Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 26, *Issue* 1 2015 *Article* 5

VOLUME XXVI BOOK 1

Internet Privacy Enforcement After Net Neutrality

Thomas B. Norton*

*Fordham Center on Law and Information Policy (CLIP); Fordham University School of Law

Internet Privacy Enforcement After Net Neutrality*

Thomas B. Norton

Abstract

In March 2015, the Federal Communications Commission reclassified broadband Internet access service providers as "common carriers" subject to obligations under Title II of the Communications Act. One such obligation is to comply with the Act's section 222 privacy provisions. As a result of reclassification, the Federal Communications Commission claims privacy enforcement jurisdiction over a broad swath of companies that formerly fell within the Federal Trade Commission's regulatory reach. The Federal Trade Commission and industry players have been outwardly critical of this effect. This Note explores the resulting tension between the two agencies and proposes potential resolutions for it.

KEYWORDS: Net Neutrality, Internet, Internet Privacy, Privacy, FCC, FTC

---

*I would like to thank Professor Olivier Sylvain for his thoughtful advice and insightful feedback on this Note. I would also like to thank Professor Joel Reidenberg for his commentary and support. Special thanks to Liz Walker and the Fordham IPLJ editors for the opportunity to publish this Note, and to the IPLJ staff for their efforts.

Internet Privacy Enforcement After Net Neutrality

Thomas B. Norton*

In March 2015, the Federal Communications Commission reclassified broadband Internet access service providers as "common carriers" subject to obligations under Title II of the Communications Act. One such obligation is to comply with the Act's section 222 privacy provisions. As a result of reclassification, the Federal Communications Commission claims privacy enforcement jurisdiction over a broad swath of companies that formerly fell within the Federal Trade Commission's regulatory reach. The Federal Trade Commission and industry players have been outwardly critical of this effect. This Note explores the resulting tension between the two agencies and proposes potential resolutions for it.

* Privacy Fellow, Fordham Center on Law and Information Policy (CLIP); J.D. Candidate, 2016. I would like to thank Professor Olivier Sylvain for his thoughtful advice and insightful feedback on this Note. I would also like to thank Professor Joel Reidenberg for his commentary and support. Special thanks to Liz Walker and the Fordham IPLJ editors for the opportunity to publish this Note, and to the IPLJ staff for their efforts.

INTRODUCTION: THE FCC'S OPEN INTERNET ORDER HAS CAUSED INTERAGENCY TENSION OVER INTERNET PRIVACY ENFORCEMENT

In March 2015, the Federal Communications Commission ("FCC") released its Open Internet Order (the "Order"), which established new net neutrality rules applicable to broadband Internet access service providers.[1] These rules, which will apply to both fixed and mobile broadband providers, have multiple effects. Among others, the rules prohibit blocking, throttling, and paid prioritization of broadband Internet services.[2] The rules also require heightened transparency from broadband service providers and dictate their future conduct.[3] But most significantly for this Note, the rules reclassify broadband Internet access service as a telecommunications service under Title II of the Communications Act.[4]

In the Order, the FCC elected to forbear from applying some provisions of Title II to newly reclassified broadband Internet services providers.[5] But with respect to certain of the Title's other provisions, the FCC elected *not* to forbear application. One of these provisions is section 222 of Title II of the Communications Act, which governs the privacy of data known as Customer Proprietary Network Information ("CPNI").[6] The FCC's election to not forbear from applying this section means that newly reclassified broadband Internet service providers are subject to the same privacy obligations as those imposed upon telephone service providers.[7] By extending section 222 to cover broadband Internet service providers this way, the FCC's rule supplants the Federal Trade Commission's ("FTC") authority to regulate those companies,

---

1 *See In re* Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601 (2015) [hereinafter 2015 Open Internet Order].

2 *See id.* paras. 110–32.

3 *See id.* para. 109.

4 *See id.* paras. 306–87.

5 *See id.* paras. 434–60.

6 *See id.* paras. 462–67; *see also infra* notes 31–33 and accompanying text.

7 *See* 2015 Open Internet Order, *supra* note 1, para. 462.

because the FTC lacks jurisdiction over telecommunications service providers.[8]

Because of this, some FTC representatives have spoken out in opposition of reclassification.[9] Other privacy advocates, on the other hand, view reclassification and section 222 forbearance as a victory for consumer privacy.[10] Nevertheless, the FCC's action has created an interagency tension that raises many interesting questions. First, what does the Order say about privacy, and how does this alter the FCC and FTC's respective privacy enforcement authority? What effect do the Order's mandates have on the FTC and FCC's ability to adequately address those privacy concerns that each is charged with policing? What explains the perceived interagency tension to which the FCC's action gives rise? And finally, what might be done to resolve that tension? I address these questions in the remainder of this Note.

I proceed in four Parts. In Part I, I recount the pre-Open Internet Order online privacy landscape. I will describe both the FTC and FCC's privacy enforcement authority and summarize recent privacy enforcement actions taken by each agency.

In Part II, I discuss the Order's approach for regulating online privacy. I will note the ways in which the Order addresses or fails to address a shifting online privacy enforcement regime.

In Part III, I outline how the Order's language drastically alters the online privacy landscape. First, I describe how the FCC's election to not forbear from applying section 222 privacy obligations to broadband Internet service providers dramatically expands those providers' privacy obligations. I also explain how these broad new obligations expose those providers to increased risk of enforcement. Finally, I devote substantial discussion to jurisdictional challenges that result from reclassification. This discussion focuses mainly on the FTC's discontent with the effect of reclassification of broadband Internet service providers as Title II "common carri-

---

[8] *See* 15 U.S.C. §§ 44, 45(a)(2) (2012). Because broadband Internet services have hitherto not been offered on a common carrier basis, the FTC has exercised jurisdiction over those services. *Id.*; *see also* FTC v. Verity Int'l, Ltd., 443 F.3d 48, 58–60 (2d Cir. 2006).

