Double Trouble: Why Two Internet Privacy Enforcement Agencies Are Not Better Than One for Businesses or Consumers

Alison M. Cheperdak *

TABLE OF CONTENTS

* J.D. Candidate, The George Washington University Law School, May 2018. Senior Notes Editor, *Federal Communications Law Journal*, Vols. 69–70. B.A., Communications, Villanova University. I thank the entire staff of the Federal Communications Law Journal for their assistance in this Note's production. I am deeply grateful to GW Law Journal Adjunct Professor Jodie Griffin and Reference Librarian Lori Fossum for their instrumental guidance. Thank you also to Brooke Ericson, Nathan Halford, and Howard Waltzman for their invaluable insights, and the many Senate and House staff who provided helpful comments. I dedicate this Note to my husband, Jason, and parents, Tom and Paula, for their unending support.

I. INTRODUCTION

In 1890, a formative *Harvard Law Review* article developed "the basic principle of American privacy law" that privacy is the "right to be let alone."[1] Samuel D. Warren and Louis D. Brandeis' *The Right to Privacy* was published "in response to invasions of personal privacy caused by the technological [advances] of newspapers and photographs".[2] Much has changed since Warren and Brandeis' article influenced American privacy common law jurisprudence.[3] In the digital era, the right to privacy may be more appropriately characterized as "knowing what data is being collected and what is happening to it, having choices about how it is collected and used, and being confident that it is secure."[4] Given the ubiquitous nature of collection, retention, and dissemination of data in the digital age, appropriate privacy regulations are required.[5]

The Internet is critical to virtually all aspects of life throughout the U.S., especially economically and socially.[6] For instance, through the use of networked technologies, people are able to express themselves in infinite ways, establish "social connections, transact business, and organize politically."[7] "An abundance of data, inexpensive processing power, and increasingly sophisticated analytical techniques drive innovation in our increasingly networked society."[8] The U.S. government has two strong interests in establishing and enforcing appropriate privacy policies;[9] privacy is important to Americans and they expect their privacy to be protected from intrusion by the government or private entities,[10] and strong privacy

---

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 5 (1890).
2. *Id.* at 195-96.
3. *See* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), https://perma.cc/78VD-Z7MJ [hereinafter WHITE HOUSE PRIVACY FRAMEWORK] (statement of President Barack Obama). "Never has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones. In just the last decade, the Internet has enabled a renewal of direct political engagement by citizens around the globe and an explosion of commerce and innovation creating jobs of the future."
4. *The State of Online Consumer Privacy: Hearing Before S.Comm. on Commerce, Science, and Transportation*, 112th Cong. 4, pg. 32 (2011) (statement of Erich Andersen, Deputy Gen. Counsel, Microsoft Corp.).
5. *See generally* WHITE HOUSE PRIVACY FRAMEWORK at 5.
6. *Id.* at 5.
7. *Id.* at 5.
8. *Id.* at 5.
9. *Id.*
10. *See generally The State of Privacy in Post-Snowden America*, PEW RES. CTR. (Sept. 21, 2016), https://perma.cc/R5HR-Q6KC (86% of Internet users have taken steps online to remove or mask their "digital footprints," and many would like to take additional steps to protect their online privacy and are unaware of how to do so. 74% of Americans surveyed said it is "very important" to them that they be in control of *who* can get information about them, and 65% said it is "very important" to them to control *what* information is collected about them.); WHITE HOUSE PRIVACY FRAMEWORK at 4-5.

protections are essential to sustaining the trust necessary for Internet commerce, which consequentially fosters innovation and economic growth.[11]

Consumers should not have to be a lawyer or a network engineer to understand whether the information they provide via the Internet will or will not be protected.[12] However, the current rules and regulations governing Internet data security are just that—needlessly complex and confusing.[13] The current Internet data security legal landscape is complicated primarily because "there is no comprehensive federal privacy statute that protects personal information."[14] Instead, federal privacy rules are disjointed; both the FTC and the FCC have authority to regulate different parts of the Internet, and states also have authority to enact and enforce their own privacy laws despite the inherently interstate elements of online transactions.[15]

Significantly, the FTC and the FCC's frameworks differ in that the FTC's priority is security, whereas the FCC's priority is privacy.[16] The FTC appropriately focuses more on security, including personally identifiable information (PII), whereas the FCC focuses more on privacy, [17] which is considerably more subjective and personal versus security which is primarily about safety.

This Note explores the ways in which the FCC's Broadband Privacy Order is harmful to both businesses and consumers, and the ways in which the regulations that apply to Edge Service Providers (ESPs) and Internet Service Providers (ISPs) can be legally harmonized. The Note begins with a discussion of the harms the uneven privacy models of the FCC and the FTC impose on customers and businesses, including confusion and increased transactional costs. Next, the Note discusses how the FCC failed to adequately explain why it chose not to follow the FTC's preexisting and successful approach to data security, including an analysis of the numerous ways in which the FCC needlessly diverged from the FTC's reasonable model. While the FTC is the ideal enforcer of Internet data security because of its long

---

11. WHITE HOUSE PRIVACY FRAMEWORK at 4-5.

12. *See* Dissenting Statement of Ajit Pai, Comm'r, FCC, at 1, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 16-106 (Nov. 2, 2016), https://perma.cc/6MSN-7GMN [hereinafter Pai Dissenting Statement].

13. *See generally,* Dissenting Statement of Michael O'Rielly, Comm'r, FCC, at 5, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 16-106 (Nov. 2, 2016), https://perma.cc/Q3GE-UL8K [hereinafter O'Rielly Dissenting Statement].

14. *See* GINA STEVENS, CONG. RESEARCH SERV., PRIVACY PROTECTIONS FOR PERSONAL INFORMATION ONLINE 5, 7 (2011), https://perma.cc/E866-HJ3R; *see also* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY forward, (2012) ("White House Privacy Framework") ("neither consumers nor companies have a clear set of ground rules in the commercial arena. As a result, it is difficult today for consumers to assess whether a company's privacy practices warrant their trust.").

15. *See generally*, The Federal Trade Commission Act 15 U.S.C. § 45(a) ("FTC Act"); Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Report and Order*, 16-101 FCC Rcd 16-148, para. at 1 (2016), https://perma.cc/F7EW-PCKN [hereinafter *Privacy Order*]; *see generally*, *State Laws Related to Internet* Privacy, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 5, 2016), https://perma.cc/X53G-JADT/.

16. *See generally*, *Privacy Order*; FTC REPORT.

17. *See* FTC REPORT at 18; *Privacy Order* at para. 1, 92, 134.

history of providing consumer protection and online data security, the FTC must provide a clearer description of what BIAS and ESPs must do to adequately protect consumers' privacy and security. Finally, the Note will explain the ways in which ESP and ISP privacy regulations can be legally harmonized after the Privacy Order's recent repeal.

II. BACKGROUND

A. Components of the Internet

The Internet is comprised of four major actors: "end users, broadband providers [(also known as ISPs)], backbone networks, and edge [service] providers [(ESPs)]."[18] Many customers, also known as end users, access the Internet "using an ISP, which delivers high-speed Internet access using technologies, such as cable modem service, digital subscriber line (DSL) service, and fiber optics."[19] ISPs "interconnect with backbone networks," which are the "long-haul fiber-optic links and high-speed routers" that transmit "vast amounts of data."[20] ESPs are content, "application, service, and device" providers, and their name comes from the position that they operate "at the edge of the network rather than the core of the network."[21] Examples of ESPs include Netflix, Google, and Amazon.[22] Under the current privacy legal landscape, the FTC has authority over ESPs, and the FCC has authority over ISPs.[23]

B. FTC's Strong History of Internet Privacy Regulation

The FTC derives its authority for enforcement actions against ESPs under The Federal Trade Commission Act 15 U.S.C. § 45(a) (FTC Act), which prohibits "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[24] The FTC Act does not provide industry-specific duties, but instead applies a technology-neutral approach.[25] However, while the FTC Act does not provide specific duties for ESPs (or any other type of company that falls under its jurisdiction), the FTC's 2012 report, *Protecting Consumer Privacy in an Era*

---

18. U.S. Telecom Association v. FCC 825 F.3d 674, 690 (D.C. 2016), https://perma.cc/KQ4C-JATN [hereinafter U.S. Telecom Association.

19. *See,* Protecting and Promoting the Open Internet, *Report and Order on Remand, Declaratory Ruling, and* Order, 14-28 FCC Rcd 15-24, at para 5 (2015), https://perma.cc/4TLY-74MB [hereinafter *2015 Open Internet Order*].

20. *See* U.S. Telecom Association.

21. *See* Preserving the Open Internet Broadband Industry Practices, *Report and Order*, 07-52 FCC Rcd 10-201, para. 4, 20, n.2 (2010), https://perma.cc/K4PX-3VGQ (2010) [hereinafter *2010 Open Internet Order*].

22. *See* U.S. Telecom Association.

23. *See generally* http://adage.com/article/privacy-and-regulation/ftc-regain-isp-privacy-oversight-easy/308487/.

24. *See* 15 U.S.C. § 45(a) (2012).

25. *Id.*

of Rapid Change (FTC Report), provides more specific recommendations for Internet businesses and policymakers.[26] The FTC Report set forth a final privacy framework after taking into consideration more than 450 public comments from stakeholders.[27] Although the FTC Report by its nature does not consist of binding rules, it urges companies to implement "best practices" to protect consumers' private information immediately, such as "making privacy the 'default setting' for commercial data practices" and increasing "consumers' control over the collection and use of their personal" information.[28] The FTC Report also stipulates that "companies should view the comprehensive privacy programs mandated by consent orders as a roadmap as they implement privacy by design in their own organizations."[29] Perhaps most importantly, the FTC's "proposed framework is not a one size fits all model for consumer choice mechanisms."[30] Instead, the FTC urges companies to offer "clear and concise choice mechanisms that are [both] easy to use and delivered at a time and context that is relevant to the consumer's decision about whether to allow data collection or use."[31]

The FTC, which regulates ESPs, "has brought numerous legal actions against organizations that have violated consumers' privacy rights, or misled [consumers] by failing to maintain security for [their] sensitive information."[32] In most of these cases, "the FTC has charged the defendant with violating Section 5 of the FTC Act," which prohibits "unfair and deceptive acts and practices in or affecting commerce."[33] For example, the FTC "brought enforcement actions against mobile applications that violated

26. *See generally*, FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESS AND POLICYMAKERS (2012) [hereinafter FTC REPORT], https://perma.cc/L53D-5QJY; In keeping with the White House Privacy Framework terminology, throughout this Note, "'company' means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture established to make a profit, or nonprofit entity, that collects, uses, discloses, stores, or transfers personal data in interstate commerce, to the extent such organizations are not subject to existing Federal data privacy laws." WHITE HOUSE PRIVACY FRAMEWORK at 5.

27. FTC REPORT at i.

28. *Id.*

29. *Id.* at 31.

30. *Id.* at 49;13 (FTC calls on Congress to enact "baseline privacy legislation that is technologically neutral and sufficiently flexible to allow companies to continue to innovate").

31. *Id.* at 49-50.

32. *Protecting Consumer Privacy: Enforcing Privacy Promises*, FTC, https://perma.cc/4UQE-JKY4 (last accessed Apr. 11, 2017).

33. *Id.*

the Children's Online Privacy Protection Act,[34] as well as against entities that sold consumer lists to marketers in violation of the Fair Credit Reporting Act" (FCRA).[35] During the first 40 years of the FTC's enforcement of the FCRA, "the FTC brought 87 enforcement actions against [consumer reporting agencies] (CRAs)."[36]

C. The FCC's New Role in Internet Privacy Regulation

The Privacy Order establishing the FCC's privacy enforcement power was passed in 2016 during the final year of the Obama Administration.[37] However, on April 3, 2017, President Donald J. Trump signed a joint resolution that repealed the FCC's Privacy Order.[38] The passage of S.J. Res. 34 came less than a month after the Republican majority FCC voted 2-1 to issue a temporary stay on the data security obligations of the Privacy Order, which were to take effect March 2, 2017.[39] This action indicates that the new Republican leadership at the FCC disfavored the prior Democratic-leaning Commission's previous plans.[40]

The Privacy Order is problematic because without a uniform technology-neutral standard for all, or at the very least, most Internet activity, under the current rules and regulations it is incumbent upon an Internet user to understand (1) the specific type of Internet businesses she uses; (2) the corresponding legal obligations of those businesses; and (3) how to opt-in or

---

34. *See* https://www.ftc.gov/news-events/press-releases/2015/12/two-app-developers-settle-ftc-charges-they-violated-childrens; Mobile game company TinyCo Inc. and online review site Yelp settled separate Department of Justice charges that they improperly collected information from children via their mobile applications. According to the FTC's complaint against TinyCo, the app which had been downloaded more than 34 million times, was targeted at children and some of the company's apps included an optional feature that collected email addresses from all users, including those younger than 13. In its complaint against Yelp, the FTC alleged that Yelp Inc. collected personal information from children without first notifying parents and obtaining their consent. *United States v. Yelp Inc.*, 3:14-cv-04163, *proposed stipulated order filed* (N.D. Cal. Sept. 16, 2014); *United States v. TinyCo Inc.*, No. 3:14-cv-04164, *proposed stipulated order filed* (N.D. Cal. Sept. 16, 2014); Fair Credit Reporting Act (FCRA) violations by FTC-regulated entities are considered unfair and deceptive practices and are subject to the remedies provided by Section 5 of the FTC Act. Section 621(a); *see also* 15 U.S.C. §§ 41 *et seq*. The FTC also has authority to file civil actions in federal court to recover civil penalties of up to $3,500 per violation for a "knowing violation, which constitutes a pattern or practice of violations." FTC, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATION 4 (2011).

35. https://www.ftc.gov/news-events/press-releases/2016/05/debt-collector-settles-ftc-charges-it-violated-fair-credit.

