Minnesota Journal of Law, Science & Technology

Volume 18 | Issue 2 Article 6

June 2017

Only the Good Regulations Die Young: Recognizing the Consumer Benefits of the FCC's Now-Defunct Privacy Regulations

Paul R. Gaus
University of Minnesota Law School

Only the Good Regulations Die Young: Recognizing the Consumer Benefits of the FCC's Now-Defunct Privacy Regulations

*Paul R. Gaus**

[Editor's Note: This Note was well into the publication process when the United States Congress passed Senate Joint Resolution 34, signed into law on April 3, 2017.[1] The resolution repealed the Federal Communication Commission's rule relating to "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," on which the author's argument principally focused. Nevertheless, the Note's analysis regarding the FCC's role in data privacy regulation still stands as it applies to any similar framework proposed in the future.]

A recent study by the Pew Research Center[2] demonstrates American consumers' concern about the use and storage of their personally identifiable information online. Surveys estimate that 86% of Americans take some steps to minimize their digital footprints.[3] Whereas Americans once trusted online providers to protect data,[4] consumers currently express little confidence in

---

* BA Marquette University, 2012; JD Candidate 2017, University of Minnesota Law School. Thank you to Mr. Charles Ragan for his feedback and critique of this Note and for being a friend. Thank you to many San Franciscans for their guidance and friendship throughout my life including, Kathy Grogan, Steve Piuma, Joe Strizich, Daniel Hackett, Officer Christopher Viehweg, and Dr. Edward Powers, M.D. Finally, thank you to my mom, Therese Gaus, and my late father, William A. Gaus, for the sacrifices they made in their life to give me the opportunities I have today.

1. S.J. Res. 34, 115th Cong. (2017) (enacted); 163 Cong. Rec. H2749-01 (daily ed. Apr. 5, 2017).

2. The Pew Research Center describes itself as a "non-partisan fact tank" that focuses primarily on United States policy. *See About Pew Research Center*, PEW RES. CTR., http://www.pewresearch.org/about/ (last visited Jan. 3, 2017).

3. Lee Raine, *The State of Privacy in Post-Snowden America*, PEW RES. CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

4. *See, e.g.*, Joseph Turow et al., Open to Exploitation: America's Shoppers Online and Offline 3 (June 1, 2005) (unnumbered working paper), http://repository.upenn.edu/cgi/viewcontent.cgi?article=1035&context=asc_pap

organizations, both public and private, to properly handle their personally identifiable information.[5] Consequently, 91% of digital consumers worry that they have lost control over their personal data, and seek greater autonomy over information collected, stored, and disseminated about them.[6] As noted frequently in scholarly literature, no overarching federal regulation or law controls these practices.[7] The Federal Trade Commission (FTC) champions itself as the guardian of consumer data privacy,[8] but critics contend the FTC is understaffed at best and feckless at worst.[9] In theory, consumers could litigate their own privacy interests, but Courts are often unreceptive to individual data privacy claims absent a worst case scenario data breach.[10] Recently, the Federal Communications Commission (FCC) significantly altered the internet regulatory landscape with its Open Internet Order.[11] Although data privacy did not

---

ers (noting that 75% of Americans believed that websites which had privacy policies would not "share [the user's] information with other websites and companies").

5. Raine, *supra* note 3 (explaining that Americans exhibited a "deep lack of faith in organizations of all kinds, public or private, in protecting the personal information they collect").

6. *See id.*

7. *See* Daniel J. Solove & Woodrow Herzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014) (describing privacy law as a "hodgepodge of various constitutional protections, federal and state statutes, torts, regulatory rules, and treaties"). *See generally* William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959 (2016) (describing the American approach to privacy regulation as targeting specific industries, technologies, or types of information).

8. *See Protecting Consumer Privacy*, FED. TRADE COMMISSION, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy (last visited Jan. 15, 2017) ("The FTC has been the chief federal agency on privacy policy and enforcement since the 1970s . . . .").

9. Peter Maass, *Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless*, WIRED (June 28, 2012, 6:30 AM), https://www.wired.com/2012/06/ftc-fail/ (contending a lack of resources and explicit legal authority hamper the FTC's ability to execute its mission); *see* Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 359 (2015) (arguing the FTC's enforcement powers are inadequate to accomplish elements of Fair Information Practice Principles).

10. *See generally* John Biglow, Note, *It Stands to Reason: An Argument for Article III Standing Based on the Threat of Future Harm in Data Breach Litigation*, 17 MINN. J.L. SCI. & TECH. 943 (2016) (discussing how the Supreme Court's "case or controversy" requirement is a frequent roadblock for litigants in privacy cases).

11. *See generally* Protecting and Promoting the Open Internet, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order

drive the Order, the FCC ventured further, recently adopting rules related to data privacy for internet service providers (ISPs).[12]

This Note argues that the FCC's recent rulemaking provides a promising framework to spur much-needed change regarding data privacy practices. The rules are not a panacea. They target only a subset of the vast internet ecosystem, but they favor consumers. They are especially desirable when considering the FTC's limitations in this area and the judiciary's reluctance to hear consumer data cases even in the face of clear statutory violations. Section I.A of this Note provides a brief explanation of the key entities in the internet ecosystem. Section I.B defines consumer privacy. It explores theoretical concepts and policy proposals urging for greater transparency and choice for consumers relating to their personally identifiable information. Section I.C discusses the FTC's authority to police privacy interests. Section I.D then outlines the FCC's traditional jurisdiction, the recent Open Internet Order, and the subsequent FCC rulemaking. It then describes consumers' fluctuating access to Courts to litigate their own privacy interests, including the Supreme Court's recent opinion in *Spokeo v. Robins.*[13] Part II of this Note argues the FCC's recent rulemaking is the most effective federal mechanism thus far for protecting consumer privacy interests. It begins by outlining the limitations on the FTC's ability to enforce consumer privacy interests. Part II then argues that the judiciary's commitment to Article III standing impedes consumers' ability to litigate their own privacy interests. Considering these significant obstacles, this Note analyzes how the FCC's regime provides advantages to consumers in ways the FTC and the Courts cannot, or will not, do.

Protecting and Promoting the Open Internet, 30 FCC Rcd. 5601 (Mar. 12, 2015) [hereinafter Open Internet Order].

12. Protecting the Privacy of Customers of Broadband & Other Telecommunications Services, WC Docket No. 16-106, Notice of Proposed Rulemaking, 31 FCC Rcd. 2500 (Apr. 1, 2016) [hereinafter Proposed Rulemaking].

13. Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).

I. BACKGROUND

A. BRIEF PRIMER ON THE INTERNET ECOSYSTEM AND DATA MANAGEMENT

The internet ecosystem describes "organizations and communities that have organically evolved to guide the operation and development of the technologies and infrastructure that comprise the global Internet."[14] The organizations are numerous and most are beyond the scope of this Note.[15] The Telecommunications Act of 1996 defines the internet as "the combination of computer facilities and electromagnetic transmission media, and related equipment and software, comprising the interconnected worldwide network of computer networks."[16] This Note focuses on three players in the internet ecosystem: (1) internet service providers (ISPs); (2) edge providers, and (3) consumers.[17]

ISPs provide access to the internet through physical cables or digital subscriber lines (DSL).[18] In most instances, ISPs also provide the customer with telephone and cable services – Comcast's "triple play" package is an example.[19] The industry is concentrated – the five largest ISPs accounted for nearly 75% of market share in the United States in 2016.[20] ISPs possess two types of consumer data: (1) web traffic detailing an individual's

---

14. INTERNET SOC'Y, INTERNET ECOSYSTEM: NAMING AND ADDRESSING, SHARED GLOBAL SERVICES AND OPERATIONS, AND OPEN STANDARDS DEVELOPMENT 5 (2014), https://www.internetsociety.org/sites/default/files/bp_Internet%20Ecosystem_032614_en.pdf.

15. *See generally id.* The Open Internet Society defines broadly the five categories of the actors in the internet ecosystem. *Id.* Within each category, there are numerous sub-groups. *Id.*

16. 47 U.S.C. § 231(e)(3) (2012).

17. *See* Simone A. Friedlander, *Net Neutrality and the FCC's 2015 Open Internet Order*, 3 BERKELEY TECH. L.J. 905, 908 (2016).

18. *Internet Terms: ISP Definition*, TECHTERMS (May 29, 2016), http://techterms.com/definition/isp.

19. A "triple play" package gives the customer cable television services, telephone, and internet for one account. *See, e.g.*, *Xfinity Triple Play*, COMCAST, http://www.xfinity.com/Corporate/Learn/Bundles/bundles.html (last visited Jan. 15, 2017); *see also* KC Claffy & David Clark, *Platform Models for Sustainable Internet Regulation*, 4 J. INFO. POL'Y 463 (2014).