[9] *See infra* Part III.C.2.

[10] *See infra* Part III.C.2.

ers" on its privacy enforcement authority, as well as on possible explanations for this response.

In Part IV, I analyze possibilities for resolving the jurisdictional challenges that reclassification raises. These possibilities include the FCC's promulgating FTC-like privacy rules, Congress' repealing the Federal Trade Act's common carrier exception, and an FCC/FTC co-governance regime.

I. THE PRE-OPEN INTERNET ORDER PRIVACY ENFORCEMENT LANDSCAPE

As consumers grow more interested in the privacy of their personal information, so grow efforts to regulate privacy online. While many are familiar with the FTC's role as a privacy and security enforcer, the FCC very recently adopted an aggressive approach to broadening its authority to enforce privacy against the entities it regulates. In this Part, I frame both agencies' authority and approach to privacy enforcement.

A. FTC Privacy Enforcement

The FTC is the agency charged with protecting consumers and their privacy.[11] As part of its privacy efforts, the FCC conducts studies and issues reports, hosts public workshops, develops educational materials for both consumers and industry, and influences privacy-related legislation and regulation.[12] The FTC has authority to enforce a variety of sectoral privacy laws, such as the Children's Online Privacy Protection Act ("COPPA") and the Gramm-Leach-Bliley Act ("GLB").[13] In addition, the FTC offers an "en-

---

[11] *See* FED. TRADE COMM'N, 2014 PRIVACY AND DATA SECURITY UPDATE 1 (2015), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf [https://perma.cc/H9FF-UV99] [hereinafter 2014 PRIVACY AND SECURITY UPDATE].

[12] *See id.*

[13] *Id.* COPPA requires websites and apps to obtain parental consent before collecting personal information from users who are under the age of thirteen. *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6502 (2000). The FTC has brought over twenty COPPA cases and has revised the COPPA rule to meet developments in social networking, Internet access on smartphones, and geolocation tracking that implicate children's privacy. 2014 PRIVACY AND SECURITY UPDATE, *supra* note 11, at 7. The GLB Act requires financial institutions to send consumers annual privacy notices and

forcement backstop" for the Safe Harbor Agreement through which United States companies transfer customer data to and from the European Union in a manner consistent with European Union law.[14]

But recently, the primary thrust of the FTC's consumer protection authority has come from section 5 of the Federal Trade Commission Act ("FTC Act"), which prohibits unfair or deceptive market practices.[15] Through investigation and subsequent enforcement action, the FTC addresses consumer protection violations by ordering companies to remedy unlawful behavior.[16] Such orders typically require that malfeasant companies take specific remedial steps, including that they implement comprehensive privacy and data security programs, delete unlawfully-obtained consumer information, provide adequate notice and choice about privacy practices, and other measures.[17] The FTC has brought enforcement actions against, and has entered into settlements with, many companies, including well-known companies such as Google, Facebook, Twitter, and Microsoft.[18]

---

provide the opportunity to opt out of having their information shared with certain third parties. *Id.* The FTC has brought nearly thirty cases against GLB Act violators, including three in 2014. *See id.* at 6.

14 *See* 2014 PRIVACY AND SECURITY UPDATE, *supra* note 11, at 6–7. On October 6, 2015, the Court of Justice of the European Union declared the safe harbor framework invalid as a means to legitimize transfers of personal data between the EU and the United States. *See* Case C-362-14, Schrems v. Data Protection Comm'r (Oct. 6, 2015), http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en [http://perma.cc/JAJ8-K5XC].

15 *See* 15 U.S.C. § 45 (2012) (declaring unfair methods of competition unlawful and delineating means for preventing them). In August 2015, the FTC issued a Statement of Enforcement Principles that "describes the underlying antitrust principles that guide the [FTC's] application of its statutory authority to take action against unfair methods of competition prohibited by [s]ection 5 of the FTC Act." Fed. Trade Comm'n, *FTC Issues Statement of Principles Regarding Enforcement of FTC Act as a Competition Statute*, FTC (Aug. 13, 2015), https://www.ftc.gov/news-events/press-releases/2015/08/ftc-issues-statement-principles-regarding-enforcement-ftc-act [https://perma.cc/4BUS-TGQV]; *see also* Fed. Trade Comm'n, *Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act*, FTC (Aug. 13, 2015), https://www.ftc.gov/system/files/documents/public_statements/735201/150813section5enforcement.pdf [https://perma.cc/R5CV-24HS].

16 *See* 2014 PRIVACY AND SECURITY UPDATE, *supra* note 11.

17 *Id.*

18 *See id.*

Several recent enforcement actions exemplify the FTC's enforcement approach. In one, the FTC charged a company called Jerk, LLC (operating under the domain Jerk.com) for perpetuating an extortionary scheme that involved harvesting information from individuals' Facebook profiles to fabricate false profiles labeling the individuals either as a "Jerk" or "not a Jerk."[19] After it created a profile, Jerk.com would then contact those individuals whose information appeared in the profile to advise them that they could revise those profiles by paying the company thirty dollars in "membership" fees.[20] The FTC's complaint alleged that Jerk.com misled its victims by claiming that the profiles had been created by other Jerk.com members and that by paying for a site membership they would have access to "premium" features.[21] On March 25, 2015, the FTC announced that in a five-to-zero vote, it granted summary decision against Jerk.com for these misleading practices.[22]

In *In re Snapchat, Inc.*, another recent enforcement action, the photo-sharing app settled charges that it deceived consumers by promising that "snaps"—photos taken by one user and sent to another—would "disappear[ ] forever" after a sender-specified time period expired.[23] The FTC intervened because, in reality, photo recipients could save snaps indefinitely using relatively simple methods (such as by taking screenshots or installing third-party apps).[24] Here, the FTC again voted five-to-zero to settle its charges

---

[19] Fed. Trade Comm'n, *FTC Charges Operators of "Jerk.com" Website With Deceiving Consumers*, FTC (Apr. 7, 2014), https://www.ftc.gov/news-events/press-releases/2014/04/ftc-charges-operators-jerkcom-website-deceiving-consumers [https://perma.cc/939G-SZ6P]. *See generally* Complaint, *In re* Jerk, LLC, No. 122 3141 (F.T.C. Apr. 2, 2014), https://www.ftc.gov/system/files/documents/cases/140407jerkpart3cmpt.pdf [http://perma.cc/RGT8-WAEM] [hereinafter Jerk Complaint].