36. FTC, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATION 4 (2011).

37. *See generally Privacy Order*; *see also* https://www.reuters.com/article/us-usa-internet-trump/trump-signs-repeal-of-u-s-broadband-privacy-rules-idUSKBN1752PR.

38. https://www.reuters.com/article/us-usa-internet-trump/trump-signs-repeal-of-u-s-broadband-privacy-rules-idUSKBN1752PR; FN 38 on annotated sources.

39. *See generally* S.J. Res. 34.

40. *See generally O'Reilly dissenting See generally, id.*; Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Order Granting Stay Petition in Part*, 16-106 FCC 17-19 (2017).

opt-out of the collection, retention, and dissemination of her personal information based on relevant legal authorities.[41] The steps required to understand Internet data security laws are too complicated for the average person.[42] The Internet data security framework should, therefore, be amended so the average, non-attorney Internet user can understand the laws that apply.[43]

Although consumer protection is chief among the goals of privacy regulations, the lack of uniform laws in this area is far too confusing for the average customers to possibly understand how the regulations may be helpful to them.[44] Under the Privacy Order, for a consumer to understand the privacy laws that apply to her Internet activity, she must understand both the distinction between ISPs and ESPs, as well as the differences between the FCC and the FTC's privacy policies, and how those policies apply to her personal browsing activity.[45] The following scenario demonstrates the inherent complexity of relatively basic Internet use. A customer purchases an Internet service plan from Verizon FIOS (an ISP) to access the Internet. This transaction would be governed by the FCC because the FCC has jurisdiction over ISPs. While browsing the Internet, the user reads several articles on *The New York Times* website and watches a program on Netflix. These activities would be governed by the FTC because the FTC has jurisdiction over ESPs.[46] Here, both *The New York Times* and Netflix's websites are ESPs because they provide content and services in the form of news and entertainment online.[47]

Buttressing the inherent complexity of having "two cops" on the Internet privacy "beat", an ESP's liability may be different according to the way a customer uses the service.[48] For example, Google is an ESP that can be accessed via an ISP, but the company has begun connecting directly to broadband providers' networks, thus eliminating the need to interconnect with

41. O'Rielly Dissenting Statement at 5; Pai Dissenting Statement at 1 (For the last two decades, the Federal Trade Commission applied the same privacy framework to all internet businesses, so consumers had a reasonable uniform expectation of privacy. "[C]onsumers should not need to be network engineers to understand who is collecting their data and they should not have to be lawyers to determine if their information is protected.").

42. *See generally* Smith, What Internet Users Know about tech and web.

43. *See* Pai Dissenting Statement at 1.

44. *See generally* Pai Dissenting.

45. *Id.* Internet activity using an ISP, also known as a broadband internet access service (BIAS) is governed by the FCC pursuant to the *Privacy Order* para. 1. ESPs are exempt from FCC regulation and are instead regulated by the FTC pursuant to its broad consumer protection authority found in Section 5 of the FTC Act.

46. Id. *See* also 15 U.S.C. § 45(a) (2012).

47. *See* U.S. Telecom Association.

48. *See* Maureen K. Ohlhausen, Commissioner, FTC, Address at the 33rd Annual Institute on Telecommunications Policy & Regulation 4 (Dec. 4, 2015) [hereinafter Ohlhausen address] ("Consumers will be worse off if overlapping efforts unnecessarily divert resources from more pressing issues. When two cops are on one beat, another beat may be left vulnerable. Additionally, if enforces fail to leverage their comparative advantages, consumers will be worse off.").

a backbone network, as is typical in transactions involving ISPs and ESPs.[49] Moreover, some ISPs, "such as Comcast and AT&T[] have begun developing their own backbone networks."[50] The blurred lines between ISPs, ESPs, and backbone networks illustrate the technical differences that determine which parts of the Internet are governed by the FCC versus the FTC.[51]

D. The Major Impacts of Differing Consumer Consent Models and Privacy Definitions

The most significant difference between the FTC and the FCC's approaches to data security concerns when a company must obtain "opt-in" versus "opt-out" permission from individual consumers before using contextual information for advertising and related purposes.[52] The FCC and the FTC both use "sensitivity-based customer choice frameworks", but the agencies make judgements using different definitions of sensitive data.[53]

The FCC defines sensitive customer proprietary information ("PI") as "financial information, health information, Social Security numbers, precise geo-location information, information pertaining to children, content of communications, web browsing history, application usage history, and the functional equivalents of web browsing history or application usage history."[54] The Privacy Order also requires ISPs to provide customers with a "mechanism to adjust their choice options."[55]

Contrarily, the FTC's definition of sensitive customer data is narrower. It includes "Social Security numbers [,] financial, health, children's and geographical information", but does *not* include content of communications, web browsing activity or application usage history, as delineated in the FCC's Privacy Order.[56] The Privacy Order also applies to more than merely sensitive data; the scope of information covered by the FCC's rules includes "Customer Proprietary Network Information (CPNI), [customer proprietary information

49. Jon Brodkin, *Google Fiber Makes Expansion Plans for $60 Wireless Gigabit Service, Ars Technica* (Feb. 22, 2017, 11:44 AM), https://arstechnica.com/information-technology/2017/02/google-fiber-makes-expansion-plans-for-60-wireless-gigabit-service/; 15 U.S.C. § 45(a) (2012); *2010 Open Internet Order* at n.2; U.S. Telecom Association.

50. *See generally* U.S. Telecom Association.

51. *Id.*

52. *See Privacy Order* at para. 9 (carriers must obtain opt-in approval for use and sharing of sensitive PI). In contrast, the FTC generally requires opt-in approval for use and sharing of sensitive personal information. The FTC staff made this point in its comment to the *Privacy Order* NPRM. The FTC Staff recommended that the FCC require opt-in consent for the use and sharing of sensitive data and opt-out consent for the use and sharing of non-sensitive data. Bureau of Consumer Protection of the FTC Comment, https://perma.cc/YND2-X6WR; FTC Report at vii-viii; FTC REPORT at 15; Bureau of Consumer Protection of the FTC Comment, https://perma.cc/YND2-X6WR.

53. *Id.*

54. *See Privacy Order* at para. 9; FTC Report at vii-viii, 15.

55. *See* Privacy *Order* at para. 167.

56. *See* FTC REPORT at 15.

(PI)], personally identifiable information (PII), and content of communications."[57]

The FTC and the FCC also differ on consumer consent policies. The FCC's Privacy Order adopts three categories of approval with respect to the use of customer PI obtained by ISPs, including: (1) opt-in approval; (2) opt-out approval; and (3) congressionally-recognized exceptions to customer approval requirements.[58] The Privacy Order also adopts "heightened disclosure and affirmative consent requirements for BIAS that offer its consumers financial incentives, [such as sales and promotions], in exchange for the right to use the customers' confidential information."[59]

Instead of establishing *per se* categories, the FTC's "framework sets forth best practices" designed to "work in tandem with existing privacy and security statutes."[60] The FTC's approach is more flexible.[61] For instance, the FTC does not require "entities that collect limited amounts of non-sensitive data from under 5,000 [customers] to comply with the framework, as long as they do not share the data with third parties."[62] This policy is designed to prevent regulating smaller entities out of business, like a "cash-only-curb-side food truck business that offers to send messages announcing [deals]."[63] The FTC's flexible standard also recognizes that "some business practices create fewer potential risks to consumer information" than others. The FTC believes that for some business transactions, "the benefits of providing choice are reduced—either because consent can be inferred or because public policy makes choice unnecessary."[64]

The FTC's "opt-out" approach recommends in most instances that ESPs allow consumers to "opt-out" of their data being used for advertising and related purposes, unless the use is consistent with the consumer's relationship with the business and thus does not necessitate consumer choice.[65] The FTC believes that "whether a practice requires" consumer consent depends "on the extent to which the practice is consistent with the context of the transaction or [user's] existing relationship with the business, or is required or specifically authorized by law."[66] Therefore, companies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the particular transaction, or the parties' relationships, or required or authorized by law.[67] The FTC also continues to believe that there are "five categories of data practices that

57. *See Privacy Order* at para. 6.
58. *See Privacy Order* at para. 9.
59. *Id.* at para. 12.
60. FTC REPORT at 16.
61. FTC REPORT at 16-17.
62. *Id.* at 16.
63. *Id.*.
64. *Id.* at 38.
65. *Id.* at 39-40.
66. *Id.* at 38-39; *see also*, WHITE HOUSE PRIVACY FRAMEWORK at 1 (Obama Administration's Privacy Bill of Rights requirements include: "Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.").
67. FTC REPORT at 48.

companies can engage in without offering consumer choice," because the "data collection and use" in the particular contexts are "either obvious" or "sufficiently acceptable or necessary for public policy reasons."[68] The categories include: "(1) product and service fulfillment; (2) internal operations; (3) fraud prevention; (4) legal compliance and public purpose; and (5) first-party marketing."[69]

Both the FCC and the FTC require affirmative express consent from customers for the data collection and use of certain types of information in particular contexts, but the agencies have different standards.[70] The FCC requires ISPs to obtain opt-in consent to track a user's Internet browsing activity.[71] The FTC does not require consent for such activity.[72] However, the FTC does require affirmative express consent in the following circumstances: (1) ESPs should obtain consent before making material retroactive changes to privacy representations; and (2) ESPs should obtain consent before collecting sensitive data.[73] Here, it is legally significant that the FTC employs a narrower definition of "sensitive" compared to the FCC.[74]

The opt-out policy of the FTC means that an Internet user does not have an expectation of privacy with respect to her online activities as they relate to ESPs, unless she affirmatively opts-out of the collection, retention, and/or dissemination of her Internet browsing history.[75] However, regardless of an Internet user's opt-out or opt-in preference with the ESPs it interfaces with, a user does have an expectation of privacy concerning the information her ISP, the entity that provides online access to her home, collects on her Internet usage.[76] This is because ESPs like Google, YouTube, and Amazon are ESPs and are therefore governed by the FTC under the FTC Act; ISPs like Comcast, Charter Communications, and Verizon are instead governed by the FCC and consequentially have different legal obligations.[77]

Numerous broadband providers, their associations, and other stakeholders submitted comments to the Notice of Proposed Rulemaking for the Privacy Order arguing that because broadband providers are part of a larger online ecosystem that includes ESPs, they should be subject to the same

68. *Id.* at 36-39.

69. *Id.*at 36.

70. *Id.* at 47 ("affirmative express consent is appropriate when a company uses sensitive data for marketing to a first- or third-party." Due to heightened privacy risks associated with sensitive data, like health or children's information, first parties should provide a consumer choice mechanism at the time of data collection); *Privacy Order* at para. 9.

71. *Privacy Order* at para. 9. *Conf.* FTC REPORT at 15.

72. FTC REPORT at 15; Based on its expertise, the FTC staff submitted a comment to the *Privacy* NPRM, indicating its recommendation that the FCC require opt-in consent for the use and sharing of sensitive data and opt-out consent for the use and sharing of non-sensitive data. Bureau of Consumer Protection of the FTC Comment, https://perma.cc/YND2-X6WR.

73. *Id.* at 57.

74. *Privacy Order* at para. 9. *Conf.* FTC REPORT at 58.

75. FTC REPORT at 47.

76. ISPs are exempt from Section 5 of the FTC Act. Instead ISPs, which are common carriers, are governed by the Communications Act; *Fact Sheet: The FCC Adopts Order to Give Broadband Consumers Increased Choice Over Their Personal Information*, FCC 4, https://perma.cc/NNT6-G5LF (last accessed Apr. 11, 2017).

77. *Id.*

set of regulations as ESPs.[78] Responding to the commenters' concerns, the Privacy Order maintains that a ISPs should be subjected to stricter standards than ESPs because an ISP "sits at a privileged place in the network, the bottleneck between the customer and the rest of the Internet."[79] The Privacy Order maintains that because ISPs serve as "gatekeepers" to the Internet, whereas ESPs see only a slice of a user's online activity, ISPs should be subject to stricter online privacy standards.[80] The unequal obligations of Internet businesses due to a lack of uniform Internet data security standards are unfair to both ISPs and their consumers because the stricter standards under the Privacy Order increase transaction costs for ISPs, which will ultimately be absorbed by consumers.[81] Additionally, the Privacy Order does not adequately articulate the harm that it seeks to prevent by implementing its new privacy standards.[82]

E. The FCC and FTC Differ in Internet Privacy Enforcement Practices

The FCC and the FTC also have different enforcement philosophies concerning Internet data security.[83] Demonstrating how the FCC's approach to privacy and data security enforcement differs from the FTC's, soon after the Protecting and Promoting the Open Internet Report and Order reclassified

78. *See* generally, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Notice of Proposed* Rulemaking, 16-106 FCC Rcd 16-39 (2016) [hereinafter *Privacy NPRM*]; *Privacy Order* at para. 28.

79. *Privacy Order* at para. 28.

80. *Id.* at para. 36.

81. "The goal of consumer protection enforcement isn't to make headlines; it is to make harmed consumers whole and incentivize appropriate practices. The costs imposed by a regulator on a legitimate, non-fraudulent company are ultimately born by its consumers. If enforcement action imposes costs disproportionate to the actual consumer harm, that enforcement action may make consumers worse off if prices rise or innovation slows." Ohlhausen Address at 5.

82. *Privacy Order* at para 28 (FCC provides that in formulating its rules, the FCC considered the FTC REPORT and the WHITE HOUSE PRIVACY FRAMEWORK. However, the FCC declined to sufficiently explain why it found the "heightened protections" for sensitive customer information was necessary due to the "vast swathes of customer data" available to ISPs). Moreover, the *Privacy Order* expands the definition of "proprietary information" to include information beyond what a customer would "keep secret from any other party." The FCC dismisses multiple strong arguments as to why expanding the definition of proprietary information is appropriate without providing adequate justification. *Privacy Order* at para. 28.