20. *See* MADELINE LECLAIR, IBISWORLD INDUSTRY REPORT 51711D: INTERNET SERVICE PROVIDERS IN THE US 28 (Oct. 2016), http://clients1.ibisworld.com.ezp1.lib.umn.edu/reports/us/industry/competitivelandscape.aspx?entid=1901#MSC.

internet consumption, and (2) personally identifiable information regarding physical location corresponding to the account for internet services.[21] Technologies such as encryption and the proliferation of mobile devices fracture ISPs' access to this data.[22] However, the ability to create a "device map" for any particular consumer remains.[23]

By contrast, edge providers, like Netflix, Google, and Facebook, furnish content on the internet.[24] Edge providers depend on ISPs for functionality.[25] The type and scope of data edge providers access largely hinges on the service provided. For example, Google knows search queries tied to a certain device.[26] Similarly, most websites require consumers to provide certain types of information in order to accomplish the website's purpose.[27] In such cases, users willingly provide information

---

21. Because ISPs provide the gatekeeping function from the internet to the consumer, they "carry users' data traffic on their network. In most cases, ISPs have relatively accurate information about a subscriber's name and billing address, and may have their credit card information and phone number." Peter Swire et al., Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Less than Access by Others 23 (2016) (Inst. for Info. Sec. & Privacy at Ga. Tech. Working Paper), http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf. *But see id.* at 6–7 (discussing the "mistaken view" that ISPs possess more personally identifiable information online).

22. *Id*. at 24–25.

23. *Id*. at 116–18.

24. *See* Friedlander, *supra* note 17, at 908; *see also* Hon. Maureen K. Ohlhausen, *The FCC's Knowledge Problem: How to Protect Consumers Online*, 67 FED. COMM. L.J. 203, 232 (2015) (listing Google, Facebook, Amazon, Youtube, LinkedIn, and Pandora as typical edge providers).

25. One of the issues surrounding the net neutrality debate centers on ISPs' ability to prevent consumers from reaching edge providers through practices like "throttling." *See* Ohlhausen, *supra* note 24, at 224; *see also Definition of: Edge Network*, PC MAG., http://www.pcmag.com/encyclopedia/term/42363/edge-network (last visited Feb. 28, 2017).

26. *See, e.g.*, Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 439, 445 (2014).

27. *See, e.g.*, HAROLD FELD ET AL., PROTECTING PRIVACY PROMOTING COMPETITION: A FRAMEWORK FOR UPDATING THE FEDERAL COMMUNICATIONS COMMISSION PRIVACY RULES FOR THE DIGITAL WORLD 45 (2016), https://www.publicknowledge.org/assets/uploads/blog/article-cpni-whitepaper.pdf ("Edge providers generally have only one or the other of [users' internet access habits or physical location], and importantly consumers always have the ability to opt out . . . ."); *see also* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1441 (2009) ("Google cannot know what users buy on Amazon or eBay, what they read on the *New York Times*, or who they friend on Facebook.").

such as birth date, hometown, and in some cases, financial information.[28]

Defining the internet consumer seems like a facile task, but it must incorporate how the person uses digital devices to connect to the internet and use content.[29] In the context of ISPs, the digital consumer conforms to a traditional definition in that the consumer purchases ISP services to access the internet.[30] In the space of edge providers, the digital consumer engages in traditional retail, watches content, interacts with others via social media, and performs a plethora of other activities that provide a telling summary about a person's life.[31]

B. DEFINING CONSUMER EXPECTATIONS ABOUT THEIR PERSONALLY IDENTIFIABLE INFORMATION AND THE POSSIBLE HARM

A large-scale discussion of theoretical privacy concepts is unnecessary for this Note beyond the contention that privacy is a fluid concept that consumers value.[32] Surveys, news articles, and other studies demonstrate how digital proliferation shifted consumers' privacy expectations.[33] For example, a telephone

---

28. *See* FELD ET AL., *supra* note 27, at 55–56.

29. *See The U.S. Digital Consumer Report*, NIELSEN (Feb. 10, 2014), http://www.nielsen.com/us/en/insights/reports/2014/the-us-digital-consumer-report.html.

30. *Definition of Consumer*, MERRIAM-WEBSTER (last visited Feb. 28, 2017), https://www.merriam-webster.com/dictionary/consumer (defining a consumer as "one that consumes such as one that utilizes economic goods").

31. *See* NIELSEN, *supra* note 29.

32. For the most cited theory of privacy, see Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890), where Justice Brandeis posits

> [t]hat the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.

Id. at 193.

33. *See, e.g.*, *What's a Consumer to Do? Consumer Perceptions and Expectations of Privacy Online: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy and Commerce*, 112th Cong. (2011) (testimony of Pam Dixon, Executive Director, World Privacy Forum), http://www.worldprivacyforum.org/wp-content/uploads/2011/10/PamDixon ConsumerExpectationTestimonyfsshort.pdf (listing, in 2011, several consumer misconceptions about privacy). In the testimony, Dixon details complaints she received from consumers. *Id.* For example, she mentions consumer concerns

survey conducted in 2005 revealed that 75% of Americans believed that online privacy policies signaled a commitment from entities to safeguard information.[34] Subsequent news and information revealed the extent to which companies derived value from doing the exact opposite. The emergence of big data—whereby companies compiled and sold consumers' fractured online browsing habits—fostered digital advertising.[35] Exploration of this industry disclosed certain unsavory practices and subsequent consumer backlash.[36] For example, these processes allowed companies to make predictions about personal preferences, based on a few data points, like child birth, geographic location, and sensitive health information of consumers.[37]

Technology's ability to create consumer tapestries prompted new theories about acceptable use, storage, and dissemination of consumer data. Solove identifies several ways unregulated use and dissemination of data harms consumers.[38] For example, information processing facilitates efficiency, but also creates

---

about Google Street View presenting pictures of people's backyards and frustration about not being able to exercise certain opt-out functions on websites. *Id.*; *see also* Bob Sullivan, *Privacy Under Attack, but Does Anybody Care?*, NBC NEWS (Oct. 17, 2006, 4:14 PM), http://www.nbcnews.com/id/15221095/ns/technology_and_science–privacy_lost/t/privacy–under–attack–does–anybody–care/# (describing, in 2006, Americans' "indifference" towards online privacy matters).

34. *See, e.g.*, Turow et al., *supra* note 4.

35. *See, e.g.*, Dennis D. Hirsch, *That's Unfair! Or Is It? Discrimination and the FTC's Unfairness Authority*, 103 KY. L.J. 345, 345–46 (2014) ("Still it is clear that a growing number of businesses are using big data to . . . determine 'people's life opportunities – to borrow money, work, travel, obtain housing, get into college, and far more.'") (quoting Danielle Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 18 (2014)); *see also* DANIEL SOLOVE, UNDERSTANDING PRIVACY 118–19 (2008) (discussing how, through the process of data aggregation, technology produces "digital dossiers" on people).

36. *See, e.g.*, Charles Duhigg, *How Companies Learn Your Secret*s, N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html; Kashmir Hill, *Data Broker Was Selling Lists of Rape Victims, Alcoholic, and "Erectile Dysfunction Sufferers*, FORBES (Dec. 19, 2013, 3:40 PM), http://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/.

37. *See* Duhigg, *supra* note 36; Hill, *supra* note 36 (discussing how one data broker, MEDbase 2000, compiled lists pertaining to consumers' medical history, including "erectile dysfunction sufferers, alcoholism sufferers, and AIDS/HIV sufferers").

38. SOLOVE, *supra* note 35, at 101–70.

anxiety about "risks of downstream harm that can emerge from inadequate protection of compendiums of personal data."[39] Furthermore, unfettered secondary use of the data outside the context of the original purpose for collection erodes trust between the consumer and the online world.[40]

While lagging well behind many foreign states, the public sector in the United States inched in recent years towards defining consumer expectations about the collection, use and dissemination of personally identifiable information. In 2012, the Obama Administration provided a new framework in its Consumer Privacy Bill of Rights.[41] Among other items, the Consumer Privacy Bill of Rights focused on individual control, transparency, security, focused collection, and accountability.[42] Individual control encouraged companies to provide consumers appropriate control of their data at the time of collection.[43] Transparency sought to bridge the knowledge gap between the consumer and company through "meaningful understanding of privacy risks and the ability to exercise Individual Control . . . ."[44] Focused collection challenged companies to "engage in considered decisions about the kinds of data they need to collect to accomplish specific purposes."[45] Finally, security and accountability placed the onus on companies to handle data in a responsible manner and conduct ongoing reviews of data management.[46]

C. THE FTC'S CURRENT ROLE AS A PRIVACY WATCHDOG

An agency born out of the Woodrow Wilson administration has seized responsibility for regulating the vast internet ecosystem.[47] The Federal Trade Commission Act (FTC Act)[48]

---

39. *Id.* at 127.