[20] *See* Jerk Complaint, *supra* note 19, at 2.

[21] *See id.* at 5–6.

[22] Fed. Trade Comm'n, *FTC Rules Jerk, LLC and John Fanning Deceived Consumers, Violated FTC Act*, FTC (Mar. 25, 2015), https://www.ftc.gov/news-events/press-releases/2015/03/ftc-rules-jerk-llc-john-fanning-deceived-consumers-violated-ftc [https://perma.cc/7XMB-M7EF].

[23] Complaint at 1, 2–4, *In re* Snapchat, Inc., No. 132 3078 (F.T.C. Dec. 23, 2014), https://www.ftc.gov/system/files/documents/cases/140508snapchatcmpt.pdf [http://perma.cc/NM49-GQ64].

[24] *See id.* at 3–4.

against Snapchat.[25] The FTC noted that the settlement marked another example of the agency's "ongoing effort to ensure that companies market their apps truthfully and keep their privacy promises to consumers."[26]

These are just a few examples—the FTC has brought over 115 privacy and security-related enforcement actions over the past fifteen years.[27] The FTC's privacy jurisprudence is so robust that some contend that it amounts to the functional equivalent of a "common law of privacy."[28] Though there exists "hardly any judicial opinions to show for it" (as most of the enforcement actions end in settlement), privacy law professionals and lawyers facing privacy issues "parse and analyze the FTC's settlement agreements, reports, and activities as if they were pronouncements by the Chairman of the Federal Reserve."[29] Accordingly, the FTC's privacy-related activity is said to be "the broadest and most influential regulating force on information privacy in the United States."[30]

But the FTC is not the lone privacy sheriff. The FCC has the authority to enforce privacy violations against entities falling within its regulatory domain.

B. FCC Privacy Enforcement

Like the FTC, the FCC protects consumers' privacy enforcement. The FCC's privacy enforcement authority comes from section 222 of the Communications Act,[31] which requires that telecommunications carriers "protect the confidentiality of [custom-

---

[25] Fed. Trade Comm'n, *FTC Approves Final Order Settling Charges Against Snapchat*, FTC (Dec. 31, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-approves-final-order-settling-charges-against-snapchat [https://perma.cc/DTB6-AWAK].

[26] *Id.*

[27] *See* Joel R. Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, I/S: J.L. & POL'Y FOR INFO. SOC'Y (2014), http://moritzlaw.osu.edu/students/groups/is/files/2015/01/Privacy-Harms-and-Notice-and-Choice-01-12-2015-1-4.pdf [http://perma.cc/6YDC-LZZT].

[28] *See, e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 583 (2014).

[29] *Id.* at 585.

[30] *Id.* at 587.

[31] 47 U.S.C. § 222 (2008).

ers'] proprietary information" and ensure that it is not disclosed to third parties without consumers' consent.[32] The Communications Act defines "customer proprietary network information" ("CPNI") as that information related to customers' use of a telecommunications service and the customers' billing information as it relates to that service.[33] CPNI includes details about customers' calls, including duration, frequency, time, and number dialed.[34] It does not include "subscriber list information" such as name, address, and phone number.[35]

The core privacy requirement for telecommunications carriers is contained in section 222(c), which sets forth the confidentiality protections that apply to CPNI.[36] Per this provision, a carrier may only use, disclose, or permit access to customers' individually identifiable CPNI in limited circumstances: (1) as required by law; (2) with the customer's approval; or (3) as part of its provision of the telecommunications service from which such information is derived, or as part of services necessary to or used in the provision of such telecommunications service.[37] Exceptions to the confidentiali-

---

[32] *See id.* § 222(a).

[33] *See id.* § 222(h)(1) (defining "customer proprietary network information" as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier").

[34] *See id.*

[35] *See id.*

[36] *See id.* § 222(c)(1) ("Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories."). Section 222(a) imposes a general duty on telecommunications carriers to protect the confidentiality of proprietary information relating to other carriers, equipment manufacturers, and customers. *See id.* § 222(a). Section 222(b) provides that a carrier receiving or obtaining proprietary information from other carriers for the purpose of providing a telecommunications service is restricted to use such information only for that purpose; the provision further provides that a carrier may not use that information for its own marketing efforts. *See id.* § 222(b).

[37] *See id.* § 222(c).

ty provisions permit carriers to use, disclose, or permit access to customer proprietary network information in other limited circumstances, including: (1) to initiate, provide, bill for, and collect payment for telecommunications services; (2) to protect the rights or property of the carrier, its customers, and other carriers from improper use of those services; (3) to provide inbound telemarketing, referral, or administrative services to customers; and (4) to provide a customer's call location information in cases of emergency.[38]

In October 2014, the FCC took a "significant step"[39] toward protecting the privacy of information that falls beyond the traditional scope of CPNI.[40] In *In re TerraCom, Inc.*, the FCC held that the Communications Act's privacy protections extend to "all types of information that should not be exposed widely to the public, whether because that information is sensitive for economic reasons or for reasons of personal privacy."[41] Though the FCC did not precisely define those data types included within the scope of "personal privacy" protection, it found "informative" the National Institute of Standards and Technology's ("NIST") definition of "personally identifiable information."[42]

---

[38] *See id.* § 222(d).