83. Former Obama FTC Chairman Jon Leibowitz disagreed with the FCC's proposal to prohibit ISPs from offering discounted services in exchange for customers opting in to great data collection and use is not optical. In opposition to his fellow-Democrat appointees at the FCC, Leibowitz believed the rules' prohibition of something that consumers don't find problematic would stifle the development of free online services, and other low cost resources, due to increased transactional costs. John Eggerton, *Former FTC Chair Has Issues with FCC's Opt-in CPNI Regime*, MULTICHANNEL (May 11, 2016, 1:45 PM EST), https://perma.cc/PLF7-GTXG.

ISPs, the FCC resolved its first security case against a cable operator.[84] The matter concerned a breach "involving information about 61 of Cox Communication's more than 6 million subscribers."[85] During the case, "amateur hackers social-engineered Cox employees, there was no technical failure involved," and "no payment information accessed."[86] "[H]ackers posted some information about *eight* affected customers on social media," and "Cox detected" and thwarted the breach "within a matter of days."[87] Cox also cooperated with the Federal Bureau of Investigation (FBI) which arrested the hacker.[88] Even though "the FCC's Order and Consent Decree offers no evidence of any resulting identity theft" or other consumer harm, "the FCC settlement imposed a $595,000 fine" (which equals about "$10,000 per affected consumer") and "extensive compliance measures."[89]

In contrast to the FCC's apparent "strict liability" approach, as seen in the Cox matter, the FTC employs a "reasonable security" approach.[90] Since the beginning of the FTC's role in data security enforcement, the FTC "has recognized that there is no such thing as perfect security," and that security is a "continuing process of detecting risks" and adjusting accordingly.[91] Based on this perspective, the touchstone of the FTC's approach to data security has been and continues to be reasonableness—that "a company's data security measures must be reasonable in light of the volume and sensitivity of information the company holds, the size and complexity of the company's operations, the cost of the tools that are available to address vulnerabilities, and other factors."[92]

84. 47 U.S.C. § 222 (2012); *2015*; Cox Communications, *Order*, 0001834696 FCC Rcd 15-1241 (2015), https://perma.cc/Z8ZE-6GP9 [hereinafter *Cox Order*]*; see also* Thomas M. Lenard, *The FCC Flexes Its Privacy Muscles*, THE HILL (Nov. 18, 2015, 7:30 AM EST), https://perma.cc/KF98-YHBY.

85. Ohlhausen Address at 5; *Cox Consent Decree* at para. 9.

86. Ohlhausen Address at 5; *Cox Consent Decree* at para. 2; Thomas M. Lenard, *The FCC Flexes Its Privacy Muscles*, THE HILL (Nov. 18, 2015, 7:30 AM EST), https://perma.cc/KF98-YHBY.

87. Ohlhausen Address at 5; *Cox Consent Decree* at para. 9.

88. Ohlhausen Address at 5; *Cox Consent Decree* at para. 9.

89. Ohlhausen Address at 5; *Cox Consent Decree* at para. 17, 22.

90. Ohlhausen Address at 5; The FTC advocates for policies that ensure strong privacy protections for consumer data. The FTC participated in developing revised guidelines for protecting consumers in e-commerce at the Organization for Economic Co-operation and Development (OECD). The revised guidelines call for companies to implement "reasonable security safeguards and digital security risk management measures." FTC, PRIVACY & DATA SECURITY UPDATE 16 (2016*)*, https://perma.cc/3GSY-BNJ6.

91. Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FTC (Aug. 31, 2016, 2:34 PM), https://perma.cc/M9WM-Y2J8.

92. *Id.*

F. The FTC's Internet Privacy Regulation Stems From its Longtime Leadership in Consumer Protection

The FTC's heavy involvement in data security regulation stems from its longtime role as a leader in consumer protection.[93] In 1938, Congress gave the FTC authority to enforce against "unfair and deceptive acts or practices,"[94] and in 1975 Congress gave the FTC the power to adopt industry-wide trade regulation rules.[95] The FTC's jurisdiction over Internet privacy violations today is based on the agency's authority to proscribe "unfair or deceptive" practices impacting commerce.[96]

The FCC officially interjected itself in the privacy protection space on April 1, 2016, when it published its Privacy Notice of Proposed Rulemaking (NPRM).[97] The Privacy NPRM proposed significant privacy obligations for ISPs, which are the businesses that provide the necessary equipment for the Internet to function, such as Time Warner Cable, Verizon, AT&T, Cox, Charter, and others. [98] However, the notion that the FCC should enforce Internet privacy standards has not been a long-held belief of Democrats.[99] In fact, the Obama Administration's *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* ("Consumer Protection Bill of Rights") which was published in 2012 described the existing consumer data privacy framework as "strong."[100] Moreover, the Obama Administration's Consumer Protection Bill of Rights maintained that the legal landscape prior to the FCC's NPRM of 2016 "rests on fundamental privacy values, flexible and adaptable common law protections and consumer protection statutes, Federal Trade Commission

93. *Our History*, FTC, https://perma.cc/4XUD-KXM5 (since 1915, the FTC's mission has been to protect consumers and promote competition).

94. The FTC was adopted in 1914. Ch. 311, 38 Stat. 719 (1914). Section 5(a)(1) of the Act originally read: "Unfair methods of competition in commerce are hereby declared unlawful." The "unfair or deceptive acts or practices" language was added via the Wheeler-Lea Amendment in 1938. Ch. 49, 52 Stat. 111 (1938). The section was subsequently amended in 2003; Section 5(a)(1) presently provides that "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce are hereby declared unlawful." 15 U.S.C. § 45(a)(1) (2012).

95. *Id.*; Hart-Scott-Rodino Antitrust Improvements Act of 1975 15 U.S.C. § 18(a).

96. FTC, PRIVACY & DATA SECURITY UPDATE 2 (2016*)*, https://perma.cc/3GSY-BNJ6.

97. *See* generally, Privacy *NPRM*.

98. *See* generally, Privacy *NPRM*; *Internet Service Provider Reviews*, TOP TEN REVIEWS, https://perma.cc/YP7E-7RGZ (last accessed Apr. 11, 2017).

99. Former Obama FTC Chairman Jon Leibowitz disagreed with the FCC's proposal to prohibit ISPs from offering discounted services in exchange for customers opting in to great data collection and use is not optical. In opposition to his fellow-Democrat appointees at the FCC, Leibowitz believed the rules' prohibition of something that consumers don't find problematic would stifle the development of free online services, and other low cost resources, due to increased transactional costs. John Eggerton, *Former FTC Chair Has Issues with FCC's Opt-in CPNI Regime*, MULTICHANNEL (May 11, 2016, 1:45 PM EST), https://perma.cc/PLF7-GTXG.

100. WHITE HOUSE PRIVACY FRAMEWORK at forward.

(FTC) enforcement, and policy development that involves a broad array of stakeholders."[101]

The Privacy NPRM demonstrated an expansion of the FCC's authority because it marked the first step of regulating a segment of industry that the FCC recently acquired jurisdiction of in the 2015 Open Internet Order, which reclassified BIAS as a common carrier service, an industry category that the FTC does not have authority over.[102] Section 222 of the Communications Act of 1934 places certain obligations on telecommunications service providers to protect consumer data acquired as a result of providing service.[103] From 1934–2015, BIAS were not considered common carriers, and therefore were subject to FTC regulations.[104] That changed in 2015 when the FCC approved the Open Internet Order, reclassifying BIAS as telecommunications services and finding that the Section 222 privacy requirements apply to BIAS.[105] The Privacy Order, which was adopted on October 27, 2016, clarified that the FCC, not the FTC, has jurisdiction over BIAS providers.[106] The FCC and the FTC thus have separate authority over two crucial categories of business that both directly handle potentially sensitive consumer data.[107] The FCC has jurisdiction over BIAS providers and the FTC has jurisdiction over ESPs.[108] The FCC relied on the FTC's Internet privacy model in part to create its Privacy Order.[109] But, the FCC also relied on its own work in adopting and

101. WHITE HOUSE PRIVACY FRAMEWORK at forward (privacy framework of 2012 is overall "strong" but lacks two elements: a clear statement of basic principles that apply to businesses, and a sustained commitment to all stakeholders regarding consumer data security issues, as needed based on advanced in technologies and business models).

102. 47 U.S.C. § 222 (2012); *see also,* 2015 Open Internet Order, 30 FCC Rcd at para. 193-95.

103. 47 U.S.C. § 222 (2012).

104. *Id.*; U.S. Telecomm. Ass'n v. FCC, 825 F.3d 674, 689 (D.C. 2016) (rejected numerous petitions for review and upheld the 2015 Open Internet Order).

105. *Id.*

106. "Because common carriers subject to the Communications Act are exempt from the FTC's Section 5 authority, the responsibility falls to this Commission to oversee their privacy practices consistent with the Communications Act." *Privacy Order* at para. 24; Order finds that BIAS—like other telecommunications carriers—were already "on notice that they have a duty" to keep private customer information confidential because of the FTC guidance that applied to BIAS *prior to* the FCC's reclassification of BIAS) (emphasis added). *Privacy Order* at para. 87; The Order "does not regulate the privacy practices of websites or apps, like Twitter or Facebook, over which the Federal Trade Commission has authority." *Fact Sheet: The FCC Adopts Order to Give Broadband Consumers Increased Choice Over Their Personal Information*, FCC 4, https://perma.cc/NNT6-G5LF (last accessed Apr. 11, 2017); "By reclassifying BIAS as telecommunications service, we have an obligation to make certain that BIAS providers are protecting their customers' privacy while encouraging the technological and business innovation that help drive the many benefits of our increasingly Internet-based economy." *Privacy Order* at 3.

107. *Privacy Order* at para. 9; FTC Report at vii-viii.

108. *Id.*; U.S. Telecomm. Ass'n v. FCC, 825 F.3d 674, 675 (D.C. 2016) (rejected numerous petitions for review and upheld the 2015 Open Internet Order).

109. *Privacy Order* at para. 9 (FCC provides that in formulating its rules, the FCC considered the FTC REPORT and the WHITE HOUSE PRIVACY FRAMEWORK. However, the FCC declined to sufficiently explain why it found the "heightened protections" for sensitive customer information was necessary due to the "vast swathes of customer data" available to ISPs).

revising rules under Section 222.[110] Even though the Privacy Order was repealed in April 2017, the FCC still has authority over ISPs under Title II.[111] However, the Privacy Order was repealed using the Congressional Review Act, which prohibits the agency from creating a new rule that is "substantially the same" as the one struck down.[112]

Unlike the FCC, the FTC has been involved in online privacy issues since nearly the beginning of the online marketplace.[113] The FTC does not have explicit authority to regulate privacy, but interprets Section 5 of the FTC Act's prohibition on unfair and deceptive trade practices to include, among other practices, violations of a company's stated privacy policy.[114] The FTC has "brought enforcement actions against Google and Facebook;" the court "orders obtained in these cases required the companies to obtain users' affirmative express consent before materially changing certain data practices."[115] The court orders also required the businesses "to adopt company-wide privacy programs that [external] auditors will assess for 20 years."[116] Additionally, the FTC has taken enforcement actions *inter alia* against mobile applications that violated the Children's Online Privacy Protection Act, entities that sold consumers lists to marketers in violation of the Fair Credit Reporting Act, and companies that failed to maintain reasonable data security standards.[117]

While the FTC has more experience in the data security realm than the FCC, the FTC does not employ specific rules like the FCC does.[118] Instead, the underlying reasonableness standard of the FTC's privacy framework is

---

110. *Privacy* Order at para. 4.

111. U.S. Telecomm. Ass'n v. FCC, 825 F.3d 674, 675 (D.C. 2016) (upheld FCC's reclassification of ISPs as telecommunication service in the 2015 Open Internet Order).

112. Congressional Review Act, 5 U.S.C. §§ 801(b)(2) (2012).

113. Press Release, *FTC Releases Report on Consumers' Online Privacy* (June 4, 1998), https://perma.cc/8YJU-J5EH.

https://www.ftc.gov/news-events/press-releases/1998/06/ftc-releases-report-consumers-online-privacy.

114. *See FTC v. Accusearch, Inc*., 570 F.3d 1187 (10th Cir. 2009) (holding the FTC Act was violated when a company sold confidential information).

115. *See United States v. Google Inc.* No. CV 12-04177 SI at *1-3 (N.D. Cal. 2012), https://perma.cc/6RY3-G38G (order approving stipulated order for permanent injunction and civil penalty judgement against Google Inc. ("Google") for violating a consent order with the FTC. Consent order was violated when Google used Gmail users' private information despite telling those users the information would be used only for Gmail services. Google must (1) pay a civil penalty of $22.5 million; (2) must maintain systems that delete cookies from Safari browsers; and (3) must report to the FTC within twenty days, setting forth how it is in compliance with the Proposed order); *In Re: Facebook, Inc.*, F.T.C. No. C-4365 3-7 (requiring Facebook to implement a comprehensive privacy program which is subject to independent third-party audit).

116. FTC REPORT at ii.

117. *Id.*

118. *Compare,* Thomas Pahl, *Your Cop on the Privacy Beat,* FTC BUSINESS BLOG (April 20, 2017, 11:12 AM) https://perma.cc/C9R4-MN2W ("As law enforcers, we walk the walk. To date, we've brought over 130 spam and spyware cases, over 120 Do Not Call cases targeting illegal marketing, over 100 Fair Credit Reporting Act actions, approximately 60 data security cases, more than 50 consumer privacy actions, almost 30 cases for violations of the Gramm-Leach-Bliley Act, and over 20 actions enforcing COPPA"); *with Privacy Order* at para. 1 (FCC began regulating data security with the implementation of the 2015 Privacy Order.

that "[c]ompanies should incorporate substantive privacy protections into their practices, such as data security reasonable collection limits, sound retention and disposal practices, and data security."[119] Holding companies responsible for adhering to their own privacy policies allows companies to craft their privacy policies in accordance with their respective business needs and size.[120] The flexibility that the FTC affords industry is much greater than the black and white rule of the FCC's Privacy Order, which determines a business's duty not based on its respective services or size, but based on the sensitivity of the data the business obtains.[121]

G. Despite Apparent Intent, the FCC's Privacy Order Stifles Innovation and Economic Growth, Ultimately Harming Consumers

The Privacy Order asserts that it gives BIAS consumers "the tools they need to make informed choices about the use and sharing of their confidential information" and ultimately protects consumers from harm.[122] The primary harms that the Privacy Order seeks to address include: (1) ISPs have access to too much data on their user's Internet activity;[123] (2) "truly pervasive encryption on the Internet is still a long way off";[124] and (3) ISPs have a special duty to their customers because of their relationship which is different from those involving ESPs because "consumers generally pay a fee for broadband service, and therefore do not have reason to expect that their broadband service is being subsidized by advertising revenues as they do with other Internet ecosystem participants."[125] The FCC unabashedly recognizes that its Privacy Order is not technology neutral, but it justifies the sector-specific rules with the argument that ISPs have distinctive characteristics and that the Privacy Order will somehow increase consumer confidence in ISPs and consequently improve business for ISPs.[126] Additionally, the FCC relies

119. FTC REPORT at vii.

120. *Id.*

121. *Privacy Order* at para. 3, 9.