40. *See id.* at 131.

41. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), *reprinted in* 4 J. PRIVACY & CONFIDENTIALITY 95 (2012).

42. *See id.* at 103–04.

43. *See id.* at 105.

44. *Id.* at 108.

45. *Id.* at 115.

46. *See id.* at 113, 116.

47. *Our History*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc/our-history (last visited Jan. 15, 2017).

48. 15 U.S.C. §§ 41–58 (2012).

tasked the FTC (the Agency) with protecting consumers and promoting competition.[49] FTC enforcement authority lies in Section 5 of the FTC Act (Section 5) which directs the Agency to regulate "unfair or deceptive acts or practices."[50] An unfair or deceptive trade practice is one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[51] The meaning of "unfair" remained shrouded in ambiguity until the FTC put forth a test known as the "Cigarette Rule" that declared a practice unfair if it "offends public policy as it has been established by statutes, the common law, or otherwise . . . 2) whether it is immoral, unethical, oppressive, or unscrupulous; 3) whether is causes substantial injury to consumers."[52] The Rule experienced a period of dormancy, but Congress later codified a more precise version of the Cigarette Rule requiring the injury to be (1) substantial, (2) not outweighed by countervailing benefits to consumers, and (3) not reasonably avoided.[53]

1. The FTC's Notice-and-Choice Model

Now, the FTC enjoys the status as "the de facto federal data protection authority."[54] Its first foray into the world of online privacy occurred when the Agency presented a 1998 report to Congress on "fair information practice codes."[55] The fair

---

49. *About the FTC*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc (last visited Jan. 15, 2017).

50. 15 U.S.C. § 45(a) (2012).

51. 15 U.S.C. § 45(n); *see also* DANIEL SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 2013, at 135 (Int'l Ass'n of Privacy Prof'ls, 2013).

52. Statement of Basis and Purpose, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8355 (1964). The Supreme Court tacitly accepted this test as a basis for determining unfair practices in *FTC v. Sperry & Hutchinson*, 405 U.S. 233, 244 n.5 (1972). *See also* Amy Grewal Dunn, *Bridging the Gap: How the Injury Requirement in FTC Enforcement Actions and Article III Standing Are Merging in the Data Breach Realm*, 20 J. CONSUMER & COM. L. 9, 10–11 (2016).

53. 15 U.S.C. § 45(n).

54. Solove & Herzog, *supra* note 7, at 600; *Protecting Consumer Privacy*, FED. TRADE COMMISSION, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy (last visited Jan. 15, 2017) ("The FTC has been the chief federal agency on privacy policy and enforcement since the 1970s.").

55. FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

information practice codes encompassed five core principles concerning data privacy: (1) notice/awareness; (2) choice/consent; (3) access/participation; (4) integrity/security; and (5) enforcement/redress.[56] Within the enforcement/redress prong, the FTC promoted a mix of internal and external mechanisms to regulate online privacy practices.[57] First, the Agency proposed self-regulation rooted in accepted standards that establish remedies to correct errors and provide monetary compensation to consumers where necessary.[58] Second, the Agency advocated "[a] statutory scheme [to] create private rights of action for consumers harmed by an entity's unfair information practices."[59] Third, the FTC proposed a rigorous legislative scheme bolstered by Agency investigation and enforcement powers.[60]

Currently, the FTC practices a "notice and choice" model for online consumer data practices.[61] Scholars believe that the notice-and-choice model reflects the FTC's preference for industry self-regulation enhanced with flexible consumer options regarding data practices.[62] Under this framework, companies inform consumers about the use and storage of their data—a privacy policy is one example—and provide consumers with certain opt-out options.[63] Commentators touted this as

---

56. *Id*.
57. *Id*. at 10–11.
58. *Id*.
59. *Id*. at 11.
60. *Id* at 11, 62 n.160.
61. Solove & Herzog, *supra* note 7, at 592.
62. *See id*. at 598. Attempts at industry self-regulation have come in various degrees and forms. For example, the Payment Card Industry Data Security Standards provides organizations that conduct business with member card companies must set up a data security infrastructure with a vulnerability management system that is subject to regular testing. *See* PCI SEC. STANDARDS COUNCIL, DSS QUICK REFERENCE GUIDE 14 (2010), https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf. Additionally, the Digital Advertising Alliance comprises various digital advertising organizations that established guidelines for consumer privacy protections. *About the Digital Advertising Alliance*, DIGITAL ADVERT. ALLIANCE, http://digitaladvertisingalliance.org/about (last visited Feb. 19, 2017).
63. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICY MAKERS i (2012); *see also* Andrew Hasty, *Treating Consumer Data Like Oil: How Re-Framing Digital Interactions Might Bolster the Federal Trade Commission's New Privacy Framework*, 67 FED. COMM. L.J. 293, 296 (2015).

creating a happy medium between onerous regulations that may be unable to keep up with technological change and a completely unregulated frontier.[64]

2. The FTC Moves to a Harm-Based Model

In a 2010 report, the FTC acknowledged the notice-and-choice model's shortcomings.[65] The FTC also proposed the "harm-based model" which emphasized specific enforcement of consumer privacy laws.[66] The harm-based approach sanctions poor data practices under the umbrella of the FTC's traditional definition of unfair or deceptive practices.[67] Five FTC statutes permit the FTC to take enforcement action for privacy violations.[68] Enforcement actions are procedure heavy: an enforcement action begins with an investigation, the Agency weighs whether further action is necessary, and submits a proposed complaint.[69] Following the complaint, the focus of the FTC's investigation may choose to litigate the complaint "in

64. Siona Listokin, *Industry Self-Regulation of Consumer Data Privacy and Security*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 15, 17 (2015) (examining the effects of membership in voluntary consumer data privacy standards).

65. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS iii (2010) ("[T]he notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand."); *see also* Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norm, and Consent*, 14 J. HIGH TECH. L. 370, 390–91 (2014) (arguing that privacy policies, an essential component of notice-and-choice, cannot provide enough information to provide adequate notice).

66. *See* FED. TRADE COMM'N, *supra* note 65, at 9–10.

67. Vaibhav Garg & L. Jean Camp, Ex Ante v. Ex Post: Economically Efficient Sanctioning Regimes for Online Risks 4 (Mar. 31, 2013) (41st Res. Conf. on Comm. Info. & Internet Pol'y Working Paper), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2242474 (discussing harm-based approach in the context of environmental torts that take place after an environmental calamity).

68. *E.g.*, Federal Trade Commission Act (FTCA), 15 U.S.C. §45(n) (2012); Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x (2012); Telemarketing and Consumer Fraud Abuse Prevention Act (TCFAPA), 15 U.S.C. §§ 6101–6108 (2012); Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506 (2012); Gramm–Leach–Bliley Act (GLBA), 15 U.S.C. §§ 6801–6809 (2012).

69. *See* Solove & Herzog, *supra* note 7, at 609; *see also* David C. Grossman, *Blaming the Victim: How FTC Data Security Enforcement Actions Make Companies and Consumers More Vulnerable to Hackers*, 23 GEO. MASON L. REV. 1283, 1302 (stating the FTC will conduct an investigation about data practices and it will conduct a multi-layered investigation) ("This [investigation] is not limited to the initial data collection, but any use of data after it is collected that is inconsistent with the context within which the company originally collected it.")

front of an administrative or federal district court judge."[70] Triggers for FTC complaints generally range from allegations of insufficient security measures, to negligent training and security procedures, to failing to honor security and privacy policies, to insufficient disclosure of data collection, and to deceptive data collection practices.[71]

Critics of FTC enforcement actions contend that they are arbitrary and fail to provide entities clear guidelines on the Agency's positions.[72] These objections peaked when the FTC's authority to regulate data privacy was challenged in *FTC v. Wyndham Worldwide Corp*.[73] The FTC lodged a complaint against Wyndham Hotels alleging that the company's security measures unreasonably exposed consumers' personal data.[74] Wyndham countered that the FTC did not have authority to regulate cybersecurity as an unfair practice because the FTC has never taken a clear position on the issue.[75] The Third Circuit upheld the FTC's jurisdiction for several reasons. First, the Third Circuit determined the "unfairness" prong of Section 5 permitted the FTC to regulate cyber-security practices.[76] Second, even though Congress later passed specific statutes permitting the Agency to regulate certain types of data practices, it did not negate the FTC's general regulatory authority over cybersecurity practices.[77]

Despite the favorable results of *Wyndham*, the scope of the FTC's jurisdiction remains in purgatory. In 2013, the FTC filed a complaint against LabMD, a Georgia medical corporation.[78]

---

70. Solove & Herzog, *supra* note 7, at 609.

71. *See, e.g.*, Microsoft Corp., 134 F.T.C. 709, 742–43 (2002) (issuing an order that Microsoft establish security and confidentiality measures for personally identifiable information); Eli Lilly & Co., 133 F.T.C. 763, 766–67 (2002) (alleging an employee negligently disclosed email addresses of subscribers to a healthcare information service).