[39] Alex Stout, *FCC Imposes Record Penalty for Data Breach*, LATHAM & WATKINS: GLOBAL PRIVACY & SEC. COMPLIANCE L. BLOG (Apr. 14, 2015), http://www.globalprivacyblog.com/privacy/fcc-imposes-record-penalty-for-data-breach/ [http://perma.cc/F479-7CEM].

[40] *See generally In re* TerraCom, Inc., Notice of Apparent Liability for Forfeiture, 29 FCC Rcd. 13325 (2014) [hereinafter TerraCom Notice of Apparent Liability for Forfeiture] (determining that TerraCom, Inc. and YourTel America, Inc. have apparently willfully and repeatedly violated sections 222(a) and 201(b) of the Communications Act of 1934).

[41] *Id.* para. 14.

[42] *See id.* para. 17. NIST defines "personally identifiable information" as:

> [A]ny information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) 2-1 (2010), http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf [http://perma.cc/T5RS-YN3X] (quoting U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-

In the case, TerraCom and YourTel—companies that offered telephone services to low-income Americans through the FCC's Lifeline program[43]—faced investigation for their treatment of personal information that they collected from individuals to determine those individuals' eligibility to participate in the Lifeline program.[44] Discovery revealed that the companies left collected information, which included Social Security numbers and evidence of participation in other government assistance programs, unencrypted in the form of readable text accessible on the Internet.[45] This prompted the FCC's investigation.

In finding culpability, the FCC first noted that regulated entities have a duty to protect their customers' general "proprietary information"—not only their specific CPNI information.[46] The FCC determined that TerraCom and YourTel had breached that duty.[47] In addition to relying on section 222, the FCC cited section 201(b)'s requirement that regulated entities engage in "just and reasonable" conduct and determined that TerraCom and YourTel's failure to use "even the most basic and readily available technologies and security features," and the companies' failure to notify affected customers that their data had been breached, were neither just nor unreasonable.[48]

08-0536, PRIVACY: ALTERNATIVES EXIST FOR ENHANCING PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (2008), http://www.gao.gov/new.items/d08536.pdf [http://perma.cc/8UQL-PKUM]).

[43] The Lifeline program is a "retail voice telephony service that telecommunications carriers provide to qualifying low-income consumers for a reduced charge." TerraCom Notice of Apparent Liability for Forfeiture, *supra* note 40, at 1 n.1 (citing 47 C.F.R. § 54.407(b) (2015)); *see also* 47 C.F.R. §§ 54.400–.422; Lifeline and Link Up Reform and Modernization, 27 F.C.C. Rcd. 6656, paras. 11–18 (2012).

[44] *See* TerraCom Notice of Apparent Liability for Forfeiture, *supra* note 40, para. 2.

[45] *See id.* paras. 4–5.

[46] *See id.* para. 14–15 (noting that "[s]ection 222(a) of the Communications Act imposes a duty on every telecommunications carrier to protect the confidentiality of [customers'] 'proprietary information,'" that "Congress used the term 'proprietary information' broadly to encompass all types of information that should not be exposed widely to the public," and that "[h]ad Congress wanted to limit the protections of subsection (a) to CPNI, it could have done so").

[47] *See id.* para. 30 (explaining that the companies' failure to "employ[ ] appropriate security measures" to protect their customers' information amounted to a breach of the duty imposed by section 222(a)).

[48] *See id.* para. 12.

By a three-to-two vote, the FCC fined the two companies $10 million.[49] The case marks the first time that the agency wielded its enforcement authority to police data security practices, and according to Enforcement Bureau Chief Travis LeBlanc, it "will not be the last."[50]

The FCC followed the aggressive approach it took in *TerraCom* when it took enforcement action against AT&T. In *In re AT&T Services, Inc.*,[51] the FCC investigated whether the company failed to properly protect customers' confidential information.[52] In that case, third-party vendors in Mexico, Colombia, and the Philippines handled customer service calls.[53] The third-party representatives in these locations had access to customers' sensitive personal information, including names and at least the last four digits of Social Security numbers.[54]

Third-party representatives in Mexico used their login credentials to access the customer information.[55] The representatives then used the accessed customer data to unlock stolen AT&T handsets via online request forms.[56] In total, the Mexican employees made more than 290,000 unlock requests using data from more than 50,000 customers.[57] Similarly, representatives in Colombia and the Philippines accessed the data of approximately 211,000 customers.[58]

---

[49] *See id.* para. 55; *see also* Fed. Comm. Comm'n, *FCC Plans $10 Million Fine for Carriers that Breached Consumer Privacy*, FCC (Oct. 24, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-330136A1.pdf [https://perma.cc/JN54-ASPD].

[50] *See* Brian Fung, *With a $10 Million Fine, the FCC Is Leaping into Data Security for the First Time*, WASH. POST (Oct. 24, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/24/with-a-10-million-fine-the-fcc-is-leaping-into-data-security-for-the-first-time/ [http://perma.cc/5GWF-32H2].

[51] *In re* AT&T Servs., Inc., Order and Consent Decree, 30 FCC Rcd. 2808 (2015) [hereinafter AT&T Order and Consent Decree].

[52] *See id.* para. 1.

[53] *See id.*

[54] *See id.*

[55] *See id.* para. 7.

[56] *See id.*

[57] *See id.* para. 8.

[58] *See id.* para. 11.