122. *Privacy Order* at para. 9.

123. "BIAS providers maintain access to a significant amount of private information about their customers' online activity, including what websites a customer has visited, how long and during what hours of the day the customer visited various websites, the customer's location, and what mobile device the customer used to access those websites. *Privacy Order* at para. 33.

124. *Privacy Order*, at para. 34.

125. *Id.* at para. 35.

126. "[W]e disagree with commenters that argue that BIAS providers' insight into customer online activity is no greater than large edge providers because customers' Internet activity is "fractured" between devices, multiple Wi-Fi-hotspots, and different providers at home and work… 'customers who hop between ISPs on a daily basis often connect to the same networks routinely,' and as such over time, 'each ISP can see a substantial amount of that user's Internet traffic'." *Privacy Order* at para. 29-32, 53.

on a comment from Mozilla, an ESP that stands to gain from the FCC's sector-specific rules, to buttress its argument.[127]

The FCC's position that it should crack-down on ISPs due to the "unprecedented breadth" of data they may have access to does not acknowledge the arguably greater breadth of information that ESPs may have access to, which are not subject to the FCC's rules.[128] The FCC also declined to respond in its *Privacy Order* to the argument that ISPs often have limited insight into consumers' Internet use because consumers regularly switch to different BIAS providers as they use different devices, multiple Wi-Fi hotspots, and generally move from home to work throughout the day.[129]

The FCC requires BIAS providers to provide a way for consumers to affirmatively consent (opt-in) to the use, retention, and sharing of their data, whereas the FTC's privacy model encourages that Internet companies allow consumers to opt-out of the use, retention, and sharing of their data, and places special requirements on sensitive data.[130] The FCC's Privacy Rules require ISPs to ask permission of their customers to collect and use personal information; however, the scope of what constitutes personal information is overly broad.[131] The FTC and the FCC's frameworks differ in that the FTC's priority is security, whereas the FCC's priority is privacy.[132] The FTC appropriately focuses more on security, including PII, whereas the FCC focuses more on privacy, which is considerably more preferential than security which is primarily about safety.[133]

The newly adopted FCC broadband consumer privacy rules and the previously established FTC privacy protection policies, which apply to non-BIAS Internet businesses, appear to present multiple problems. First, it appears at best confusing and at worst unfair to customers for the FCC and the FTC to have inconsistent privacy protection practices.[134] Second, the

127. "The strength of the Web and its economy rests on a number of core building blocks that make up its foundational DNA. When these building blocks are threatened, the overall health and well-being of the Web are put at risk. Privacy is one of these building blocks." *Privacy Order* at para. 37.

128. *See, e.g.*, Peter Swire, Associate et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* at 24-25 (May 27, 2016) (The Institute for Information Security & Privacy at Georgia Tech, Working Paper) [hereinafter Swire Working Paper]; *see generally*, Andreea M. Belu, *The Massive Data Collection by Facebook – Visualized*, Data Ethics (June 26, 2017), https://perma.cc/DQ9X-MXJ6.

129. *See generally, Privacy Order*; Swire Working Paper at 3 ("[T]he average internet user has 6.1 connected devices, many of which are mobile and connect from diverse and changing locations that are served by multiple ISPs.").

130. *Privacy Order* at para. 9; FTC Report at vii-viii.

131. *Privacy Order* at para. 9; FTC Report at vii-viii, 15.

132. *See generally*, *Privacy Order*; FTC REPORT. Pai Dissenting Statement at 2 (commenting that the order is not "data-driven" but instead creates "corporate favoritism").

133. FTC REPORT at 18; *Privacy Order* at para. 1, 92, 134.

134. "I agreed with my colleague that consumers have a 'uniform expectation of privacy' and that the FCC thus 'will not be regulating the edge providers differently' from ISPs. I agreed that 'consumers should not have to be network engineers to understand who is collecting their data and they should not have to be lawyers to determine if their information is protected.'" Pai Dissenting Statement at 1.

inconsistent rules are unfair to businesses.[135] To the extent a business's ability to collect data on a customer is a problem, ESPs could potentially collect more data than their ISP counterparts.[136] For example, when a user checks her Gmail or uses Instagram multiple times a day, each time the user logs in to either Instagram or Gmail, both ESPs can track the user's browsing activity regardless of the ISP used in the transaction.[137] Conversely, the relevant ISPs involved in an individual's Gmail and Instagram activity are likely exposed to only a fraction of the user's Internet activity.[138] This is because a user may access ESPs using a variety of ISPs as she uses different devices on different Wi-Fi hotspots at home, work, and public spaces throughout the day.[139] Third, the FCC's Privacy Order does not appear to protect consumers' privacy in a substantial way, especially because edge providers, which are not subject to FCC regulations, are likely to have more private information from consumers than ISPs, which do not fall under the FCC's jurisdiction.[140]

Given that Internet data security is important to the government, private companies, and consumers,[141] it is essential that the federal government establish clear and reasonable online privacy policies that adequately protect consumers without needlessly stifling corporate competition or innovation. The Consumer Technology Association argued in its comment to the Privacy NPRM that "[b]y setting such stringent restrictions, consumers likely will miss out on what could otherwise be welcomed opportunities, such as receiving discounts, offerings, and information about new services, or even enjoying customized user experiences based on data collected."[142] The problems presented by the Privacy Order are threefold.[143] The FCC and FTC's respective online privacy rules are inconsistent such that they are confusing

135. Pai Dissenting Statement at 2 (order is not data-driven, and creates corporate favoritism).

136. Swire Working Paper at 4, 8 (non-ISPs have unique insights into "user activity" via "many contexts," including "social networks, search engines, webmail, and messaging, operating systems, mobile apps, interest-based advertising, browsers, Internet video, and e-commerce").

137. *Id*. at 4. This concept is referred to as "cross-context tracking." Cross-context tracking is dominated by non-ISPs. Services provided by non-ISPs that dominate cross-context tracking include social networks, search engines, webmail and messages, operating systems, mobile apps, interest-based advertising, browsers, internet video, and e-commerce.

138. *Id.*

139. *Id.*; "Nothing in these rules will stop edge providers from harvesting monetizing your data, whether it's the website you visit or the YouTube videos you watch or the emails you send or the search terms you enter on any of your devices." Pai Dissenting Statement at 2.

140. Pai Dissenting Statement at 1-2 (ESPs are currently "dominant" in online advertising marketing, and the Privacy Order doesn't stop ESPs from "harvesting or monetizing" data).

141. *See generally*, Alden Abbot, *The Federal Gov't's Appropriate Role in Internet Privacy Regulation*, THE HERITAGE FOUNDATION (Oct. 27, 2016), https://perma.cc/VWJ2-EPMB.

142. Comment of Consumer Technology Association at 9-10, *Privacy NPRM*.

143. *Privacy Order*.

to consumers,[144] unfair to businesses, and harmful to consumers, ESPs, and ISPs.[145] To understand why the Privacy Order is an inappropriate response to an arguably nonexistent harm, one must first understand the legal framework for Internet service businesses, including ISPs, and their respective histories relating to privacy rules and regulations.

1. The Evolution of the Open Internet Order and its Impact on ISP Privacy Rules

The FCC did not have the authority to enact rules applicable to Title II common carriers, which include BIAS, until the agency adopted the Protecting and Promoting the Open Internet Order (Open Internet Order) on February 26, 2015.[146] The Open Internet Order reclassified wired and mobile BIAS as telecommunications services.[147] More specifically, the reclassification subjected BIAS to several new rules and to certain provisions of Title II of the Communications Act.[148] The Open Internet Order did not focus on privacy; however, it provided the necessary legal groundwork for the Privacy Order.[149]

Prior to the Open Internet Order, the FCC treated BIAS as a largely unregulated information service.[150] In *National Cable & Telecommunications Ass'n v. Brand X*, the Supreme Court upheld the FCC's decision to classify cable broadband service as an information service.[151] The Court also found that the definitions of telecommunication service and information service in the Communication Act were ambiguous, and that the FCC reasonably interpreted the ambiguous provisions.[152] However, after reassessing the nature of BIAS, in addition to changes in consumer perception since *Brand X*, the FCC reclassified wired and broadband BIAS as a telecommunication service.[153] This reclassification included interconnection agreements between ISPs and ESPs within the scope of the newly-regulated broadband service.[154]

---

144. "I agreed with my colleague that consumers have a "uniform expectation of privacy" and that the FCC thus "will not be regulating the edge providers differently" from ISP. I agree that "consumers should not have to be network engineers to understand who is collecting their data and they should not have to be lawyers to determine if their information is protected." Pai Dissenting Statement at 1.

145. Pai Dissenting Statement at 3-4 (order is not data-driven, and creates corporate favoritism); Ohlhausen Address at 5.

146. *2015 Open Internet Order*, *supra* note 18, at para. 5, 25.

147. *2015 Open Internet Order*, *supra* note 18, at para. 29.

148. *U.S. Telecomm. Ass'n v. FCC*, 825 F.3d 674, 675 (D.C. Cir. 2016) (rejected numerous petitions for review and upheld the 2015 Open Internet Order).

149. KATHLEEN ANN RUANE, CONG. RESEARCH SERV., R40234, NET NEUTRALITY: THE FCC'S AUTHORITY TO REGULATE BROADBAND INTERNET TRAFFIC MANAGEMENT 6 (2014), https://perma.cc/9KV3-5F8P.

150. *See* Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 976 (2005) (upholding BIAS classification as information service).

151. *Id.* at 974.

152. *Id.* at 986-87.

153. *See 2015 Open Internet Order*., 355.

154. *Id.* at para. 29.

In *U.S. Telecomm. Ass'n v. FCC* the Court of Appeals for the D.C. Circuit upheld the Open Internet Order, specifically the FCC's reclassification of broadband services as telecommunications services subject to common carrier regulation under Title II of the Communications Act of 1934.[155] By upholding the Open Internet Order in its entirety, the D.C. Circuit essentially upheld nearly "open-ended power by the FCC to regulate BIAS", including BIAS rate regulation, regulation of when and how broadband networks exchange traffic, and "general conduct" regulation of network management decisions by broadband providers.[156]

2. The FTC has Long Been the Nation's Premier Privacy and Data Security Enforcement Agency

To understand the inappropriateness of the FCC's new privacy rules, it is instructive to understand the FTC's already existing high-functioning model. The primary law enforced by the FTC is the FTC Act which prohibits "unfair" and "deceptive" acts or practices in or affecting commerce.[157] Under Title 5 of the FTC Act, the FTC has brought data security enforcement actions against *inter alia* major ESPs like Google and Facebook, as well as violators of the FCRA, and online advertising networks that failed to honor consumers' opt-out choices.[158] A misrepresentation or omission under the FTC Act is deceptive if it is both material and likely to mislead consumers acting reasonably under the circumstances.[159] Additionally, an act or practice is unfair under the FTC Act if it causes, or is likely to cause, substantial injury that is not reasonably avoidable by consumers, as well as not outweighed by any benefits to consumers or competition generally.[160]

While the FCC has just begun its ISP regulation, the FTC has long been the nation's premier privacy and data security enforcement agency, bringing over 500 enforcement actions regarding the privacy and security of customer information.[161] Moreover, the FTC has extensive experience with actions against ISPs and against some of the most powerful Internet companies.[162] Some of the many companies under FTC orders include Microsoft, Facebook,

---

155. *See* Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 976 (2005).

156. *2015 Open Internet Order*; Seth L. Cooper, *DC Circuit Upholds Open-Ended Power to Regulate Broadband*, The Federalist Society (June 15, 2016), https://perma.cc/26DJ-39ZS.

157. An act or practice is "unfair" if it causes, or is likely to cause, substantial injury that is not reasonably avoidable by consumers, and not outweighed by other benefits to consumers or competition. 15 U.S.C. § 45(a) (2012); *See* FTC Policy Statement on Unfairness, *appended to Int'l Harvester Co*., 104 F.T.C. 949, 1070 (1984), *available* https://perma.cc/YG4Y-RU2Y; 15 U.S.C. §45(n) (2012).

158. FTC REPORT at ii.

159. *Id.*

160. *Id.*

161. *See* Letter from Edith Ramirez, Chairwoman, FTC, to Věra Jourová, Commissioner for Justice, Consumers, and Gender Equality, European Commission, 3 (Feb. 23, 2016), https://perma.cc/2DJC-LGKQ.

162. https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises.