72. *See, e.g.*, Solove & Herzog, *supra* note 7, at 607 ("Critics of the FTC have complained that the FTC acts in an unpredictable fashion and that companies lack guidance about what they ought to do.").

73. 799 F.3d 236 (3d Cir. 2015).

74. *Id.* at 240.

75. Wyndham alleged that the FTC never indicated a clear agency position about data practices being unfair under Section 5. *Id.* at 253.

76. *Id*. at 248.

77. *Id.*

78. Complaint, LabMD, Inc., No. 9357, F.T.C. File No. 1023099 (F.T.C. Aug. 29, 2013), http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf.

The complaint stemmed from inadvertent exposure of client files on a peer-to-peer network that was "likely to cause injury to consumers."[79] An administrative judge dismissed the complaint, but the FTC followed through with an order requiring LabMD to "notify affected individuals, establish a comprehensive information security program, and obtain assessments regarding its implementation of the program."[80] LabMD appealed directly to the Eleventh Circuit, which granted a stay on the FTC's order.[81] The Circuit cast doubt on whether a reasonable interpretation of the Agency's enforcement powers encompasses speculative injuries.[82] Compounding this, the Eleventh Circuit held that the FTC did not show a high probability that consumers would be harmed.[83]

D. THE FEDERAL COMMUNICATIONS COMMISSION: REGULATORY POLICY, SCOPE, AND NEW DEVELOPMENTS

Congress established the Federal Communications Commission "[f]or the purpose of regulating interstate and foreign commerce in communication by wire and radio so as to make available . . . a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges."[84] Title II of the 1934 Communications Act applies to "common carriers" of communications services, providing "[i]t shall be the duty of every common carrier engaged in interstate or foreign communication by wire or radio to furnish such communication service upon reasonable request."[85] Section 201(b) of the Federal Communications Act states, "[a]ll charges, practices, classifications, and regulations for and in connection with [foreign and interstate communication service by wire or radio], shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is

79. *Id*. at *5.

80. Order, LabMD, Inc., No. 9357, at *37 (F.T.C. 2013), https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf.

81. LabMD, Inc. v. FTC, No. 16-16270-D, 2016 WL 8116800, at *1 (11th Cir. Nov. 10, 2016).

82. *Id*. at *3.

83. *Id*. at *5.

84. 47 U.S.C. § 151 (2012).

85. 47 U.S.C. § 201(a) (2012).

declared to be unlawful."[86] Furthermore, Section 222 of the Communications Act of 1996 places a duty of care on telecommunications providers to "protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers."[87]

Whereas consumer protection drives FTC policy, it is a secondary consideration in telecommunications regulation.[88] More often, telecommunications regulatory policy stems from the premise that telecommunications are a public good that should be regulated as a utility.[89] Therefore, policy goals center on "eliminat[ing] 'wasteful' competition, set[ting] reasonable prices, and guarantee[ing] universal service."[90] However, the FCC does oversee some consumer protection statutes like the Telephone Consumer Protection Act (TCPA).[91] Congress passed the TCPA "to protect the privacy interests of residential telephone subscribers by placing restrictions on unsolicited, automated telephone calls."[92] In response to consumer sentiments about this deeply unpopular practice, the FCC, in conjunction with the FTC, created the national do-not-call list.[93]

1. The FCC Brings ISPs within Its Regulatory Scope

The FCC created a titanic shift in the landscape for data regulation in 2015 when the Commission published the Open

86. 47 U.S.C. § 201(b).

87. 47 U.S.C. § 222(a).

88. *See, e.g.*, James B. Speta, *Reconciling Breadth and Depth in Digital Age Communications Policy*, *in* COMMUNICATIONS LAW AND POLICY IN THE DIGITAL AGE: THE NEXT FIVE YEARS 67 (Randolph J. May ed., 2012) (discussing antitrust as the foremost consideration for communications policy); *accord* MARC EISNER ET AL., CONTEMPORARY REGULATORY POLICY 120 (2d ed. 2006) (discussing the Congressional goal of creating a communications infrastructure with universal service).

89. EISNER ET AL., *supra* note 88, at 123 ("Telephone service has always been considered an essential public good; that is, providers, customers, politicians, and regulators all believe in universal service as a primary policy goal.").

90. *Id.*

91. 47 U.S.C. § 227 (2012).

92. S. REP. NO. 102–178, at 1 (1991).

93. *See, e.g.*, Spencer Weber Waller et al., *The Telephone Consumer Protection Act of 1991: Adapting Consumer Protection to Changing Technology*, 26 LOY. CONSUMER L. REV. 343, 355 (2014) (noting the volume of complaints Congress received about telemarketing calls).

Internet Order.[94] In the lengthy Order, the Commission removed broadband internet access service (BIAS) from the definition of information services and reclassified it as a telecommunications service subject to the Commission's regulatory authority under Title II.[95] The Commission defined BIAS as "a mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints."[96] The reclassification brought anyone "engaged" in providing broadband internet access within the scope of the Communications Act.[97] In layman's terms, this meant ISPs, previously beyond the reach of the FCC, were now subject to FCC jurisdiction.[98]

2. The FCC Proposes Privacy Rules Specifically for ISPs

Concerns about data privacy did not prompt the FCC's monumental Open Internet Order.[99] However, in the short period following the Order, the FCC (here, the Commission)

---

94. *See generally* Open Internet Order, *supra* note 11.

95. *See id.* ¶ 47. The Open Internet Order was a culmination of court decisions giving the FCC the authority to regulate broadband internet access service providers as telecommunications services. *Id.* ¶ 308. In *National Cable and Telecommunications Ass'n v. Brand X Internet Services*, the Supreme Court held the FCC's definition of telecommunications service lawful under the *Chevron* framework. 545 U.S. 967, 1002 (2005) (citing *Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.* numerous times in the opinion; *see* 467 U.S. 837 (1984)); *see also* Friedlander, *supra* note 17, at 918. Following the *Brand X* decision, the D.C. Circuit identified an avenue for the FCC to regulate broadband providers in *Verizon v. FCC*. *See generally* 740 F.3d 623 (D.C. Cir. 2014). In the opinion, the D.C. Circuit cited § 706(a) of the Telecommunications Act which permitted the FCC regulation on broadband internet access service providers if such entities were properly reclassified as telecommunications providers. *Verizon*, 704 F.3d at 649–50.

96. *See* Open Internet Order, *supra* note 11, § 8.2, at 5884.

97. *Id.* ¶ 339.

98. *See* Kimberlee Morrison, *Net Neutrality: FCC Reclassifies ISPs as Common Carriers*, ADWEEK (Feb. 26, 2015), http://www.adweek.com/digital/net-neutrality-fcc-reclassifies-isps-as-common-carriers/; Marguerite Reardon, *FCC and Net Neutrality: What You Really Need to Know*, CNET (Feb. 7, 2015, 5:00 AM), https://www.cnet.com/news/fcc-and-net-neutrality-what-you-really-need-to-know/.

99. The concept of "net neutrality" was the primary driver behind the FCC's Open Internet Order. *See Open Internet*, FED. COMM. COMMISSION, https://www.fcc.gov/general/open-internet (last visited Feb. 16, 2017). Net neutrality rules prohibited BIAS providers from blocking access to certain types of content, compromising internet traffic, and prioritizing internet in exchange for fees. *See id.*

exercised its newfound jurisdiction over ISPs.[100] On April 1, 2016, the Commission issued a notice of proposed rulemaking (NPRM) on the privacy of customers of broadband and communications services.[101] The NPRM garnered over 275,000 submissions from providers, consumers, and other interested parties—including the FTC.[102]

The Commission adopted the proposed rules following the notice-and-comment period.[103] The regulations focused on providing consumers "transparency, choice, and data security" combined with "heightened protection for sensitive customer information."[104] The Commission established mechanisms to protect personally identifiable information—defined as "any information that is linked or reasonably linkable to an individual or device."[105] First, the Commission mandated "opt-in" consent to use and share location services, financial information, social security numbers, web browsing history, and other similar data.[106] Second, the Commission prohibited "take-it-or-leave-it" offers—situations where ISPs refused to provide services to non-consenting consumers.[107] Third, the rules mandated disclosure of data breaches.[108] Notably, the

100. *See, e.g.*, Proposed Rulemaking, *supra* note 12, at 2501.