As in *TerraCom*, no CPNI was compromised in the AT&T incident.[59] But here again, the FCC based its investigation and enforcement action on the disclosure of "personal information."[60] AT&T consented to pay a record $25 million civil penalty and agreed to implement mandatory privacy-related compliance and monitoring procedures.[61]

TerraCom and *AT&T* represent an FCC trend to take enforcement actions to protect consumers' privacy and data security. In total, the FCC has taken five such major enforcement actions and imposed fines valued at over $50 million in the past year.[62] In May 2014, the FCC announced that it planned to fine Dialing Savings, LLC $2.9 million for violating rules that protect consumers from receiving harassing, intrusive, or unwanted robo-calls on their mobile devices.[63] In the same month, the FCC entered into a $7.5 million settlement agreement with Sprint to resolve an investigation into the company's failure to honor consumers' do-not call or do-not-text requests.[64] And in September 2014, the FCC reached a $7.4 million settlement agreement with Verizon to address allegations that the company marketed to two million customers without receiving their consent or notifying them of their privacy rights.[65]

In these recent enforcement actions, the FCC has carved out for itself a major consumer protection role by policing privacy violations. Though the FTC is the agency that usually comes to mind when one thinks of privacy and data security enforcement, the FCC's recent enforcement actions demonstrate the agency's willingness to scrutinize the privacy and security practices of compa-

---

59 *See id.* paras. 8, 11.

60 *Id.* paras. 1–2.

61 *See id.* para. 24.

62 *See* Fed. Comm. Comm'n, *AT&T to Pay $25 Million to Settle Consumer Privacy Investigation: FCC's Largest Data Security Enforcement Action*, FCC (Apr. 8, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-332911A1.pdf [https://perma.cc/Q489-PLWW].

63 *See In re* Dialing Services, LLC, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd. 5537 (2014).

64 *See In re* Sprint Corporation f/k/a Spring Nextel Corporation, Order, 29 FCC Rcd. 4759 (2014).

65 *See In re* Verizon Compliance with the Commission's Rules and Regulations Governing Customer Proprietary Network Information, Adopting Order, 29 FCC Rcd. 10303 (2014).

nies that fall within its jurisdiction. Though telecommunications companies are "accustomed to the high standards required for protecting CPNI," the FCC's aggressive approach in recent privacy and security enforcement decisions may have a transformative effect on all regulated entities, including the recently reclassified broadband Internet access service providers.[66]

II. THE FCC'S POST-NET NEUTRALITY APPROACH TO INTERNET PRIVACY

The FCC in its Open Internet Order continues this aggressive approach and as a result drastically alters the online privacy enforcement landscape. This Part dissects the Order's language addressing privacy, analyzes what the order neglects to say about privacy, and details these statements and omissions' overall effect on the Internet privacy enforcement landscape.

A. How Does the Order Address Privacy Enforcement?

In the Order, the FCC elects to not forbear from applying section 222's privacy protections to newly reclassified broadband Internet access service providers.[67] There, the FCC remarks that it "take[s] . . . seriously" section 222's mandate that every telecommunications carrier protect the confidentiality of its customers' private information.[68] The FCC points out that it "has long supported protecting the privacy of users of advanced services."[69] In a footnote, the Order notes that even "long before Congress enacted section 222," the FCC "recognized the need for privacy requirements associated with the provision of advanced services" and had accordingly adopted appropriate privacy requirements.[70] Against

---

[66] *See, e.g.*, Stout, *supra* note 39 (describing implications of an aggressive FCC privacy and security enforcement policy).

[67] 2015 Open Internet Order, *supra* note 1, para. 462.

[68] *Id.* para. 462 n.1381.

[69] *Id.* para. 463.

[70] *Id.* para. 463 n.1384 (quoting *In re* Appropriate Framework for Broadband Access to the Internet Over Wireline Facilities et al., Report and Order and Notice of Proposed Rulemaking, 20 FCC Rcd. 14853, para. 149 & n.447 (2005) [hereinafter Wireline Broadband Classification Order]).

this background, the Order asserts that retaining section 222 "thus is consistent with the [FCC's] general policy approach."[71]

Additionally, the FCC justifies its decision to not forbear from applying section 222 on the ground that forbearance would "not [be] in the public interest," as section 222 is "necessary for the protection of consumers."[72] The FCC emphasizes that "[c]onsumers' privacy needs are no less important when consumers communicate over and use broadband Internet access than when they rely on [telephone] services."[73] The FCC explains that because consumers rely on their broadband service providers as conduits for information exchange on the Internet, those providers are poised to obtain "vast amounts" of customers' private information.[74] Without appropriate safeguards, the FCC argues, broadband providers could use or disclose such information in manners "at odds with . . . customers' interests."[75]

According to the FCC, a lack of adequate privacy protections might cause consumers to be concerned about how broadband providers treat their private information.[76] This concern, the FCC believes, would result in consumers' refraining from making full use of broadband Internet access, which in turn would lower both demand for and adoption of broadband services.[77] Adequate privacy protections for customers' personal information, on the other hand, would spur demand for services and encourage broadband investment and deployment consistent with the FCC's goals.[78]

---

71 *Id.* para. 463.

72 *Id.* In these statements, the FCC references Communication Act section 10, which requires the agency to "forbear from applying any regulation or provision of the Communications Act to telecommunications carriers or . . . services if the [FCC] determines that [certain conditions are met]." *See* 47 U.S.C. § 160(a) (2012).

73 *See* 2015 Open Internet Order, *supra* note 1, para. 463 (citing Wireline Broadband Classification Order, *supra* note 70, para. 148).

74 *See id.*

75 *Id.*

76 *See id.* para. 464.

77 *Id.*

78 *Id.* (quoting *In re* Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd. 6927, para. 59 (2007)).