Google, Equifax, HTC, Twitter, Snapchat, and Wyndham Hotels.[163] The FTC also conducts "extensive consumer and business outreach and guidance, coordinate[s] workshops to foster discussions about emerging privacy and data security issues, coordinate[s] on international privacy efforts, and advocate[s] for public policies that protect privacy, enhance security, and improve consumer welfare."[164] In a broad array of cases, "the FTC has alleged that companies" of varying sizes "made deceptive claims about how they collect, use, and share consumer data; failed to provide reasonable security for consumer data; deceptively tracked consumers online; spammed and defrauded consumers; installed spyware or other malware on consumers' computers; violated … telemarketing rules; shared highly sensitive, private consumer data with unauthorized third parties; and publicly posted such data online without consumers' knowledge or consent."[165] The FTC is so well-versed in the issues of privacy and consumer protection that it distributes educational materials on a host of topics, including mobile applications (apps), children's privacy, and data security.[166] The FTC's most recent business education program is the "Start with Security" initiative, which includes new guidance for businesses on the lessons learned from the FTC's data security cases, as well as seminars across the nation.[167]

3. The Privacy Order Demonstrated the Expanded Scope of the FCC's New Privacy Authority, Including a Broader Definition of the Types of Data Needing Special Protections

The Privacy Order established new legal obligations for ISPs.[168] The new requirements apply to customer proprietary information, a newly defined term which includes "individually identifiable CPNI, personally identifiable information and content of communications."[169] The Privacy Order also

163. *See generally,* Privacy and Security Cases, FTC, https://perma.cc/Y46E-LH6V.

164. *Statement of FTC Commissioner Maureen K. Ohlhausen Regarding Comment of the Staff of the Bureau of Consumer Protection of the FTC* , *Privacy NPRM* at 1 (May 27, 2016), https://perma.cc/767V-U759 [hereinafter Ohlhausen *Privacy NPRM* Statement]; *see, e.g.*, FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES (Jan. 2016), https://perma.cc/R7FC-MCYL [hereinafter Big Data Report]; FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (June 2015), https://perma.cc/78JP-4XUB.

165. Comment of the Staff of the Bureau of Consumer Protection of the FTC at 2-3, *Privacy NPRM*, https://perma.cc/3EXY-7WRX.

166. *See generally* Press Release, *FTC Kicks Off "Start with Security" Business Education Initiative* (June 30, 2015); FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (June 2015), https://perma.cc/78JP-4XUB; *Mobile App Developers: Start with Security*, FTC, https://perma.cc/8ABD-MSHX; *Protecting Your Child's Privacy Online*, FTC, https://perma.cc/QHQ8-UUYC.

167. *See generally* Press Release, *FTC Kicks Off "Start with Security" Business Education Initiative* (June 30, 2015); FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (June 2015), https://perma.cc/78JP-4XUB.

168. *Privacy Order* at para. 27.

169. *Privacy Order* at para. 85.

broadly defines a customer as any current or former subscriber to a telecommunications service, or an applicant for a telecommunications service, meaning that an ISP's duty to protect customer PI begins before service starts and continues after service is terminated.[170] As defined in Section 222(h)(1) of the Communications Act, CPNI is information that relates to "the quantity, technical configuration, type, destination, location, and amount of use" of telecommunications service that is provided by the customer in the context of a carrier-customer relationship.[171] Consistent with its past binding and guidance documents, the FCC's Privacy Order did not provide a comprehensive list of CPNI, but instead provides that CPNI in the broadband context includes but is not limited to the following: broadband service plans, geolocation, Mac addresses and other device identifiers, IP addresses and domain name information, traffic statistics, port information, application header, application usage, application payload, and customer premises equipment and devise information.[172]

The FTC has developed its privacy program using its long-established principles of combatting unfairness and deception.[173] Due to the FTC's focus on long-established principles of unfairness and deception, the FTC's privacy program focuses on the sensitivity of consumer data and the specific promises made about data collection and use, instead of the type of entity that collects or uses the data.[174] Notably, the FTC's definition of sensitive customer data includes Social Security numbers, financial, health, children's and geographical information, but does *not* include content of communications, web browsing activity or application usage history, which are included in the FCC's Privacy Order.[175]

4. The Privacy Order Sets New Transparency and Notice to Consumer Requirements for ISPs

The Privacy Order places the following new requirements on all ISPs: (1) provide privacy notices that explain what user information they collect, how that information is used, in what context it is shared, and the types of entities it is shared with; (2) "inform customers" of their "rights to opt-in or opt-out of the use or sharing of their information"; (3) "present their privacy notices to customers at [both] the point of sale" and after in an "easily accessible" manner; and (4) "give customers advance notice of material changes" to the ISP's "privacy policies."[176] "Heightened disclosures" are

170. *Id.* at 64.2002(e) (Definition of 'Customer').

171. 47 U.S.C. § 222(h)(1) (2012).

172. *Privacy Order* at para. 53.

173. The FTC's case-by-case application of these general principles has major advantages over a prescriptive rulemaking approach. The FTC's approach minimizes the regulator's knowledge problem, fosters incrementalism, and focuses limited resources on addressing consumer harm. *See* Maureen K. Ohlhausen, *The FCC's Knowledge Problem: How to Protect Consumers Online*, 67 FED. COMM. L.J. 203 (2015), https://perma.cc/Z9XM-U2MC.

174. FTC REPORT at 24.

175. FTC REPORT at 15; *Privacy Order* at para. 9.

176. *Privacy Order* at para. 125.

necessary under the Privacy Order for what the Commission calls "pay for privacy plans," which is when an ISP offers discounts or other incentives in exchange for a customer's express affirmative consent to the use and sharing of their personal information.[177]

H. The Privacy Order Sets New Customer Choice and Consent Rules, which Includes a Three-tiered Approach: Opt-in, Opt-out, and Inferred Consent

Before an ISP can use or share customer PI under the Privacy Order, it must obtain that individual's consent.[178] The three allowable consent mechanisms under the Privacy Order are: opt-in, opt-out, and inferred consent.[179] All the consent mechanisms apply to different types of customer PI. The appropriate method depends on the information's sensitivity and its treatment under the statute. For example, opt-in consent requires affirmative permission from the customer to use or share "sensitive" customer PI.[180] Opt-in consent is also necessary for retroactive changes to an ISP's privacy policies.[181] Secondarily, opt-out consent is required for the use and share of all non-sensitive PI.[182] Thirdly, inferred consent is permissible in limited circumstances. For example, ISPs may infer consent to use customer information to provide the underlying service, bill for that service, to prevent fraudulent use of the ISP's network, and other purposes specified in the statute.[183]

I. The Most Significant Difference Between the FCC's Three-tiered Consent Framework and the FTC's Existing Privacy and Data Security Guidelines is the Privacy Order's Treatment of Web Browsing and Application Usage History

The most significant difference between the consent framework articulated in the Privacy Order and the FTC's existing privacy and data security is the order's treatment of web browsing activity and application usage history.[184] The FTC has never considered this information *per se* sensitive, and therefore, has never required opt-in consent for use or

177. *Id.* at para. 298-303.
178. *Id.* at para.192-195.
179. *Id.* at para. 365.
180. *Id.* at para. 193.
181. *Id.* at para. 195.
182. *Id.* at para. 194.
183. *Id.* at para. 201.
184. *Privacy Order* at para. 9; FTC Report at vii-viii.

sharing.[185] The Privacy Order dramatically diverges from the FTC's position on web browsing and app usage history.[186] In the Order, the FCC asserts that because ISPs have the unique ability to see all of a user's unencrypted traffic, that browsing and app usage history must be considered sensitive in the communications context and be subject to opt-in consent.[187] The FCC declines "to define a subset of non-sensitive web browsing and app usage history."[188] The Privacy Order also dismisses numerous commenters' arguments that the existence of encryption on websites and apps significantly decreases the potential amount of data an ISP may access.[189]

In contrast to the FCC's over-inclusive definition of sensitive data, the FTC considers the application of its privacy framework on a case-by-case basis. The FTC recognizes that Internet companies in the healthcare and financial services industries are also subject to other statutes, like "the Health Insurance Portability and Accountability Act ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and the Gramm-Leach-Bliley Act ("GLBA")," which "impose privacy protections and security requirements through legal obligations" on companies.[190] Since the FTC's privacy framework is intended to encourage best practices, rather than create conflicting or duplicative requirements, "to the extent that components of the [FTC's privacy framework] exceed, but do not [contradict] existing statutory requirements, [companies] covered by those statutes should view the [FTC's framework] as best practices to promote consumer privacy."[191]

Thus, according to the FTC's definition of sensitive data, the FCC's rule would require opt-in consent for many uses of non-sensitive consumer data by ISPs, as compared to the FTC's sensitivity framework.[192] The opt-in consent system that the FCC advocates is similar to the standards employed in Europe, where citizens have a "right[s] to make search engines remove

185. FTC REPORT at 16-17; CTIA Comment ("To justify diverging from the FTC's framework and defining Web browsing history as 'sensitive,' the commission… cherry-picked evidence in an attempt to show that ISPs have unique and comprehensive access to consumers' online information."); Rather than finding web browsing *per se* sensitive, the FTC considers if the types of data the software will monitor, record, or transmit are "clearly and prominently" communicated to users. Sears Settles FTC Charges Regarding Tracking Software, FTC (June 4, 2009), https://perma.cc/J4LJ-2CQA.

186. *Privacy Order* at para. 9; FTC Report at vii-viii.

187. *Privacy Order* at para. 134 - 135. .

188. *Id.* at para. 15, 181.

189. *Compare Privacy Order* at para. 186 ("[T]he existence of encryption on websites or even in apps does not remove browsing history from the scope of sensitive information… [E]ncryption is far from fully deployed; the volume of encrypted data does not represent a meaningful measure or privacy protection…"), *with* Swire Working Paper at 3 ("We present new evidence on the rapid shift to encryption, such as the HTTPS ersion of the basic web protocol. Today, all of the top 10 web sites either encrypt by default or upon user log-in, as do 42 of the top 50 stes… Encryption such as HTTPS blocks ISPs from having the ability to see users' content and detailed URLs.").

190. FTC REPORT at 16, 58.

191. *Id.*

192. *Id.* at 47, 58-59; Comment of the Staff of the Bureau of Consumer Protection of the FTC at 2-3, *Privacy NPRM,* https://perma.cc/5SMW-5DCW.

search results about themselves, including links to news articles and other information."[193] The European Union's broad embrace of opt-in policies, and its recognition of the "right to be forgotten" has proven highly problematic for businesses and challenging to execute.[194] However, the FTC recommends, but does not require, opt-in consent for unexpected collection or use of consumers' sensitive data, such as Social Security numbers, financial information, and information about children. [195]

While the FTC's policies are better than those in the FCC's Privacy Order, they are not without fault. The FTC urges that companies adopt industry best practices, but falls short of providing a clear delineation of what duties an ISP owes to its consumers; the gaps in the FTC's privacy framework present opportunities for Congressional action.

Unlike the FCC's approach, the FTC's approach reflects the fact that consumer privacy preferences differ greatly depending on the type of data and its use. The FTC's research and the Pew Research Center have found that consumers overwhelmingly object to entities accessing their sensitive data without permission, but do not object to the access of their non-sensitive data.[196] Notably, to the extent consumers are concerned about entities accessing their financial and medical data without permission, both financial institutions and healthcare entities are subject to heightened statutory standards.[197]

1. The FTC's Online Privacy Rules are Designed to Minimize the Burden on Consumers and Business, Whereas the FCC's Approach Needlessly Creates a Burden

The FTC approach to privacy takes into consideration that obtaining consent can be burdensome for consumers and business. Reading a notice about privacy and making a decision based on that notice takes time, which,

193. Daphne Keller & Bruce D. Brown, *Europe's Web Privacy Rules: Bad for Google, Bad for Everyone*, N.Y.TIMES (Apr. 25, 2016), https://perma.cc/QP4D-PQJT.

194. *Id.*

195. *Compare Privacy Order* at para. 125,*with* FTC REPORT at vii-viii; Comment of FTC Staff of the Bureau of Consumer Protection 2-3, *Privacy NPRM,* https://perma.cc/5SMW-5DCW.

196. See, Remarks of Maureen K. Ohlhausen, 2016 Advertising and Privacy Law Summit (June 8, 2016), 5 n.11, https://www.ftc.gov/system/files/documents/public_statements/955183/160608kellydrye.pdf (A recent Pew survey and focus groups testing consumer privacy preferences with regard to six different scenarios found 17% of polled rejected all the scenarios, 4% accepted all the scenarios, and the substantial majority indicated that at least one of the scenarios was potentially acceptable. Lee Rainie & Maeve Duggan, Privacy and Information Sharing, PEW RESEARCH CENTER (Dec. 2015), http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/).

197. FTC REPORT at 16 (statutes such as HIPAA, HITECH, and GLBA already impose privacy protections and security requirements through legal obligations on companies regulated by the FTC).

"in the aggregate, can be quite substantial."[198] The FTC's policy is based on the theory that regulations should impose costs in a way that maximizes benefits and simultaneously minimizes costs.[199] In its enforcement capacity, the FTC generally urges an opt-out approach for non-sensitive information, and an opt-in approach for uses of sensitive information.[200] Clarifying the FTC's position on regulations and their corresponding transactional costs, former FTC Chairman Tim Muris and former Director of the FTC's Bureau of Consumer Protection Howard Beales stated:

> Consumers rationally avoid investing in information necessary to make certain decisions ... when their decision is very unlikely to have a significant impact on them ... Default rules should be designed to impose those costs on consumers who think they are worth paying. An opt-out default rule means that consumers who do not think that decision making costs are worthwhile do not need to bear those costs. Consumers who care intensely, however, will face the costs of making a decision.[201]

The FTC also chooses not to impose regulation defaults that do not coincide with consumer preferences, because doing so imposes an unnecessary cost to consumers and businesses without improving consumer outcomes.[202] Additionally, a broad opt-in requirement could burden and negatively affect industry innovation, growth, and competition as businesses must reallocate resources to comply with regulations.[203]

Moreover, lumping app usage histories and "their functional equivalents" in the same category of sensitivity as Social Security numbers, as the Privacy Order does, is too broad of a category that will create unnecessary transaction costs for businesses and consumers.[204] For example, under the FCC's approach, a customer's medical and financial records would require the same degree of privacy as a customer's shopping or media preferences if that information is shared with a BIAS, because shopping and

198. Remarks of Maureen K. Ohlhausen, 2016 Advertising and Privacy Law Summit (June 8, 2016), https://www.ftc.gov/system/files/documents/public_statements/955183/160608kellydrye.pdf.