101. *See generally id.*

102. Protecting the Privacy of Customers of Broadband & Other Telecommunications Services, WC Docket No. 16-106, Report and Order ¶ 4 (Oct. 27, 2016), https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1.pdf [hereinafter Report and Order]. *See generally* Protecting the Privacy of Customers of Broadband & Other Telecommunications Services, WC Docket No. 16-106, Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission (May 27, 2016), https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf [hereinafter Comment of the Staff].

103. Report and Order, *supra* note 102, ¶¶ 399–404.

104. *Id.* ¶ 5.

105. *Id.* ¶ 89.

106. FED. COMMC'N COMM'N, FACT SHEET: THE FCC ADOPTS ORDER TO GIVE BROADBAND CONSUMERS INCREASED CHOICE OVER THEIR PERSONAL INFORMATION 2 (Feb. 16, 2016) [hereinafter FACT SHEET]. The Commission does "infer consent" for certain purposes such as use and sharing of non-sensitive information to provide and market services and equipment typically marketed with the broadband service subscribed to by the customer. *Id.*

107. *Id.* at 3.

108. *Id.*

Commission explicitly stated that regulation over edge providers remained within the province of the FTC.[109]

E. DATA PRIVACY LITIGATION: PRELIMINARY PRECEDENT AND THE COURT'S OPINION IN *SPOKEO*

Data privacy lawsuits present three types of plaintiffs: victims of data breaches who have suffered material harm, victims of breaches who have yet to suffer harm, and those seeking to force companies into compliance with lawful data practices.[110] Plaintiffs in the first category generally have access to courts because they have suffered an injury like identity theft.[111] However, for the other classes of data privacy plaintiffs, Article III's "case-or-controversy" requirement presents a significant barrier to court access.[112] The Supreme Court outlined the "case-or-controversy" requirement in *Lujan v. Defenders of Wildlife*,[113] requiring putative plaintiffs to allege "an injury in fact," *i.e.*, a "concrete and particularized," "actual or imminent" "invasion of a legally protected interest."[114] Second, "a causal connection between the injury and the conduct complained of" must exist.[115] "Third, it must be 'likely' . . . that the injury will be 'redressed by a favorable judicial decision.'"[116]

1. Precedent Vacillates on Future Harm for Data Breaches

Plaintiffs' access to court—based on the possibility of future harm from data breaches—teetered between the Circuits. The Seventh Circuit noted "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's

---

109. *Id.* at 4.

110. *See generally* Caroline C. Cease, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395 (2014).

111. *Id.* at 397–98; *see, e.g.*, *Lambert v. Hartman*, 517 F.3d 433, 437–38 (6th Cir. 2014) (concluding plaintiff suffered an injury sufficient for Article III standing when a third party made purchases on her account using information on a ticket she received).

112. *See* U.S. CONST. art. III, § 2.

113. Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992).

114. *Lujan*, 540 U.S. at 560.

115. *Id.*

116. *Id.*

actions."[117] By contrast, the Sixth Circuit determined that allegations based on future harm failed to confer Article III standing in the absence of a "certainly impending" injury.[118]

The Supreme Court appeared to restrict Article III standing requirements in *Clapper v. Amnesty International USA*.[119] Though not a data breach case, the plaintiffs brought claims based on the "objectively reasonable likelihood" that the government would surveil their communications and the costs the plaintiffs incurred to protect client confidentiality.[120] The Supreme Court rejected these claims as an attempt to "manufacture standing."[121] Although the Court did not foreclose threatened injury as a proper basis for Article III standing, it articulated a fairly stringent temporal requirement, noting "'[a]llegations of *possible* future injury' are not sufficient."[122] Instead, threatened injury must be "certainly impending" to constitute injury in fact.[123]

---

117. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (citing Denney v. Deutsche Bank AG, 443 F.3d 253, 264–65 (2d. Cir. 2006) (stating future risk from exposure to toxic substances is a sufficient injury for Article III purposes); Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 574–75 (6th Cir. 2005) (holding a defective medical device's increased risk of future health problems a sufficient injury for Article III standing purposes); and Cent. Delta Water Agency v. United States, 306 F.3d 938, 947–48 (9th Cir. 2002) (permitting plaintiffs suit to continue even when the plaintiff's injury is a factual issue)). In *Pisciotta*, the plaintiffs sued Old National Bank after a data breach resulted in no identity theft, but forced the plaintiffs to incur costs for credit monitoring. *Pisciotta*, 499 F.3d at 631.

118. Reilly v. Ceridian Corp., 664 F.3d 38, 43 (6th Cir. 2011). *Reilly* presented facts similar to *Pisciotta*. *Id.* at 40. A hacker penetrated an information system belonging to Ceridian, a payroll processing company. *Id.* The plaintiffs brought claims based on increased threat of identity theft, incurred costs to monitor credit, and emotional distress. *Id.* The Sixth Circuit held that, unless the plaintiffs could show the hacker copied the information and used it, they did not suffer any harm. *Id.* at 43.

119. *See generally* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2012).

120. *Clapper*, 133 S. Ct. at 1143. The plaintiffs in *Clapper* believed government agencies monitored their communications with foreign individuals under § 1881 of the Foreign Intelligence Surveillance Act (FISA). *Id.* FISA authorized government agencies to engage in surveillance provided the government received approval from FISA courts. *Id.* at 1154–55. Plaintiffs believed they engaged in communications with "'people located in geographic areas that are a special focus' of the Government's counterterrorism or diplomatic efforts." *Id.* at 1145 (quoting plaintiff's App. to Pet. for Cert.).

121. *Id.* at 1155.

122. *Id.* at 1147 (alteration in original) (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

123. *Id.* at 1155.

The Seventh Circuit acknowledged *Clapper's* holding, but permitted a data breach class action to continue in *Remijas v. Neiman Marcus Group, LLC*.[124] Neiman Marcus suffered a data breach and disclosed it to customers who shopped in stores over the course of a year.[125] The evidence did not prove actual identity theft.[126] Given the uncontested evidence that hackers stole the plaintiffs' data, the Seventh Circuit declared, "it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach."[127] For the Seventh Circuit, this met the threshold for a certainly impending injury.

2. *Spokeo*: The Supreme Court Denies Court Access for Consumers Seeking to Enforce Their Privacy Interests

The Supreme Court kept the status of consumer data litigation in flux in *Spokeo v. Robbins*.[128] Spokeo operated a "people search engine" that gathered information about individuals and disseminated reports about them on publicly accessible websites.[129] Spokeo generated an inaccurate profile on the plaintiff in violation of the Fair Credit Reporting Act's requirement that consumer reporting agencies "'follow reasonable procedures to assure maximum possible accuracy of' consumer reports."[130] The plaintiff charged, among other matters, that the inaccurate report impaired his ability to secure employment.[131] The issue in *Spokeo* centered on whether the statutory violation put forth in the complaint satisfied the "[f]irst and foremost" requirement of Article III standing—whether the injury was concrete and particularized.[132] Although the Court took no position on the propriety of the Ninth Circuit's ultimate conclusion, it held the Circuit Court did not properly delineate between "concrete" and "particularized."[133] For standing

---

124. *See* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 697 (7th Cir. 2015).

125. *Remijas*, 794 F.3d at 690.

126. *Id*. at 692.

127. *Id*. at 693.

128. *See generally* Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).

129. *Id*. at 1544.

130. *Id*. at 1545 (quoting 15 U.S.C. § 1681e(b) (2012)).

131. *Id*. at 1554 (Ginsburg, J., dissenting).

132. *Id*. at 1547–48 (quoting Steel Co. v. Citizens for a Better Environment, 523 U.S. 83, 103 (1998)).

133. *Id*. at 1550.

purposes, "concrete" does not equate to tangible.[134] Justice Alito, quoting the opinion and Justice Kennedy's concurrence in *Lujan*, noted that Congress can elevate certain injuries "that were previously inadequate in law" and "articulate chains of causation that will give rise to a case or controversy where none existed before."[135] However, the Court held, "Article III standing requires a concrete injury even in the context of a statutory violation."[136] The Court did not detail how an intangible injury may satisfy the concrete requirement, but opined "[a] violation of one of the FCRA's procedural requirements may result in no harm."[137] Based on this, the Supreme Court determined that an inaccurate report by a credit agency, without more, was not a sufficiently concrete injury and remanded to the Ninth Circuit for further consideration.[138]

II. ANALYSIS

A dichotomy exists between the law and consumers' reasonable expectations about their privacy. Consumers want greater autonomy over their personally identifiable information and are unsettled by companies like Spokeo—even if the company produces a completely accurate report.[139] The FCC's slight entry into data privacy rulemaking in conjunction with

---

134. *Id.* at 1549 ("Although tangible injuries tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete.") (citing Pleasant Grove City v. Summum, 555 U.S. 460, 481 (2009) (recognizing intangible harm in restricting free speech); and Church of Lukumi Babalu Aye, Inc. v. City of Hialeah, 508 U.S. 520, 547 (1993) (classifying city ordinances restricting the free exercise of religion as an intangible injury sufficient for Article III purposes)).