Before issuing the final Order, the FCC received and considered comments that opposed the application of section 222 to broadband Internet access service providers. In the Order, the FCC rejects these comments as being too general and lacking any "meaningful analysis" of how commenters' concerns over application of the section outweigh the FCC's privacy concerns.[79] Accordingly, the FCC concludes that applying section 222 is in the public interest.[80] In similar fashion, the FCC rejects arguments that the Communications Act's section 706—which requires the FCC to determine whether "advanced telecommunications capability . . . is being deployed to all Americans in a reasonable and timely fashion"[81]—provides adequate privacy protections to warrant section 222 forbearance.[82] The FCC notes that though section 706 would indeed apply even if the FCC had elected to forbear from applying section 222, the latter provides "a more certain foundation" for regulating broadband providers' privacy-implicating conduct.[83]

Though the FCC elected to not forbear from applying section 222 generally, it did elect to forbear from applying section 222's existing CPNI rules to broadband providers, insofar as those rules would be triggered by reclassification.[84] Because those rules are more applicable to "problems that historically arise regarding voice service," the FCC elects to forbear from applying those rules "pending further proceedings" to devise Internet-specific rules.[85]

---

79 *See id.*

80 *Id.*

81 47 U.S.C. § 706(a) (1996).

82 2015 Open Internet Order, *supra* note 1, para. 465. For an analysis of how section 706 might come into play despite reclassification, see Daniel T. Deacon, *Common Carrier Essentialism and the Emerging Common Law of Internet Regulation*, 67 ADMIN. L. REV. 133 (2015) (arguing that "the emergence of [s]ection 706 as a standalone basis for jurisdiction may push the FCC toward a more common-law, antitrust-like system of regulation than the command-and-control-style system with which it is historically most familiar").

83 *See* 2015 Open Internet Order, *supra* note 1, para. 465.

84 *Id.* para. 467.

85 *Id.* paras. 466–67. The Order leaves unclear when such proceedings might occur, or when the rules they spawn might take effect. On April 28, 2015, however, the FCC held a public workshop on consumer broadband privacy with the goals of "explor[ing] the [FCC's] role in protecting the privacy of consumers that use broadband Internet access service," "provid[ing] an opportunity for diverse stakeholders to explore a range of matters associate with the application of statutory privacy protections to broadband

B. What Does the Order Fail to Address?

The Order lacks reference to the FTC's traditional role as a privacy enforcer for online activity. Though the FCC describes how it has recently wielded its section 222 power to tackle privacy enforcement in *TerraCom*, it fails to draw a comparison or distinction between this power and the FTC's section 5 enforcement power.[86] The Order does not note how the reclassification of broadband Internet access service providers as common carriers affects the scope of the FTC's enforcement power.[87] Nor does the order address whether reclassification comes with any clear enforcement boundaries or limits for either agency.[88]

III. THE FCC'S INTERNET PRIVACY APPROACH DRASTICALLY ALTERS THE INTERNET PRIVACY ENFORCEMENT LANDSCAPE

By reclassifying broadband Internet access services as common carriers under Title II, the FCC alters the Internet privacy enforcement landscape. Applying section 222's privacy protection framework to broadband Internet access service providers subjects them to stronger privacy obligations than those to which they are accustomed. In this vein, it may prove costly for reclassified entities to comply with these suddenly-imposed duties, and this in turn may increase the risk that the FCC may take enforcement action against them. Finally, reclassification gives rise to jurisdictional challenges, as reclassification has the effect of shielding a significant group of business entities from the FTC's enforcement authority.

Internet access service," and "address[ing] whether and to what extent the [FCC] can apply a harmonized privacy framework across various services within [its] jurisdiction." *See Public Workshop on Broadband Consumer Privacy*, FCC (April 28, 2015, 10:00 AM), https://www.fcc.gov/events/wcb-and-cgb-public-workshop-broadband-consumer-privacy [https://perma.cc/6QZA-HGTV] [hereinafter *Public Workshop*].

86 *See* 2015 Open Internet Order, *supra* note 1, para. 53 n.48; *see also supra* notes 31–48 and accompanying text.

87 *See generally* 2015 Open Internet Order, *supra* note 1.

88 *See generally id.*

A. Expanded Privacy Obligations

In electing to not forbear from applying section 222 to broadband Internet service providers, the FCC expands that provision's strong privacy obligations to those providers. On May 20, 2015, the FCC released an enforcement advisory to remind reclassified entities that the Order "applies the core customer privacy protections of [s]ection 222," and that accordingly, they "shall only use, disclose, or permit access to individually identifiable customer proprietary network information" in the provision of services.[89] Consequently, as of June 12, 2015 (the net neutrality rules' effective date), broadband providers are obliged to comply with expanded requirements designed to more strongly protect consumer privacy and restrict customer data use.[90]

The FCC's enforcement advisory indicates that broadband Internet service providers should anticipate that their privacy and data protection programs will be subject to the agency's increased scrutiny.[91] Indeed, the enforcement advisory instructs broadband providers to take appropriate steps to protect their customers' privacy in accordance with section 222 until further rulemaking clarifies specifically how that section's provisions will apply to broadband Internet access service providers.[92] Until that rulemaking takes place, it is difficult to predict precisely how the agency will enforce those rules against providers.[93]

---

[89] FED. COMMC'NS COMM'N, ENFORCEMENT ADVISORY NO. 2015-03, ENFORCEMENT BUREAU GUIDANCE: BROADBAND PROVIDERS SHOULD TAKE REASONABLE, GOOD FAITH STEPS TO PROTECT CONSUMER PRIVACY (2015), https://apps.fcc.gov/edocs_public/attachmatch/DA-15-603A1.pdf [https://perma.cc/EM86-C2AN] [hereinafter ENFORCEMENT ADVISORY]; 47 U.S.C. § 222(c)(1) (2012).

[90] ENFORCEMENT ADVISORY, *supra* note 89; *see* 47 U.S.C. § 1302.

[91] *See* ENFORCEMENT ADVISORY, *supra* note 89.

[92] *Id.* at 2 ("[T]he [FCC's] Enforcement Bureau intends to focus on whether broadband providers are taking reasonable, good-faith steps to comply with [s]ection 222, rather than focusing on technical details. . . . [B]roadband providers should employ effective privacy protections in line with their privacy policies and core tenets of basic privacy protections.").