199. Remarks of Maureen K. Ohlhausen, 2016 Advertising and Privacy Law Summit (June 8, 2016), https://www.ftc.gov/system/files/documents/public_statements/955183/160608kellydrye.pdf.

200. Ohlhausen *Privacy NPRM* Statement 2.

201. J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 115 n.20 (2008).

202. Ohlhausen *Privacy NPRM* Statement 2.

203. *See* Daniel Castro & Alan McQuinn, *The Economic Costs of the* European *Union's Cookie Notification Policy*, THE INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (Nov. 2014) at 7, https://perma.cc/5QBL-JRHE; PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, REPORT TO THE PRESIDENT: BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE x-xi (May 2014) ("[A] policy focus on limiting data collection will not be a broadly applicable or scalable strategy – nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth.").

204. *Privacy Order* at para. 9.

media preferences fit in the category of "web browsing and application usage history."[205]

III. ANALYSIS

The FCC's Privacy Order provides that "privacy rights are fundamental because they protect important interests" including "freedom from identity theft, financial loss, or other economic harms, as well as concerns [regarding] intimate, personal details."[206] The FTC Bureau of Consumer Protections Board echoed the FCC's sentiment in its Comment on the FCC's Privacy NPRM, maintaining that the FCC's goal of promoting transparency, consumer choice, and security is laudable.[207] The Privacy Order and the FTC's Comment to the Privacy Order provide that there is universal agreement that Internet data security rules are necessary. However, the FCC is wrong in its assessment of the potential risks and harms to businesses and consumers. Manifesting the concerns of many commenters in response to the FCC's Privacy NPRM, the Privacy Order conceives of an exaggerated possible harm and is overly broad in its imposition of burdensome transactional costs on businesses and customers. Requiring ISPs to implement new customer consent platforms in accordance with the Privacy Order will create a new cost, which will ultimately be absorbed by consumers.[208] Even though the FCC and the FTC have jurisdiction over different types of Internet companies, the FCC failed to demonstrate why it was necessary for it to diverge from the long-standing and successful policies of the FTC.

Although the FTC is in a better position than the FCC to enforce Internet data security, neither agency has flawless online privacy policies.[209] While the FCC's consumer protection-focused model employs reasonableness standards and considers industry-wide best practices, it leaves exactly what a company must do to avoid liability somewhat ambiguous.[210] It is unquestionable that Internet data security is important. Americans should be able to use the Internet freely with a reasonable expectation that their confidential information, like financial and medical data, will be kept private and that there is transparency regarding the level of privacy afforded to communication via the Internet. It follows that the government should create

205. *Id.*

206. *Id.* at para. 1.

207. Comment of FTC Staff of the Bureau of Consumer Protection at 2-3, *Privacy NPRM,* https://perma.cc/5SMW-5DCW (acknowledges that FCC recognizes the importance of protecting consumer privacy ands "commends the FCC for its attention to these issues" and provides comments, based on the FTC's decades of experience).

208. "The goal of consumer protection enforcement isn't to make headlines; it is to make harmed consumers whole and incentivize appropriate practices. The costs imposed by a regulator on a legitimate, non-fraudulent company are ultimately born by its consumers. If enforcement action imposes costs disproportionate to the actual consumer harm, that enforcement action may make consumers worse off if prices rise or innovation slows." Ohlhausen Address at 5.

209. See generally, Privacy Order; FTC REPORT.

210. Ohlhausen Address at 5; FTC, PRIVACY & DATA SECURITY UPDATE 16 (2016), https://perma.cc/3GSY-BNJ6.

and enforce standards that protect Internet consumers' privacy while also recognizing the potential burdens that overregulation can place on businesses, primarily in the form of cumbersome and costly unfunded mandates for things like opt-in or out-out platforms. An appropriate data security legal framework will ensure that customers' private information is secure and that consumers are able to choose what types of information they want kept private, aside from the data that is already statutorily classified as sensitive, like financial and medical matters.

Data security breaches can cause serious harms; however, the FCC's Privacy Order goes too far and creates harms in the form of imposing unnecessary transaction costs on businesses and consumers, and potentially confusing customers. Because the FTC provides more of a patchwork common law than a clear set of standards that ESPs must abide by, as will be discussed in subsequent sections, the ideal solution is for Congress to act to streamline Internet data security policies under the FTC's jurisdiction.

A. The FCC's Privacy Order Creates Confusion for Customers

An Internet user should not need to be a lawyer or network engineer to understand how her privacy will or will not be protected. "For the last two decades, the United States has embraced a technology-neutral framework for online privacy," meaning that the framework administered by the FTC applied across all sectors of the Internet.[211] What this meant for customers is that regardless of whether they were using an ESP, like Google or Facebook, or a BIAS provider like Comcast or AT&T, the consumer had a uniform expectation of privacy. Prior to the FCC's entry into online privacy regulation, the FTC's unified approach allowed Internet users to "rest assured knowing that a single and robust regulatory approach" protected online data.[212]

By failing to parallel the FTC's approach, the FCC has created unnecessary confusion for customers. The FCC's recent Privacy Order requires users to opt-in to sharing information with BIAS providers, regardless of the sensitivity of the information. However, because a BIAS simply provides the infrastructure necessary for ESPs to function and interface with consumers, a reasonable customer may wrongly assume that when she opted-in to sharing data with her BIAS, she also opted-in to sharing data with the ESP she used by way of her BIAS provider. This not only will create confusion for customers, but will also likely create a customer service problem for BIAS and ESP companies. Customers will likely call their BIAS and ESPs concerned about their respective compliance because the FCC's opt-in/opt-out model based on the type of entity rather than the type of content is confusing. It is logical for the FCC to parallel the FTC's approach as closely as possible because doing so would allow consumers to better understand how their information is and is not protected under the law. Moreover, consumers

211. Pai Dissenting Statement at 1; *Privacy Order* at 209.
212. *Id.*

have a "uniform expectation of privacy" and an expectation that the FCC will not regulate ISPs differently from ESPs.[213]

B. The FCC's Privacy Order is Unfair to Businesses

It is problematic for the FCC and the FTC to treat ISPs and ESPs differently, especially considering the average Internet user does not understand the highly technical distinction between the two types of businesses. It is unfair to subject one sector of industry to a significantly increased burden compared to another sector of industry. Also, if the FCC is so concerned about privacy and security, it should focus on protecting sensitive information. Not only is it unfair to target BIAS providers and not ESPs, but the Privacy Order also does not serve a purpose of helping customers because it is overly broad in its classification of potentially sensitive data, ultimately making it more difficult for consumers to experience the benefits of subsidized costs by third parties, and the corresponding targeted advertisements and deals that are often associated with third party advertisers. In addition, to the extent BIAS and ESPs should be treated differently under the law, ESPs are technologically able to collect more sensitive information than ISPs. For instance, financial institutions, retail, and social media websites are predominantly ESPs, not ISPs, and are therefore obligated to follow the FTC's more lenient and reasonable approach.[214] The FTC takes a flexible approach to data security, assessing reasonableness based, among other things, on the sensitivity of the information collected, the measures the company has implemented to protect such information, and whether the company acted to address and prevent "well-known and easily addressable security vulnerabilities."[215]

Moreover, the FTC has a track record of enforcing data security. In February 2017, under a Republican-led FTC, "VIZIO, Inc., one of the world's largest manufacturers and sellers of Internet-connected 'smart' televisions, agreed to pay $2.2 million to settle charges by the FTC and the Office of the New Jersey Attorney General that it installed software on its TVs to collect viewing data on 11 million consumer TVs without the consumers' knowledge or consent."[216] In December 2016, Turn Inc., a California-based company which enables sellers to "target digital advertisement to consumers, agreed to settle FTC charges that it deceived consumers by tracking them online and through their mobile applications, even after consumers opted-out of such tracking."[217] As part of the settlement, consumers must be able to limit

213. *Id.*

214. Maureen K Ohlhausen (fn 47 above).

215. FTC REPORT at n.108.

216. Press Release, *VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges it Collected Viewing Histories on 11 Million Smart Televisions without Users'* Consent, FTC (Feb. 6, 2017), https://perma.cc/PS98-KNK9.

217. Press Release, *Digital Advertising Co. Settles FTC Charges it Deceptively Tracked Consumers Both Online and Through Their Mobile Devices*, FTC (Dec. 6, 2016), https://perma.cc/8R54-UYH4.

targeted advertisements on Turn Inc.'s website.[218] Also in December 2016, the operators of AshleyMadison.com, a dating website based in Canada, "agreed to settle [FTC] and state charges that they deceived consumers and failed to protect 36 million users' account and profile information in relation to a [major] July 2015 data breach of their network".[219] These are just a few examples of the FTC appropriately exercising its enforcement capacity to protect consumers.

The Privacy Order attempts to justify its crackdown on ISPs by saying that "edge providers only see a slice of given consumer Internet traffic" whereas "a BIAS provider sees 100 percent of a customer's unencrypted Internet traffic."[220] However, this belief is fundamentally flawed because ISPs' "access to data is not comprehensive" due to "technological developments" that "place substantial limits on ISPs' visibility." Additionally, an ISP's "access to user data is not unique" because "other companies often have access to more information and a wider range of user information than ISPs."[221]

ESPs have a strong interest in studying both identifiable and non-identifiable consumer Internet traffic because doing so allows them to better-cater to prospective and current customers, ultimately helping their businesses as consumers choose to return to their ESPs.[222] The Obama Administration discussed the benefits of ESP's capacity to collect and use "personal information in its 2014 Big Data report."[223] The report maintained that benefits include "improved fraud detection and cybersecurity, and 'enormous benefits' associated with targeted advertising" that allows consumers to reap "the benefits of a robust digital ecosystem that offers a broad array of free content, products, and services."[224]

FCC Chairman Pai maintains that the amount of data collected by ESPs daily is staggering.[225] Pai also asserts that the FCC simply wants to treat ISPs different from ESPs and is, therefore, claiming that ESPs only see a "slice" of

---

218. *Id.*

219. *Operators of AsheleyMadison.com Settle FTC, State Charges Resulting from 2015 Data Breach that Exposed 36 Million Users' Profile Information*, FTC (Dec. 14, 2016),https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting.

220. *Privacy Order* at para. 30.

221. When an ESP encrypts its website, it limits visibility to the ISP. As of 2016, "all of the top 10 websites either encrypt by default or upon user log in, as do 42 of the top 50 sites… There clearly can be no 'comprehensive' ISP visibility into user activity when ISPs are blocked from a growing majority of user activity" due to encryption. Swire Working Paper at 3. ESPs are increasingly gathering commercially valuable information about user activity via multiple contexts, such as: social networks, search engines, webmail and messaging, operating systems, mobile apps, internet-based advertising, browsers, Internet video, and e-commerce. Swire Working Paper at 4.

222. *See generally*, BIG DATA REPORT at 39.

223. "Big Data: Seizing Opportunities, Preserving Values," Executive Office of the President, The White House (May 2014).

224. BIG DATA REPORT at 40-41, 50.

225. https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A5.pdf.

users' online data.[226] However, ESPs access far more than a "slice" of customer's data.

> The FCC describes ISPs as the most significant component of online communications that poses the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem. Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services. However, all pathways lead to essentially one Internet search company and one social network company. Privacy rules for ISPs are important and necessary, but it is obvious that the more substantial threats for consumers are not the ISPs.[227]

Additionally, refuting the FCC's assertion that ISPs rather than ESPs must be reined in because ESPs have access to significantly less data compared to their ISP counterparts, are several recent news reports indicating the significant capacity of particularly powerful ESPs regarding consumer protection. In his dissenting statement, then-Commissioner Pai highlighted the following news headlines: "Google quietly updates privacy policy to drop ban on personally identifiable web tracking,"[228] "Privacy Debate Flares With Report About Yahoo Scanning Emails,"[229] "Apple keeps track of all the phone numbers you contact using iMessage,"[230] "Twitter location data reveals users' homes, workplaces,"[231]and "Amnesty International rates Microsoft's Skype among worst in privacy."[232] Thus, contrary to the FCC's position in its Privacy Order, ESPs arguably have more insight into consumer data than ISPs.[233]

Since the FCC has not presented a compelling reason as to why ISPs should be subjected to more stringent standards than ESPs, aside from the "slice" argument, which is refuted by data, the FCC's regulation of ISPs appears to be corporate favoritism because it enables ESPs to transact business in a much less cumbersome and expensive way compared to their ISP counterparts who must follow the FCC's rules and regulations.[234] If both

---

226. Pai Dissenting Statement at 2.

227. *Privacy Order* at 210, citing EPIC Comments at 15.

228. https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A5.pdf; Anmol Sachdeva, *Google Quietly Updates Privacy Policy to Drop Ban on Personally Identifiable Web Tracking*, THE TECH PORTAL (Oct. 21, 2016), https://perma.cc/X6JN-3434.

229. Robert McMillan & Damian Paletta, *Privacy Debate Flares With Report About Yahoo Scanning Emails*, WSJ. (Oct. 5, 2016), https://perma.cc/F5T3-4KF4.

230. Oscar Raymundo, *Apple Keeps Track of All the Phone Numbers You Contact Using iMessage*, MACWORLD (Sept. 28, 2016), https://perma.cc/LVV5-HBNG.

231. Patrick Nelson, *Twitter Location Data Reveals Users' Homes, Workplaces*, NETWORKWORLD (May 18, 2016), https://perma.cc/G66N-HHH9.

232. Dennis Bednarz, *Amnesty International Rates Microsoft's Skype Among Worst in Privacy*, WINBETA (Oct. 23, 2016), https://perma.cc/4QQ8-WBGJ.

233. Pai dissent.

234. "Because the *Order* wants to treat ISPs differently from edge providers, it asserts that the latter only sees a "slice" of consumers' online data. This is not data-driven decision-making, but corporate favoritism." Pai Dissenting Statement at 2.