135. *Id.* (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 578 (1992) and *Lujan*, 504 U.S. 555, 580 (Kennedy, J., concurring)).

136. *Id.*

137. *Id.* at 1550.

138. *Id.*

139. *See* SOLOVE, *supra* note 35, at 118–19 (discussing how, through the process of data aggregation, technology produces "digital dossiers" on people). *But cf.* Larry Downes, *The Downside of the FCC's New Internet Privacy Rules*, HARVARD BUS. REV. (May 27, 2016) https://hbr.org/2016/05/the-downside-of-the-fccs-new-internet-privacy-rules (arguing that data aggregation supports the services American consumers use every day, like Google, because of its dependency on ad revenue).

the FTC's enforcement approach represents what some experts consider a layered approach to internet regulation.[140]

A. THE FTC FALLS SHORT OF MEETING CONSUMER EXPECTATIONS ABOUT PRIVACY BECAUSE OF RESOURCE LIMITATIONS, ENFORCEMENT CONSTRAINTS, AND MARKET REALITIES

The FTC's measures to protect consumer data should be lauded, but the Agency's limited ability to protect consumers' privacy interests must be recognized. The Agency faces a Herculean task. Its jurisdiction over edge providers—whose numbers are in the billions—is only a subset of the Agency's oversight over the majority of American industry.[141] Seven divisions of the Agency regulate consumer protection, but only forty-six people staff the Agency's Division of Privacy and Identity Protection.[142] As such, the Agency averages about only ten complaints per year.[143] This diverts the Agency's regulatory focus from wielding industry-wide change to targeting low-hanging fruit.[144] Rather than forcing edge providers to evaluate whether they are honoring their privacy policies, the FTC's limited resources incentivize companies to ensure their practices are not so egregious as to warrant FTC scrutiny.[145]

The FTC's interactions with Google exemplifies the perverse incentives that exist under the Agency's regulatory approach. In 2012, the FTC reached a settlement with Google for violating its

---

140. Claffy & Clark, *supra* note 19, at 463. Generally, layered regulation posits different firms within the larger internet ecosystem can be subject to different regulations based on their differing speed of innovation, technological change and resources. *See id.* at 467, 480.

141. JOHN A. SPANOGLE ET AL., CONSUMER LAW: CASES AND MATERIALS 47 (4th ed. 2013) ("[The FTC] has jurisdiction over all U.S. entities except banks, savings and loan institutions, federal credit unions, common carriers and nonprofits . . . .").

142. Solove & Herzog, *supra* note 7, at 600–01.

143. *Id.* at 600 ("The FTC has lodged just over 170 privacy-related complaints since 1997, averaging about ten complaints per year.").

144. Thomas B. Norton, *The Non-Contractual Nature of Privacy Policies and the New Critique of Notice and Choice Privacy Protection Model*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 181, 204 (2016) (arguing the FTC's approach results in the agency only going after the most egregious offenders of data privacy practices).

145. *See* Grossman, *supra* note 69, at 1308 ("Thus, the FTC appears to expect companies to perform a cost-benefit analysis when designing its security program . . . .").

tracking policies.[146] The FTC heralded the victory and declared, "No matter how big or small, all companies must . . . keep their privacy promises to consumers . . . ."[147] Google begged to differ. The company did not admit wrongdoing and paid a fine many observers viewed as a drop in the bucket.[148] Moreover, during the same time period, Google announced a plan to consolidate user information across most of Google's services, which many privacy advocates viewed as a flagrant violation of its privacy policy.[149] The FTC acquiesced to this, and even worked toward dismissing complaints brought by consumer privacy groups to force the Agency to act.[150]

The FTC aspires for a harmonious balance between the divergent interests of consumers and edge providers. In reality, the latter complain the Agency does not provide concrete guidance to work with. "The FTC has been 'particularly tight-lipped about what data security standards it expects' companies to employ, and a 'chorus of lawyers and scholars have complained that enforcement is misguided absent clearer . . . standards.'"[151] Companies do not know at which point

---

146. *See Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, FED. TRADE COMMISSION (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented (highlighting Google's violation of an earlier privacy settlement between the company and the FTC, agreeing to settle for $22.5 million).

147. *See id.*

148. *See, e.g.*, Jessica Guynn, *Google Hit with Record $22.5 Million Fine for Safari Tracking*, L.A. TIMES (Aug. 10, 2012), http://articles.latimes.com/2012/aug/10/business/la-fi-google-ftc-20120810 (comparing the $22.5 million to Google's nearly $38 billion in profits the previous year).

149. Warwick Ashford, *Google Privacy Re-Write Raises Data Protection Concerns*, COMPUTER WKLY. (Jan. 25, 2015, 9:41 AM), http://www.computerweekly.com/news/2240114313/Google-privacy-re-write-raises-concerns ("Google's re-write of its privacy policies comes within months of reaching a settlement with the [FTC] for misrepresenting how it used personal information and for sharing a user's data without approval.").

150. *See, e.g.*, Motion to Dismiss, Elec. Privacy Info. Ctr. v. Fed. Trade Comm'n, No. 12-206-ABJ, 2012 WL 5884020 (D. D.C. Feb. 17, 2012); Complaint for Injunctive Relief, Elec. Privacy Info. Ctr. v. Fed. Trade Comm'n, No. 1:12-cv-00206, 2012 WL 413966 (D. D.C. Feb. 8, 2012).

151. Michael D. Simpson, *All Your Data Are Belong to Us: Consumer Data Breach Rights and Remedies in an Electronic Exchange Economy*, 87 U. COLO. L. REV. 670, 697 (2016) (quoting Patricia Bailin, *Study: What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices*, INT'L ASS'N OF PRIVACY PROFS.: WESTIN RES. CTR. (Sept. 19, 2014), https://iapp.org/news/a/study-what-ftc-enforcement-actions-teach-us-about-

their data practices will prompt an inquiry from the Agency. [152] While FTC enforcement actions may correct a particular company's practices, the ad hoc approach leaves little in the form of precedent: FTC enforcement actions generally result in settlements that permit companies to avoid any admission of wrongdoing.[153] Consequently, only three FTC actions provide any judicial guidance on unfair or deceptive data privacy practices.[154]

Perhaps recognizing its internal limitations, the FTC also "encourag[es] companies and self-regulatory organizations to adhere to high standards."[155] However, attempts at self-regulation have been plagued by "inadequate participation, weak enforcement, and standards that [are] not sufficiently protective."[156] Market incentives do not exist to meet the lofty promises of self-regulation.[157] Rather, companies seek to monetize consumer data as Google has—known as "Google envy."[158] Certainly, commoditization of data benefits consumers in that many of the essential services consumers enjoy on the internet would not be free without this phenomenon.[159]

---

the-features-of-reasonable-privacy-and-data-security-practices/)) (omission in original).

152. *See, e.g.*, Grossman, *supra* note 69, at 1309 (noting how the FTC refrains from mandating any technical changes and instead focuses on process and administrative oversight).

153. *See* Solove & Herzog, *supra* note 7, at 610 ("One of the main motivations for settling with the FTC is that it allows the company to avoid admitting wrongdoing in exchange for remedial measures.").

154. *Id.* at 610–11 (pointing to only one case resulting in a judicial opinion, and only two others currently awaiting resolution in federal district court).

155. Comment of the Staff, *supra* note 102, at 30.

156. Hirsch, *supra* note 26, at 464.

157. *See id.* at 458–59 (noting several deficiencies in the self-regulation approach).

158. Ohm, *supra* note 27, at 1426 (attributing "Google envy" to the company's ability to monetize their user's behavior); *see* Christopher Batiste-Boykin, In Re Google, Inc.: *ECPA, Consent, and the Ordinary Course of Business in an Automated World*, 20 INTELL. PROP. L. BULL. 21, 21 (2015) ("Either way, users of [edge] providers, like Google, should be wary because online communications are becoming a rich resource for companies to mine for data. As advances in technology occur . . . online communications will inform advertisers of users' tastes, preferences, beliefs, associations, interests, schedules, locations, ages, and incomes.").

159. *See, e.g.*, Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN. ST. L. REV. 777, 784 (2016) ("Services like Gmail, Google Calendar, and Facebook are only free because users' data empowers Google and Facebook to generate a lot of revenue from selling ads.").