[93] *See* Michael Pryor, *FCC Has New Privacy Requirements for Broadband Providers*, LAW360 (Feb. 9, 2015), http://www.law360.com/articles/619408/fcc-has-new-privacy-requirements-for-broadband-providers [http://perma.cc/F6CX-R3J5]. Pryor suggests that perhaps Internet-specific section 222 rules will simply adapt the types of data protected in the Internet context. For example, perhaps the adapted rule will replace protections for data about the number of calls a customer makes with protections for

B. Higher Privacy Burdens and Increased Enforcement Risk

The necessity of complying with heightened privacy obligations increases the risk that broadband Internet access service providers will be the subject of FCC enforcement action. Before reclassification, the FCC set forth on an aggressive privacy enforcement path in *TerraCom* and *AT&T*.[94] In those cases, the FCC initiated enforcement actions based on claimed data breaches—which are not explicitly addressed by existing section 222 provisions[95]—and called on both section 222 and section 201(b) to support findings of culpability.[96] The Order affirms the FCC's plan to broadly construe and aggressively police broadband Internet service providers' extensive (yet undefined) privacy duties under those sections.[97] This has caused concern among entities who now must comply with those sections' requirements.

In a May 1, 2015 lawsuit challenging the Order filed by the American Cable Association and National Cable & Telecommunications Association, Internet service providers frequently refer to the extensive burden associated with complying with section 222.[98]

---

customers' bandwidth data; similarly, perhaps the rules will protect data about customer website visits instead of customers' call destinations.

94 *See infra* Part III.B. *See generally* 47 U.S.C. § 222.

95 *See infra* Part III.B.

96 *See, e.g.*, TerraCom Notice of Apparent Liability for Forfeiture, *supra* note 40, at 30; AT&T Order and Consent Decree, *supra* note 51, paras. 3–5.

97 *See* 2015 Open Internet Order, *supra* note 1, para. 462 n.1381 and accompanying text. *But see id.* at 5985–6000 (dissenting Statement of Commissioner Michael O'Rielly) (questioning the propriety of the FCC's aggressive approach). In public statements, FCC Enforcement Bureau Chief Travis LeBlanc has described his agency's privacy enforcement plan as a broad and aggressive one. *See, e.g.*, Joseph Jerome, *Travis LeBlanc on the FCC's New Privacy Role*, FUTURE OF PRIVACY FORUM (Dec. 11, 2014), http://www.futureofprivacy.org/2014/12/11/travis-leblanc-on-the-fccs-new-privacy-role/ [http://perma.cc/LC29-66FV]; Brendan Sasso, *The FCC's $365 Million Man*, NAT'L J. (Apr. 26, 2015), http://www.nationaljournal.com/tech/the-fcc-s-365-million-dollar-man-20150426 [http://perma.cc/XU39-24VW].

98 *See* Petition of Am. Cable Ass'n and Nat'l Cable & Telecomms. Ass'n for Stay Pending Judicial Review, Protecting and Promoting the Open Internet, GN Docket 14-28 (May 1, 2015), https://www.ncta.com/sites/prod/files/2015.05.01%20ACA_NCTA%20Motion%20for%20Stay.pdf [https://perma.cc/D52Y-GRCT] [hereinafter Petition for Stay] ("Petitioners' members would face extensive burdens to comply with [s]ection 222(c)(1), including the creation of processes to ensure that CPNI is not used in marketing without customer approval."). The 184-page petition mentions CPNI 137 times.

For example, Cox argues that applying existing CPNI rules to its broadband services will force the company to "evaluate its current processes for authenticating individuals who contact Cox via phone, online, or in retail locations to obtain [broadband Internet access service]-related customer data to determine whether it is protecting customer information using processes that specifically comply with the requirements of section 222."[99] Cox also argues that complying with section 222 will require the company to evaluate all of its contracts with vendors that interact with broadband Internet access service-related customer data to ensure that those contracts provide protections sufficient to satisfy section 222's requirements.[100] Mediacom, which has more than one million broadband customers, similarly argues that compliance with section 222 requires immediate action that risks "substantial" lost costs for the company.[101]

Small cable companies fear that burdens will fall heavily on them. The lawsuit also includes declarations from some small operators, many of whom face CPNI rules for the first time because they do not offer phone services.[102] Their arguments tend to follow a similar template and often use identical wording.[103] These statements, such as the declaration of William D. Bauer, CEO of WinDBreak Cable (a company with ten employees—three of whom are involved with the company's broadband Internet access service), focus on the "serious irreparable harms" the CPNI rules would have on the companies' "strong personal relationships with their customers."[104] Small providers also complain about the impending need to renegotiate contracts with partners in order to comply with section 222's stricter privacy rules, as well as the technical burdens (such as upgrading computer systems) asso-

---

[99] Declaration of Jennifer W. Hightower para. 7, *in* Petition for Stay, *supra* note 98.

[100] *See id.*

[101] Declaration of Thomas J. Larson para. 7, *in* Petition for Stay, *supra* note 98 ("Mediacom will have no choice but to implement new procedures to comply with [s]ection 222, including updating operating manuals, implementing necessary technical or software updates, and training its customer support staff. The substantial costs involved in taking these potentially unneeded steps cannot be recouped if the Order's reclassification is vacated.").

[102] *See generally* Petition for Stay, *supra* note 98.