ISPs and ESPs have access to the same data about a consumer's Internet usage, why should the federal government give one company "greater leeway" to use it than the other?[235] Additionally, it does not make sense to require BIAS providers to follow more stringent rules because there are less BIAS providers than there are ESPs because consumers use multiple BIAS providers on a regular basis just like they use multiple ESPs on a regular basis. A customer may use different BIAS providers when she accesses the Internet on different devices on different Wi-Fi hotspots in different locations, such as home, work, or school.

The uneven regulations are especially unfair because for Internet businesses, access to consumer information creates a significant advantage. Not only does the FCC's argument fail to consider that ESPs have a significant interest in increasing the amount of data they collect on an individual, but the FCC also ignores the major and growing limitations on each ISP's visibility into consumer data, such as encryption of most web traffic and the tendency of consumers to switch continuously among different ISPs as they carry their devices from one network to the next.[236] One of the loudest critics of the FCC's position that ISP's should be punished for the comprehensive access they allegedly have to consumer's browsing history, is Peter Swire.[237] Swire was the Chief Counselor for Privacy, in the U.S. Office of Management and Budget under President Bill Clinton, and was Special Assistant to the President for Economic Policy under President Barack Obama.[238]

C. The FCC's Privacy Order is Not Helpful to Consumers

Prior to the FCC's entry into the online privacy enforcement space, the federal government, led by the FTC, has addressed online privacy by carefully balancing the costs of undue regulation against the need to protect consumers from a genuine privacy harm. The FTC's regime is a long-established flexible one that is effective and supported in large part by industry self-governance along with the FTC's statutory prohibitions against unfair or deceptive trade practices.[239] The FTC's system is beneficial to customers because, as was said in a 2012 White House Report, its approach relies on "multi-stakeholder processes to produce enforceable codes of conduct" that market participants

---

235. Ajit Pai, Chairman, FCC & Maureen Ohlhausen, Acting Chairman, FTC, *No, Republicans Didn't Just Strip Away Your Internet Privacy Rights*, Wash. Post (Apr. 4, 2017), https://perma.cc/TLM4-KZMK.

236. The FCC claims that even when web traffic is encrypted, an ISP can "infer" consumer information from unencrypted data such as top-level URLs and amount of data usage, but numerous industry leaders. *Compare Privacy Order* at para. 29, 186 *with* Swire Working Paper; CenturyLink Comments 5-12; Verizon Comments 17-24; AT&T Comments 13-30; CTIA Comments 114; T-Mobile Comments 5-7; Comcast Comments 26-29.

237. Swire Working Paper at 24-25.

238. *Id.*

239. *See* 15 U.S.C. § 45(b), (n) (2012)*; see also* Consumer Data Privacy in Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, J. of Privacy and Confidentiality 96, 98 (2012), http://repository.cmu.edu/cgi/viewcontent.cgi?article=1096&context=jpc.

can voluntarily incorporate into their privacy policies and thereby make subject to FTC enforcement.[240] However, if a business fails to adopt an industry standard policy as appropriate for their respective business, the FTC will judge any potential data breaches using a case-by-case standard.[241]

The FCC's increased regulations will have a negative impact on consumers because most consumers are not opposed to sharing information with Internet business in exchange for free or discounted services.[242] Former Obama FTC Chairman Jon Leibowitz disagreed with the FCC's proposal to prohibit ISPs from offering discounted services in exchange for customers opting-in to grant data collection and use.[243] Leibowitz believed the rules' prohibition of something that consumers don't find problematic will stifle the development of free online services, and other low cost resources, due to increased transactional costs.[244] Leibowitz suggested that instead the FCC could require a notice and choice regime, where, as "long as ISPs provide sufficient notice, users could have the choice of putting a value on their personal data."[245] This framework, according to Leibowitz, is consistent with the FTC's 2012 Privacy Report.[246] Furthermore, to the extent that a consumer is uncomfortable with providing data to Internet companies in exchange for potential benefits like targeted advertisements, many ESPs voluntarily allow consumers to opt-out of sharing such content.[247] Additionally, the FTC has taken enforcement actions against companies who did not act reasonably and consistent with industry best practices, given their particular circumstances,

---

240. WHITE HOUSE PRIVACY FRAMEWORK at 24 ("The United States relies primarily upon the FTC's case-by-case enforcement of general prohibitions on unfair or deceptive acts and practices. This approach helps develop evolving standards for handling personal data in the private sector.").

241. "The FTC's case-by-case application of these general principles has major advantages over a prescriptive rulemaking approach. The FTC's approach minimizes the regulator's knowledge problem, fosters incrementalism, and focuses limited resources on addressing consumer harm." *See* Maureen K. Ohlhausen, *The FCC's Knowledge Problem: How to Protect Consumers Online*, 67 FED. COMM. L.J. 203 (2015), https://perma.cc/Z9XM-U2MC.

242. "Indeed, one study found that, on average, Americans assigned a value of almost $1,200 per year to the package of free, ad-supported services and content currently available to them[.]" Thomas W. Hazlett & Joshua D. Wright, The Law and Economics of Network.

Neutrality, 45 IND. L. REV. 767, 770 (2012) (internal quotation marks omitted). In addition, "[m]ore than 85 percent of respondents said they preferred [that] ad-supported Internet model instead of paying for online content." *Zogby Poll: Americans Say Free, Ad-Supported Online Services Worth $1,200/Year; 85% Prefer Ad-Supported Internet to Paid*, DIGITAL ADVERTISING ALLIANCE (May 11, 2016), https://perma.cc/UJ7D-7MZ5.

243. John Eggerton, Former FTC Chair Has Issues with FCC's Opt-in CPNI Regime, Multichannel (Oct. 22, 2017, 5:48 PM EST) http://www.multichannel.com/news/fcc/former-ftc-chair-has-issues-fccs-opt-cpni-regime/404836.

244. *Id.*

245. *Id.*

246. *Id*.

247. The Network Advertising Initiative ("NAI") is the leading non-profit, self-regulatory body governing Internet advertising technology providers consisting of nearly 100 businesses as official members. The NAI's Code of Conduct provides that Internet companies should provide "a link to an Opt-Out Mechanism for Internet-Based Advertising." NAI Code of Conduct, NAI 6-7, https://perma.cc/PH3A-EJ8H (last accessed Apr. 11, 2017).

by not providing an opt-out mechanism.[248] However, Internet consumers are less likely to opt-in to sharing information when given the choice to do so.[249] Research conducted by *Wright Economic Analysis* found that "most consumers take the path of least resistance and click 'no' when presented with opt-in notices"; however, they do so not because they object to the use of their information, but because they don't want to take the time to understand the privacy notice.[250] There is also a benefit from the consumers' perspective to consenting to the use and/or sharing of their information because opting in enables a consumer to experience a more personalized Internet browsing experience, including access to discounts and other information that is consistent with her browsing history. [251]

Conversely, an opt-out method is preferable to an opt-in method because those who care greatly about their non-sensitive data can invest the time to understand the privacy options available to them and make an informed choice.[252] ESPs are currently not *per se* required by the FTC to offer an opt-out mechanism, unless otherwise required by law.[253] To accommodate the range of customer preferences concerning privacy, the FTC should require ESPs to make an opt-out mechanism available to consumers. Opt-out mechanisms allow those who care deeply about having enhanced privacy to choose how their data will be protected, while also not slowing down the transaction process or annoying what may be the majority of an ESP's consumers who do not want enhanced privacy.[254] Under the FCC's Privacy Order, those who are not concerned with the collection of their non-sensitive data will be bombarded with continuous opt-in messages.[255]

The Privacy Order's position is that distinguishing between "sensitive and non-sensitive categories [of data] is a fundamentally fraught exercise" that is not helpful to consumers.[256] The Privacy Order appears to administer regulations that do not distinguish between sensitive and non-sensitive information because doing so would be too difficult when, in actuality, ESPs distinguish between sensitive and non-sensitive data routinely. For instance,

---

248. ScanScout, Inc., C-4344 (Dec. 14, 2011) (consent order), https://perma.cc/8T2S-X7SC (requiring company to improve disclosure of its data collection practices and offer consumers a user-friendly opt out mechanism).

249. *Consumers Want Privacy, but Don't Take Advantage of Opt-Out Techs.,* HELP NET SECURITY (Feb. 26, 2014), https://perma.cc/RA7S-5SAM ("A majority of consumers worry about how marketers use their personal data, but 79 percent are more likely to provide personal information to what they consider a 'trusted brand,'… [W]hile consumers are not comfortable with being 'tracked' in a physical store, they tend to not read brands' privacy policies or take measures to opt-out of web tracking practices.").

250. Thomas W. Hazlett & Joshua D. Wright, *The Law and Economics of Network Neutrality*, 45 IND. L. REV. 767, 770 (2012).

251. See Lee Rainie & Maeve Duggan, Privacy and Information Sharing, PEW RESEARCH CENTER (Dec. 2015), https://perma.cc/9VDE-5XKF.

252. Privacy NPRM at 2.

253. See FTC Report at 16.

254. See Privacy NPRM at 2.

255. *Privacy Order* at para. 186-87 (Regardless of whether a user objects of her web browsing history from being used or shared, under the *Privacy Order* she must reply to opt-in messages provided by ISPs pursuant to the *Privacy Order).*

256. *Id.* at para. 187.

Google explains that, "[w]hen showing you personal ads, we will not associate an identifier from cookies or similar technologies with sensitive categories, such as those based on race, religion, sexual orientation, or health."[257] Online providers, like Google, rely on guidelines issued by industry self-regulatory organizations such as the Network Advertising Initiative for insight into which categories should remain "off-limits."

The FCC fails to properly establish that a harm is created if ISPs have access to non-sensitive data and, until the FCC is able to articulate such a harm, it is unfair to impose increased burdens on Internet businesses. Also, the FCC's Privacy Order is unnecessary because, as numerous "commenters pointed out, to the extent that web browsing and application usage data concerns sensitive information," like "health or financial records, it is already covered by the other categories" of the FTC Act.[258]

D. The FCC's Privacy Order is Significantly Costly to Businesses and Consumers

The Privacy Order responds to a perceived threat to privacy presented by BIAS with the argument that it is better to be over-inclusive with respect to what constitutes sensitive or non-sensitive data.[259] This cavalier implementation of regulation without regard for transactional costs is inappropriate. Moreover, until the FCC can demonstrate that consumers have experienced a harm that would have otherwise been avoided but for the FTC's inadequate framework, the FCC's Privacy Order is unnecessary.

Commissioner O'Rielly's dissenting statement to the Open Internet Order cautions that the reclassification of broadband will likely lead to the FCC regulating edge providers and applications.[260] O'Rielly maintains that "The Commission is intentionally setting itself on a collision course with the FTC's definition to up the burdens on edge providers and all technology companies, either here or at the FTC."[261]

Because consumer data is so helpful for industry, innovation, and competition, BIAS will find a way to obtain Internet users' data despite the FCC's ruling. Therefore, what the FCC's Privacy Order has done is create an extra step for a certain segment of industry. Instead of being able to easily access consumer's data, including their browsing activity, BIAS will need to "purchase and use the information they need from other Internet companies, including edge providers, because these companies" are covered by the FTC's

---

257. Google, *About Google Ads*, https://perma.cc/HH97-JMRP (last accessed Apr. 11, 2017); *see also* Letter from James J.R. Talbot, AT&T, to Marlene Dortch, FCC, 16-106, at 3 (Oct. 17, 2016).

258. *Privacy Order* at 215; Comment of Comcast at 43, *Privacy Order*; The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Modernization Act of 1999, is a federal law enacted to control the ways that financial institutions deal with the private information of individuals. *Gramm-Leach-Biley Act*, FTC, https://perma.cc/4XYJ-5FUK (last accessed on Apr. 11, 2017); The Health Insurance Portability and Accountability Act of 1996 (HIPAA), HHS, https://perma.cc/Z4YG-VS49 (last visited Apr. 11, 2017).

259. *Compare Privacy Order* at para. 9 *with* FTC Report at vii-viii; FTC REPORT at 15.

260. https://apps.fcc.gov/edocs_public/attachmatch/DOC-341937A6.pdf.

261. O'Rielly Dissenting Statement at 5-6.

rules, and "will continue to operate under the FTC's opt-out regime".[262] The FCC's Privacy Order limits BIAS providers "from using sensitive customer proprietary information without opt-in consent, but customer proprietary information is limited to information that the provider acquires in connection with its provision of telecommunications service."[263] Thus, data BIAS "obtain from an edge provider does not meet the definition," and is therefore permissible.[264] This is also another example of how the contradictory policies of the FCC and the FTC give ESPs an advantage over BIAS providers, as ESPs can provide substantial valuable content to interested BIAS providers that are unable to do so on their own due to FCC limitations.

Therefore, since non-sensitive consumer data is so valuable to BIAS providers, it is highly likely that BIAS providers will take the additional steps despite the Privacy Order to lawfully obtain consumer's non-sensitive information. The Privacy Order does not prohibit BIAS providers from purchasing consumer data lawfully collected from ESPs under the FTC. This is because when a user does not consent to ISP data use or sharing, the consumer's choice only applies to her data within the context of her relationship with the ISP and not the various ESPs she visits by way of the ISP. Thus, the Privacy Order has simply created needless extra transactional costs. These costs will be transferred to customers, making the service BIAS offer more expensive. The Privacy Order also creates a competitive edge for ESPs that would be in the position to sell data lawfully collected from its consumers to BIAS. Again, these increased hassles and transactional costs are unnecessary because the behavior the regulations are designed to prohibit is arguably not harmful to industry nor consumers.