However, there is a difference between Google's use of personally identifiable information to generate revenue from online advertising and OkCupid soliciting information about drug use and sexual history and selling it to purveyors of personal information.[160] Self-regulation does not adequately curb the troubling conduct of the latter.

B. *SPOKEO*'S OPINION LIMITS CONSUMERS' ABILITY TO LITIGATE THEIR OWN PRIVACY INTERESTS UNDER CONSUMER PROTECTION STATUTES

As stated above, several FTC statutes permit private rights of action. However, absent a worst-case scenario data breach, the federal private rights of action provide little redress to consumers.

Spokeo exacerbated this problem. Like most consumers, the plaintiff wanted readily accessible online information about him to be accurate and Spokeo failed to live up to its statutory obligations to ensure a modicum of accuracy.[161] However, using somewhat contradictory logic, the Supreme Court determined that this alone did not entitle the Plaintiff to court access.[162] The Court professed deference to Congressional judgment when faced with a statutory private right of action, noting "Congress is well positioned to identify intangible harms that meet minimum Article III requirements, its judgment is also instructive and important."[163] Despite this acknowledgment, the Court held the false report amounted to only a bare procedural

---

160. *Id.* at 801 (discussing how OkCupid, an internet dating site, solicits users about their sexual history and drug use and sells the information off to third parties); *see* Joseph Jerome, *Big Data: Catalyst for a Privacy Conversation*, 48 IND. L. REV. 213, 233 (2014) (noting there is little consensus in offering consumers control with regards to third party advertising industries).

161. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1544 (2016). Spokeo had been in hot water for the exact same issue before. The FTC extracted an $800,000 settlement from the company for, among other things, failing to ensure its profiles contained accurate information, a violation of the Fair Credit Reporting Act. *See Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA*, FED. TRADE COMMISSION (June 12, 2012), https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed.

162. *See generally id.*

163. *Id.*

harm.[164] Justice Alito analogized the incorrect report to an improperly reported zip code, noting "it is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm."[165]

Putting aside the questionable accuracy of Justice Alito's analogy, *Spokeo*'s effect on the Circuit Courts has not been favorable to consumers. In *Gubala v. Time Warner Cable*,[166] the Seventh Circuit upheld the District Court's dismissal of the plaintiff's case for lack of standing.[167] The plaintiff alleged that Time Warner Cable violated the Cable Act when it failed to dispose of his data following his termination of the services.[168] The Seventh Circuit "tentatively [assumed] that Time Warner violated the statute by failing to destroy the personally identifiable information."[169] Nevertheless, in light of *Spokeo*'s conclusion, the Seventh Circuit held that failure to destroy personally identifiable information amounted to a procedural harm.[170] The Eighth Circuit held as much in *Braitberg v. Charter Communications, Inc.*[171] Like *Gubala*, Charter Communications failed to destroy personally identifiable information after the plaintiff terminated his services.[172] The plaintiff failed to satisfy Article III standing because he did not allege, "Charter has disclosed the information to a third party; that any outside party has accessed the data, or that Charter has used the information in any way during the disputed period."[173]

Spokeo involved an FTC statute while *Braitberg* and *Gubala* dealt with FCC private rights of action. However, the effect is clear. The judiciary's commitment to Article III standing and concerns about judicial economy adversely impacts its

---

164. *Id*. at 1549 (stating that, had Robins alleged only a "bare procedural violation," it would not satisfy Article III's requirement for injury-in-fact).

165. *Id*. at 1550.

166. Gubala v. Time Warner Cable, Inc., 846 F.3d 909 (7th Cir. 2017).

167. *Id*. at 911.

168. *Id*. at 910.

169. *Id*.

170. *Id*. at 911 (dismissing plaintiff's arguments that the violations are substantive).

171. *See generally* Braitberg v. Charter Commc'n, Inc., 836 F.3d 925 (8th Cir. 2016).

172. *Id*. at 926.

173. *Id*. at 930.

receptiveness towards individual suits seeking to enforce privacy interests.[174]

C. THE FCC SHOULD REGULATE ISPS BECAUSE OF ITS BROAD REGULATORY APPROACH AND TECHNICAL EXPERTISE IN OVERSEEING COMMUNICATIONS

As the specter of regulation tends to do, the FCC's regulatory shifts sent shudders through some interested parties.[175] As to the Commission's data privacy rulemaking, commentators lamented that the "rules would impose additional costs on both consumers (in terms of time) and broadband providers (in terms of time and resources) for no obvious beneficial purpose."[176] Others said that it would foment regulatory confusion on the matter.[177] However, for reasons stated below combined with pervasive incentives to monetize consumer data, a strong regulatory regime specific to ISPs is necessary.[178]

---

174. *See generally* Gubala v. Time Warner Cable, Inc., 846 F.3d 909 (7th Cir. 2017); *Consumer Protection*, 29 BUS. TORTS REP. 89 (2017) ("[*Spokeo v. Robins*] wreak[s] havoc on consumers' efforts to seek statutory damages for violations of consumer financial and privacy protection laws.").

175. *See* Marsha Blackburn, *Why We Need a Free Market Approach for the Communications and High-Tech Sectors*, *in* COMMUNICATIONS LAW AND POLICY IN THE DIGITAL AGE: THE NEXT FIVE YEARS, *supra* note 88, at 12 (classifying net neutrality reclassification as "freedom destroying"); *see also* Downes, *supra* note 139 (arguing that data aggregation supports the services American consumers use every day, like Google, because of its dependency on ad revenue).

176. Rosemary C. Harold, *The FCC Forgot Something in Piecing Together Its Complex Proposal for Broadband Privacy Regulation: Consumers*, 17 FEDERALIST SOC'Y REV. 62, 63 (2016).

177. *See* Protecting the Privacy of Customers of Broadband & Other Telecommunications Services, WC Docket No. 16-106, Comments of CTIA 1–2 (May 26, 2016), https://ecfsapi.fcc.gov/file/60002064853.pdf; *see also* Maureen K. Ohlhausen, Comm'r, Fed. Trade Comm'n, Public Policy Briefing on Privacy Regulation after Net Neutrality at the George Mason University School of Law: The FTC, The FCC, and BIAS (Mar. 30, 2016), https://www.ftc.gov/system/files/documents/public_statements/942823/160331gmuspeech1.pdf (arguing against different sets of regulation for similarly situated companies in the internet ecosystem and that ISPs are similarly situated to edge providers).

178. Data brokers are the prime example of the monetary incentive that exists for data. Data brokers purchase personal information from different sources to compile digital dossiers. *See* Hirsch, *supra* note 26, at 449–50. Because data brokers seek to connect the digital with the physical person, ISPs are especially attractive because they have access to both kinds of information. *See id.* (citing FED. TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS 4, 13 (2000)).

For its part, the FTC issued a measured response to the FCC's rulemaking that belied what some observers deem a "turf war" between the two agencies.[179] The Agency characterized the prospect of two regulatory regimes as "not optimal."[180] Although the FTC commended the FCC for considering privacy interests, the Agency affirmed its ability enforce consumer privacy interests under its Section 5 enforcement powers, stating that the notice-and-choice model "maximizes consumer self-determination."[181]

Instead of speculating about the prospect of a dual regulatory regime over ISPs, the FTC should relent to the FCC. Although the FCC's rules may have a negligible effect on the broader internet ecosystem, they provide rigorous guidelines that vindicate consumer privacy interests in ways the FTC and the judiciary cannot.

The FCC's rulemaking stemmed from the premise that ISPs sit in a heightened position in the internet ecosystem as the "gatekeeper."[182] The FCC's basic contention is correct for four reasons. First, ISPs provide the bridge between the edge provider and the consumer; they maintain, control, and transmit the data between the two.[183] Second, ISPs "enjoy a confluence of both a total view into subscribers' Internet access habits on one hand, and knowledge of physical information about subscribers such as home address and financial information on the other."[184]

---

179. *See, e.g.*, Kate Cox, *Final FCC Privacy Rule Won't Ban Pay-For Privacy, Will Require Some Opt-Ins*, CONSUMERIST (Oct. 6, 2016, 2:01 PM), https://consumerist.com/2016/10/06/final-fcc-isp-privacy-rule-doesnt-ban-pay-for-privacy-does-require-some-opt-ins/ (discussing ISP industry lamentations over a "turf war" between the FTC and FCC); Amir Nasr, *Roles of FTC, FCC Are Front and Center in Privacy Debate*, MORNING CONSULT (Sept. 27, 2016), https://morningconsult.com/2016/09/27/roles-ftc-fcc-front-center-privacy-debate/ ("'It's a turf war. Let's be honest. It's a turf war,' said Tim Sparapani, senior policy counsel at CALinnovates, a technology advocacy coalition."); *see also* Maureen K. Ohlhausen, *Why Is the FCC Insensitive to Data Sensitivity?*, THE HILL (Sept. 22, 2016, 10:10 AM), http://thehill.com/blogs/congress-blog/technology/297194-why-is-the-fcc-insensitive-to-data-sensitivity.

