of the sale of personal information; and (4) access to

94. Frank Pallone Jr. and Terrel McSweeny, *New Rules Intended to Protect Your Online Privacy Are Already Under Threat*, SLATE (Feb. 9, 2017), http://www.slate.com/articles/technology/future_tense/2017/02/consumer_privacy_rules_for_internet_service_providers_are_under_threat.html [https://perma.cc/C46J-ZKR6].

95. FTC v. AT&T Mobility LLC., 835 F.3d 993 (9th Cir. 2017).

96. *Id.*

97. Cal. Assemb. 375, 2017-2018 Reg. Sess. (Cal. 2018).

this personal information.[98] Unlike the federal Internet Privacy Rules, CBIPA comprehensively protects consumer privacy by including an opt-in for all information without the distinction between sensitive and non-sensitive information.[99] The California privacy protections additionally include demographic data to the type of information that cannot be used without user permission.[100] The state attorney general would be enforcing privacy law violations though this new law has big-name opponents such as AT&T, T-Mobile, and Verizon.[101] Even before the bill was passed, AT&T had expressed that it would create consumer confusion because of "diminished Internet experience."[102] Although CBIPA mirrored most of the FCC's Privacy Rule provisions, it substantively is more expansive and also covers a broader range of information.

Other states have also started to act regarding Internet privacy matters and more states may follow suit. For example, a new bill in the Kansas House would require ISPs to seek the approval of their customers before selling any information for personalized targeted advertising.[103] The steps states could take would be for state legislatures to bar ISPs from using or selling their customer's data without getting explicit permission. Additionally, bills could ban ISPs from charging extra for Internet services for customers who decline to share their personal data. An alternative plan could involve states amending their economic development budget to add broadband privacy. The statehouse would have to sign the bill and then the Governor would have to sign it into law.

D. REGULATION OF WEBSITES

Instead of Congress repealing the privacy rules for ISPs, since website operators would continue to remain unregulated, the FTC should have come up with guidelines that would have paralleled the FCC. The FTC has authority over website operators such as Facebook and Google. Currently, consumers are not protected when browsing and/or entering in sensitive personal information on their websites. If anything, consumers are exposed when perusing the web and their activity is monitored through hidden trackers. 76% of websites now contain hidden Google trackers and 24% of them have hidden Facebook trackers.[104] Facebook and Google alone have

98. Dipayan Ghosh, *What You Need to Know About California's New Data Privacy Law*, Harvard Business Review (July 11, 2018), https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law [https://perma.cc/EN58-4SVF].

99. *See* Cal. Assemb. 375, 2017-2018 Reg. Sess. (Cal. 2018).

100. *Id.*

101. *Id.*

102. *Id.*

103. Eyragon Eidam and Jessica Mulholland, *10 States Take Internet Privacy Matters Into Their Own Hands*, GOVERNMENT TECHNOLOGY (Apr. 10, 2017), http://www.govtech.com/policy/10-States-Take-Internet-Privacy-Matters-Into-Their-Own-Hands.html [https://perma.cc/3C22-D2RY].

104. Gabriel Weinberg, *Google And Facebook Are Watching Our Every Move Online. It's Time To Make Them Stop*, CNBC (Jan. 31, 2018), https://www.cnbc.com/2018/01/31/google-facebook-data-privacy-concerns-out-of-control-commentary.html [https://perma.cc/7VXH-42BQ].

collected comprehensive data profiles on each person ranging from personal interests, past purchases, browser history, and location.

These user data profiles are not just a small link in the chain. Personal user data information collected from websites are used in complex algorithms that control what ads consumers see on the web browser based on what the algorithm predicts the consumer would be interested in and click on.[105] As a result, users are unknowingly segregated into groups within a society based on online web searches and web purchases.

Sites may claim self-regulation, but website data privacy policies and business models revolve around personalized marketing, which essentially contradict any claims of effective self-regulation. Until Congress and federal agencies can be trusted to make the consumer the first priority, Americans are left to protect themselves. Browser add-ons are a way to block Google and Facebook's hidden trackers and create a more secluded browsing experience. Another simple yet unrealistic solution would be to boycott websites such as Google and Facebook.

E. IMMEDIATE STEPS USERS CAN TAKE

By using a virtual private network ("VPN"), online users can protect their devices from prying eyes by masking IP addresses and preventing ISPs from tracking browsing history.[106] VPNs scramble IP addresses so that user identities and locations are anonymized. As discussed previously, de-identification of data is not always permanent. However, VPNs create obstacles for those who want to access online user history.

V. CONCLUSION

Until ISPs are regulated, there will be no change in our online privacy. State laws surrounding online privacy issues is a start, but should not be the lone solution. We cannot let the fate of our fundamental privacy rights depend on national administrative political changes. The privacy rules would not have solved every issue or inconsistency, but instead would have been a promising start in protecting citizens' privacy online.

105. *Id.*

106. Molly McLaughlin, *How To Hide Your Browsing History From Your ISP*, LIFEWIRE (Mar. 12, 2018), https://www.lifewire.com/hide-browsing-history-from-isp-4134480 [https://perma.cc/39XY-8EZK].