E. Appropriate Changes to Existing Privacy Regulation Frameworks

The government's purpose with respect to Internet privacy is to ensure that customer's privacy is reasonably protected and that businesses clearly understand their duties to customers. In the spirit of simplifying Internet privacy laws, it is sensible for one agency to have complete jurisdiction over ISPs and ESPs. Now that the Privacy Order is reversed, Congress should pass legislation to limit the FCC's Internet privacy authority. The FCC's party-line vote in 2015 to remove ISPs from the FTC's jurisdiction was a mistake, and limiting the FCC's authority to enact Internet privacy rules and regulations will validate the FTC's role as a unilateral enforcer going forward. Congress should also pass legislation that preempts state laws on Internet data security. There are numerous conflicting state laws on Internet privacy matters, including but not limited to: children's online privacy, e-reader privacy, and privacy policies for websites and online services, privacy of PI held by ISPs,

262. *Privacy Order* at 216.

263. *Privacy Order* at 216-17; *Privacy Order*, *supra* note 15, at App. A § 64.2002(f).

264. *Privacy Order* at 216-17Even if the Commission "fixed" the definition, it would still be precluded by the statute from placing restrictions on a broadband provider's purchase or use of third-party data. *See, e.g.,* Comments of Comcast, *Privacy Order, supra note 15, at 75-76*.

and false and misleading statements in website privacy policies.[265] Federal preemption of state privacy laws will eliminate ambiguity concerning businesses' duties to consumers with respect to particular states. Differences between the HIPAA privacy rule and state physician-patient privilege laws have created substantial confusion in federal question cases.[266] This type of confusion will likely result from the duplicative and contradictory Internet privacy policies discussed in this Note.

On May 18, 2017, Republican Congresswoman Marsha Blackburn of Tennessee introduced the Balancing the Rights of Web Surfers Equally and Responsibly Act (BROWSER Act).[267] The bill would require ISPs and ESPs to "clearly and conspicuously" notify users of their privacy policies, and give users opt-in or opt-out approval rights with the respect to the "use of, disclosure of, and access to user information collected by such providers based on the level of sensitivity of such information, and for other purposes."[268] While the BROWSER Act would make the FTC the sole Internet privacy regulator, it would reinstate the FCC's higher bar for obtaining consumer consent to use certain data.[269] Moreover, the BROWSER Act would essentially have the FTC use the FCC's approach to consumer consent in the Privacy Order, and it would extend the rules beyond ISPs to also include ESPs.[270]

The BROWSER Act is unlikely to garner support in the Senate, and consequently unlikely to become law.[271] Predictably, numerous ESPs and their advocates have criticized Rep. Blackburn's bill because it would subject ESPs to a higher bar with respect to consumer privacy.[272] Additionally, the bill would eliminate the regulatory advantage ESPs had under the Privacy Order compared to their ISP competitors.[273] Since its introduction, few of Rep. Blackburn's conservative colleagues have voiced support of the bill. Significantly, the BROWSER Act is also very similar to the Privacy Order which was widely disliked by conservatives.[274] The BROWSER Act,

---

265. *State Laws Related to Internet Privacy*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 5, 2016), https://perma.cc/X53G-JADT/.

266. Jenna Phipps, *State of Confusion: The HIPAA Privacy Rule and State Physician-Patient Privilege Laws in Federal Question Cases*, 12 SUFFOLK J.TRIAL & APP. ADVOC. 159, 160 (2007).

267. H.R. 2520 115th Cong. (2017); Rep. Blackburn is Chairwoman of the House of Representatives Committee on Energy and Commerce Subcommittee on Communications and Technology.

268. H.R. 2520 115th Cong. (2017).

269. *Id.*

270. *Id.*

271. James Cooper, *The BROWSER Act: A Worthy Goal, But There's an Easier Fix to the Net Neutrality Privacy Mess*, FORBES (May 26, 2017, 5:06 PM), https://perma.cc/AFD3-R2M3.

272. Jenna Ebersole, GOP Plan Revives, Expands Part of Nixed FCC Privacy Rules, LAW 360 (June 1, 2017, 8:45 PM), https://perma.cc/V984-C8C8.

273. *Compare Privacy Order*, *with* H.R. 2520, 115th Cong. (2017).

274. H.R. 2520, 115th Cong. (2017) (Sensitive information includes not only information pertaining to children or social security numbers, but also web browsing history and app usage data, content that industry stakeholders and conservative policymakers have argued is overly broad).

ironically, would instate a very similar approach to Internet privacy as the Privacy Order except the BROWSER Act would have the FTC as the only cop on the beat and would give the FTC authority over both ESPs and ISPs.[275] Meanwhile, AT&T has praised the bill; however, AT&T is an ISP which would benefit from the regulatory crackdown on its ESP competitors that the bill would require.[276]

While there is value in leveling the playing field and applying a tech-neutral approach that does not preference ESPs nor ISPs, the opt-in and opt-out framework Blackburn supports is inappropriate. The bill and its burdensome opt-in and opt-out requirements has the potential to stifle innovation and also drastically decrease the free services available to consumers. Because the bill would require customers to opt-in to the sharing of a broad definition of sensitive information and most consumers are inclined to maintain default settings on their devices rather than opting-in due to a desire to minimize decision-making and increase the speed of their Internet use experience, the BROWSER Act would likely dramatically reduce the amount of data collected by ESPs.[277]

If ESPs collect less data from users, Internet consumers will see less relevant ads, and ESPs will earn considerably less revenue.[278] Furthermore, if ESPs cannot make enough money through advertisements, then they will need to start charging users for more services or go out of business.[279] Thus, the BROWSER Act's requirements would make the current business model of ESPs unsustainable and would push ESPs toward a pay model, ultimately harming consumers who cannot afford to pay for content and apps.[280] The BROWSER Act would be also harm industry and consumers because it would decrease competition and product quality.[281] Internet advertisements, especially of the targeted variety, create easy entry for startups and analytics performed on data collected from consumers help improve apps and personalize content.[282]

Chairwoman Blackburn's legislation also operates on the false premise that consumers would like to give up the free content and mobile apps they currently receive in exchange for enhanced privacy protections, despite

275. H.R. 2520, 115th Cong. (2017).

276. Jenna Ebersole, *GOP Plan Revives, Expands Part of Nixed FCC Privacy Rules*, LAW 360 (June 1, 2017, 8:45 PM), https://perma.cc/V984-C8C8.

277. James Cooper, *The BROWSER Act: A Worthy Goal, But There's an Easier Fi x to the Net Neutrality Privacy Mess*, FORBES (May 26, 2017, 5:06 PM), https://perma.cc/AFD3-R2M3 ("Today, almost no one reads privacy policies, and the BROWSER Act won't change that. It will dramatically reduce the amount of data collected—not because consumers will carefully consider the pros and cons of data sharing and decide to withhold consent, but rather because its not worth their time to make a decision.").

278. James Cooper, *The BROWSER Act: A Worthy Goal, But There's an Easier Fix to the Net Neutrality Privacy Mess*, FORBES (May 26, 2017, 5:06 PM).

279. *Id.*

280. *Id.*

281. *Id.*

282. *Id.*

numerous recent studies indicating otherwise.[283] For example, a recent George Mason University Antonin Scalia Law School working paper analyzed whether consumer autonomy is impacted by an increase in online surveillance by a commercial entity.[284] The study analyzed consumers' Internet browsing history and privacy choices as they relate to Google's privacy policies.[285]

Beginning in March 2012, Google combined user information across platforms, which meant that search queries would "be matched with YouTube views, Gmail or Maps activity, or Android use."[286] Google's new cross platform data collection policy prompted speculation and outcry from privacy advocates; however, direct harms caused by Google's actions are "unobservable."[287] Reduced anonymity may have deterred more privacy sensitive consumers from conducting searches on sensitive or potentially embarrassing topics on Google sites, but the overall effect was negligible and did not qualify as a direct harm for Google nor the majority of its users.[288]

A recent Pew Research Center survey also found that only about a quarter of adults believe their Internet browsing history is "very sensitive."[289] Thus, until objective evidence emerges that consumers want enhanced privacy instead of free content and mobile apps and increased competition among companies, the BROWSER Act is an inappropriate solution to a perceived but nonexistent harm.[290] While giving the FTC jurisdiction over both ISPs and ESPs is appropriate, Congress should reject the BROWSER Act or any similar proposal that attempts to replace the FTC's opt-out framework with opt-in requirements on the digital economy.

---

283. *See generally*, Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?* 45 J. LEG. STUD. S69 (2016) (when large, census-weighted samples of Americans read excerpts from Facebook's, Yahoo's, and Google's privacy policies, subjects generally stated agreement to either vague or explicit language authorizing companies to collect or use personal information seen though subjects regarded these corporate practices as intrusive); *see generally*, James C. Cooper, *Anonymity, Autonomy, and the Collection of Personal Data: Measuring the Privacy Impact of Google's 2012 Privacy Policy Change* (GEO. MASON U.L. & ECONS. RES. PAPER SERIES, Working Paper 17-06), https://perma.cc/5VT9-N4D8.

284. James C. Cooper, *Anonymity, Autonomy, and the Collection of Personal Data: Measuring the Privacy Impact of Google's 2012 Privacy Policy Change* (GEO. MASON U.L. & ECONS. RES. PAPER SERIES, Working Paper 17-06), https://perma.cc/5VT9-N4D8.

285. *Id.*

286. *Id.* at 3.

287. *Id.*

288. *Id.*

289. *The State of Privacy in Post-Snowden America*, PEW RESEARCH CENTER (Sept. 21, 2016), https://perma.cc/R5HR-Q6KC.

290. *See generally*, Lior Jacob Strahilevitz & Mathew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?* 45 J. LEG. STUD. (forthecoming 2017) (when large, census-weighted samples of Americans read excerpts from Facebook's, Yahoo's, and Google's privacy policies, subjects generally stated agreement to either vague or explicit language authorizing companies to collect or use personal information seen though subjects regarded these corporate practices as intrusive);, James C. Cooper, *Anonymity, Autonomy, and the Collection of Personal Data: Measuring the Privacy Impact of Google's 2012 Privacy Policy Change* (GEO. MASON U.L. & ECONS. RES. PAPER SERIES, Working Paper 17-06), https://perma.cc/5VT9-N4D8; *The State of Privacy in Post-Snowden America*, PEW RESEARCH CENTER (Sept. 21, 2016), https://perma.cc/R5HR-Q6KC.

Although both the current Chairman of the FCC and the Acting Chairman of the FTC support the Privacy Order's reversal and the FTC being the sole Internet privacy enforcer, these positions are not held exclusively by conservatives.[291] During the Obama Administration, the FTC concluded that "any privacy framework should be technology neutral" because "ISPs are just one type of large platform provider" and "operating systems and browsers may be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles."[292] The Privacy Order, therefore, represented the FCC's divergence from the views of its Democratic colleagues at the FTC. The Obama FTC publicly expressed its criticism of the Privacy NPRM in a unanimous bipartisan comment, calling the FCC's framework "not optimal."[293] Additionally, Peter Swire, President Clinton's Chief Counselor for Privacy and President Obama's Special Assistant for Economic Policy has been one of the loudest critics of the FCC's Privacy Order.[294]

The argument that ISPs should be treated differently because consumers face a unique lack of choice and competition in the ISP marketplace is also flawed. For instance, according to a 2017 industry analysis, "Google dominates the world of search" with a global market share of 80.5% on desktop computers and 95.9% on mobile devices.[295] Meanwhile, Verizon, the largest BIAS, holds only an estimated 35% of its market.[296]

Federal Internet privacy laws are moving in the right direction, but more needs to be done to protect consumer's privacy, and to inform businesses on what they must do to protect themselves from privacy-related enforcement actions. While the FCC waits for Congressional legislation returning ISPs to the FTC's privacy jurisdiction, the FCC should align its rules with the FTC's approach. However, the FCC should act in accordance with the limitations imposed by the Congressional Review Act and other legal and regulatory provisions which may minimize the amount of privacy-related rules the FCC

---

291. Ajit Pai, Chairman, FCC & Maureen Ohlhausen, Acting Chairman, FTC, Opinion, *No, Republicans Didn't Just Strip Away Your Internet Privacy Rights*, WASH. POST (Apr. 4, 2017), https://perma.cc/TLM4-KZMK.

292. FTC Report at 56.

293. The Federal Trade Commission, Comment, Comment of FTC Staff of the Bureau of Consumer Protection of the Federal Trade Commission at 7-8, *Privacy NPRM,* https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf.

294. *See generally*, Swire Working Paper (discussing the functionality of ISPs therein challenging the fundamental premise of the FCC's privacy NPRM framework); *see also* Ajit Pai, Chairman, FCC & Maureen Ohlhausen, Acting Chairman, FTC, *No, Republicans Didn't Just Strip Away Your Internet Privacy Rights*, WASH. POST.: OPINION (Apr. 4, 2017), https://perma.cc/TLM4-KZMK.

295. Martin Armstrong, *Google, Googler, Googlest*, STATISTA (Mar. 31, 2017), https://perma.cc/4E5G-K7XW.

296. Market Share of Wireless Subscriptions Held by Carriers in the U.S. from 1st Quarter 2011 to 4th Quarter 2016, STATISTA,https://www.statista.com/statistics/199359/market-share-of-wireless-carriers-in-the-us-by-subscriptions/ (ast accessed Apr. 11, 2017).

can impose.[297] Then, once the necessary laws are enacted to preempt state regulations and limit the FCC's role in Internet data security, Congress should create a more clear and appropriate Internet security standard which the FTC will be responsible for enforcing. The updated FTC standards should be a pro-consumer, pro-industry approach considering the potential harms and benefits of data collection to consumers and businesses.

IV. CONCLUSION

Given the FTC's long history in consumer protection, it possesses significant privacy and data security expertise and it would behoove the FCC to consider the FTC's perspective. The Privacy Order places substantial, unjustified costs on businesses and consumers. Additionally, the Privacy Order facilitates superfluous corporate favoritism and does not protect consumers from any proven Internet privacy related harm. Therefore, Congress should take steps to strip the FCC of its authority to regulate online data security, and create a stronger uniform data security policy, which the FTC will be in charge of enforcing.

297. Jenna Ebersole, *FCC Faces Quandary If Obama-Era Privacy Rules Get Boot*, LAW360 (Mar. 24, 2017).