180. *See* Comment of the Staff, *supra* note 102, at 8.

181. *See* Ohlhausen, *supra* note 177, at 3.

182. *See* Proposed Rulemaking, *supra* note 12, at 2501–03. *But see* Ohlhausen, *supra* note 177, at 4–7. The FTC questions to what extent ISPs enjoy special status in the internet ecosystem.

183. *See* Ohm, *supra* note 27, at 1423 ("[The ISP's] principal role is routing—it receives communications from its users and sends them out to the rest of the world, and vice versa . . . .").

184. FELD ET AL., *supra* note 27.

Third, the market between ISPs and edge providers are polar opposites—the former is concentrated while the latter grows exponentially.[185] Fourth, demand for ISPs is inelastic. Consumers must provide their personally identifiable information to ISPs if they want to enjoy the functionality of the internet.[186]

As stated above, the FTC's limited resources and selective enforcement hamper its ability to spur industry-wide change. Were the FTC to continue leading the way on ISP data privacy, it would perpetuate the "whack-a-mole" problem.[187] The FTC's battles with Google exemplify the issue; where the Agency succeeds in stopping one privacy practice, another one emerges.[188] The FCC's rulemaking authority offers a solution and provides a dual benefit for data privacy standards in general. First, rulemaking eschews targeted enforcement in favor of baseline standards for acceptable conduct for ISPs.[189] Although regulations in the form of rulemakings are contentious and often the subject of derision amongst policy makers, the alternative thrusts ISPs into the jurisdiction of the FTC—and the anomalous results it produces.[190] Rulemakings, by contrast, immediately establish a duty of care on the ISP without compromising the entity's ability to collect information needed to provide the service.[191]

---

185. *Compare* Seth L. Cooper, *Restoring Minimal Regulatory Environment for a Healthy Wireless Future*, *in* COMMUNICATIONS LAW AND POLICY IN THE DIGITAL AGE: THE NEXT FIVE YEARS, *supra* note 88, at 83, *with Total Number of Websites*, INTERNET LIVE STATS, http://www.internetlivestats.com/total-number-of-websites/ (last visited Mar. 9, 2017).

186. *See* FELD ET AL., *supra* note 27, at 46 ("[C]onsumers generally cannot opt out of a BIAS provider's data collection without opting out of the Internet entirely.").

187. McGeveran, *supra* note 7, at 987.

188. *See id.* at 999–1000.

189. Robert Innes, *Enforcement Costs, Optimal Sanctions, and the Choice Between Ex-Post Liability and Ex-Ante Regulation*, 24 INT'L REV. L. & ECON. 29, 31 (2004) ("The advantage of ex-ante regulation . . . is that it leverages enforcement resources to greater effect by *always* sanctioning negligent conduct . . . .").

190. *See* Blackburn, *supra* note 175 (deriding the FCC's Open Internet Order); *see also* Ohlhausen *supra* note 177 (criticizing the general outline of the FCC's privacy rules); Simpson, *supra* note 151 (identifying complaints about the FTC's privacy regulation).

191. *See* FELD ET AL., *supra* note 27, at 62.

The FCC's rulemaking provides the additional benefit of placing autonomy in the hands of consumers while closing the knowledge gap between the consumer and ISP. Observers speculate that consumers participate in an unequal playing field in terms of knowing to what extent ISPs and edge providers use their personally identifiable information.[192] Perhaps exploiting this advantage, ISPs and edge providers dictate opaque privacy policies that facilitate maximum control over consumer information.[193] The FCC's rulemaking shifts a modicum of control back to the consumer. For example, the default to opt-in of sharing information reflects consumer sentiments about seeking greater control of their data.[194] Second, the rulemaking empowers consumers to understand these polices to a greater degree because it mandates that ISPs provide information about how they collect and use data.[195]

With that said, the degree to which data engineers the internet consumers enjoy today cannot be denied. Data collection and monitoring increase cybersecurity and facilitate basic online services.[196] The FCC's policy objectives strike the delicate balance between honoring legitimate data practices while meeting reasonable privacy expectations.[197] The TCPA demonstrates how the FCC accomplishes this feat. At its peak, retail from telemarketing totaled sales of $435 billion.[198] However, telemarketing also spawned abusive practices like

---

192. Yong Jin Park, *Digital Literacy and Privacy Behavior Online*, 40 COMM'N RES. 215, 232 (2013) ("[U]sers are stratified and far from competent in exercising privacy control, different from such policy premise. Furthermore, . . . the levels of understanding of surveillance practices common in websites remain miniscule among the majority of users.").

193. Gerald R. Faulhaber, *Transparency and Broadband Internet Service Providers*, 4 INT'L J. COMMC'N 738, 745 (2010) (discussing the incentive for ISPs to hide privacy policies because of the ability of data to generate revenue).

194. *See* FACT SHEET, *supra* note 106, at 3.

195. *Id.*

196. *See* Ohm, *supra* note 27, at 1466–67 (identifying four helpful functions ISPs derive from data monitoring: (1) monitoring broadband traffic, (2) detecting spam, (3) detecting viruses, (4) securing and policing bandwidth); *see also* Downes, *supra* note 139.

197. *See, e.g.*, FELD ET AL., *supra* note 27, at 35 ("[T]he FCC has a twin mandate to protect consumers and to promote . . . competition.").

198. Consuelo Lauda Kertz & Lisa Boardman Burnette, *Telemarketing Tug-of-War: Balancing Telephone Information Technology and the First Amendment with Consumer Protection and Privacy*, 43 SYRACUSE L. REV. 1029, 1055 (1992).

telemarketing scams.[199] The FCC, in conjunction with the FTC, tailored restrictions on the time and form of telemarketing calls.[200] Twenty years later, privacy advocates declare the TCPA to be an "enormous success."[201]

Finally, from a broad policy perspective, it makes sense to demarcate regulatory jurisdiction between ISPs and edge providers, with the former subject to FCC rulemakings and the latter subject to the FTC. The FCC traditionally regulates "core communications"—be they telephone, cable, or radio communications.[202] These traditionally separate industries and services are collapsing and converging.[203] Recognizing the industry reality, it makes little sense to continue fragmented classification of broadband providers when they provide the same telecommunications services on an increasingly large scale.

III. CONCLUSION

The problems posed by voluminous compendiums of personally identifiable information show no signs of abating. What is increasing is consumer awareness about these issues. The breadth of the internet ecosystem poses significant

---

199. *See id*. at 1056.

200. *See Complying with the Telemarketing Sales Rule*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/guidance/complying-telemarketing-sales-rule (last visited Feb. 28, 2017).

201. Letter from Mark Rotenberg, President, EPIC, Claire Garland, Director, EPIC Consumer Privacy Project, & James Graves, Fellow, EPIC Law & Tech., to The Honorable Greg Walden, Chairman, U.S. House of Representatives Comm. on Energy & Commerce, & The Honorable Anna Eshoo, Ranking Member, U.S. House of Representatives Comm. on Energy & Commerce (Sept. 21, 2016), http://docs.house.gov/meetings/IF/IF16/20160922/105351/HHRG-114-IF16-20160922-SD004.pdf.

202. *See* Speta, *supra* note 88, at 71.

203.

> [E]mploying new digital broadband networks, traditional 'telephone' companies began offering multichannel video services, and 'cable television' operators began offering voice services. Both telephone companies and cable operators, along with 'cell phone' providers, offered data services over increasingly higher-speed broadband networks . . . . Of course, the old labels commonly used to denominate the various service providers, such as 'telephone' or 'cable television' or 'cell phone' companies, became increasingly obsolete as the marketplace continued to evolve.

Randolph J. May, *Introduction: Overhauling Communications Law and Policy in the Digital Age*, *in* COMMUNICATIONS LAW AND POLICY IN THE DIGITAL AGE: THE NEXT FIVE YEARS, *supra* note 88, at 5.

regulatory challenges that the FTC is ill-equipped to deal with, despite the Agency's best efforts. Therefore, consumers should welcome the FCC lending its own expertise to the matter. Although the scope of the Commission's rulemaking can only go so far, it establishes baseline default rules for actors in the internet ecosystem who have unique access to consumer data. This also frees up resources for the FTC to regulate edge providers. In addition, the regulatory environment for ISPs and edge providers must be robust, as consumers have limited recourse to litigate their own privacy interests in court.

***