[103] *See id.*

[104] Declaration of William D. Bauer para. 8, *in* Petition for Stay, *supra* note 98.

ciated with compliance.[105] Bagley Utilities argues that it, for example, "may have to renegotiate its contracts with [Momentum Telecom, a contractor that activates Bagley's customers' service and monitors Bagley's network for outages,] to ensure that CPNI is never used for marketing or sales purposes, and to ensure that Momentum Telecom takes necessary precautions to ensure the confidentiality of CPNI."[106]

Bagley, like others, further notes that if customer service suffers while companies' compliance processes are being upgraded, the companies will never be able to recover the lost customer goodwill.[107] The small providers express fear that "[a]ny misjudgment by [the companies] about the statute's requirements could have catastrophic consequences," including the possibility that the FCC might "impose large penalties—sometimes millions of dollars—for violations of [the] CPNI rules."[108]

So far, the FCC has yet to address the new privacy scheme's impact on small businesses; nevertheless, there remains the possibility that the FCC will take these companies' concerns into account when it reformulates broadband-specific CPNI in future rulemaking proceedings.

C. Jurisdictional Challenges

The FCC's decision to reclassify broadband Internet service providers as common carriers creates jurisdictional challenges. Before reclassification, the FTC could wield its section 5 enforcement authority to police broadband Internet service providers' privacy practices.[109] But as a result of reclassification, the FTC's power to

---

105 *Id.* para. 14.

106 Declaration of Michael Jensen para. 14, *in* Petition for Stay, *supra* note 98.

107 *Id.* para. 18.

108 Declaration of William D. Bauer para. 25, *in* Petition for Stay, *supra* note 98.

109 *See supra* Part I.A. Under sections 5(a) and 13(b) of the FTC Act, 15 U.S.C. §§ 45(a) & 53(b), "the FTC may proceed against unfair practices even if those practices [also] violate some other statute . . . ." FTC v. Accusearch, Inc., 570 F.3d 1187, 1195 (10th Cir. 2009) (referring to a provision of the Telecommunications Act); *see also* FTC v. T-Mobile USA, Inc., No. 2:14-cv-00967 (W.D. Wa. July 1, 2014) (exemplifying action against common carrier for deceptive and unfair practices in violation of the FTC Act resulting from T-Mobile's placing third-party charges on telephone bills); FED. TRADE COMM'N, BROADBAND CONNECTIVITY COMPETITION POLICY 38–41 (2007), https://www.ftc.gov/sites/default/files/documents/reports/broadband-connectivity-competition-

bring privacy enforcement actions against broadband providers is significantly reduced, as the FTC Act's common carrier exemption bars the FTC from policing so-classified entities when they engage in common carriage services.[110] Representatives from the FTC have spoken out against reclassification because of this effect.[111] Accordingly, there is a need for courts, Congress, or the agencies themselves to determine whether and how privacy enforcement responsibilities should be assigned.

1. The Common Carrier Exception

Per the FTC Act, the FTC lacks authority over "common carriers."[112] Under the Act, the FTC is empowered to wield its authority to prevent commercial entities, "except [for] . . . banks . . . common carriers . . . air carriers . . . [and others] . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[113]

Courts have long recognized that the FTC Act's exceptions are "binding and unalterable."[114] As far back as 1920, the court in *T.C. Hurst & Son v. FTC*[115] described the FTC's lack of authority to regulate common carriers under the FTC Act.[116] In *Hurst*, the court reviewed the express language of the Act and concluded that "[b]anks and common carriers [are] doubtless excepted from the act."[117] In 1962, the Supreme Court affirmed this conclusion in the antitrust case *United States v. Philadelphia National Bank*,.[118] and

---

policy/v070000report.pdf [https://perma.cc/BWY4-3BP4] [hereinafter BROADBAND CONNECTIVITY COMPETITION POLICY] (analyzing the application of section 5 of the FTC Act to broadband services).

110 15 U.S.C. § 45(a) (2006).

111 BROADBAND CONNECTIVITY COMPETITION POLICY, *supra* note 109, at 41.

112 38 Stat. 717, §§ 5–6 (1914) (codified as amended at 15 U.S.C. §§ 45(a)(2), 46(a), 46(b) (1994 & Supp. 1998)).

113 15 U.S.C. § 45(a)(2).

114 Harold Furchtgott-Roth & Bryan Tramont, *Commission on the Verge of a Jurisdictional Breakdown: The FCC and Its Quest to Regulate Advertising*, 8 COMMLAW CONSPECTUS 219, 223 (2000).

115 268 F. 874 (E.D. Va. 1920).

116 *See id.*

117 *Id.* at 877.

118 374 U.S. 321 (1962).

held that the FTC's authority is limited by the FTC Act's exceptions.[119]

Cases specifically involving common carriers similarly confirm the FTC's lack of enforcement authority over them. For example, in *FTC v. Miller*,[120] the court held that the FTC lacked authority to enforce a subpoena against a common carrier due to the statutory exception.[121] In that case, the FTC attempted to investigate whether an interstate motor home carrier engaged in unlawful advertising practices, and as part of the investigation, the FTC subpoenaed some of the company's records.[122] The company cited the common carrier exception as a defense to oppose the subpoenas, and the FTC sought enforcement in district court.[123] In overturning a district court ruling, the Sixth Circuit cited the common carrier exemption and dismissed the FTC's argument that advertising by common carriers is a non-common carrier activity falling within FTC control.[124] In so holding, the court confirmed that the common carrier exception is one of a number of "carve outs" in FTC authority.[125]

2. FTC Has Been Outspoken Against the Order's Effect On Its Enforcement Authority

The FTC has expressed discontent that reclassification of broadband Internet access service providers as Title II common carriers exempts those entities from its enforcement reach when they engage in common carriage services.[126] Indeed, FTC repre-

---

[119] *See id.* at 336 n.11.

[120] 549 F.2d 452 (7th Cir. 1977).

[121] *See id.* at 461.

[122] *Id.* at 454.

[123] *See id.*

[124] *See id.* at 455–58 (noting that "[t]he regulatory approach articulated by the [FTC], while it may be a desirable one, is not the one Congress appears to have adopted").

[125] *See id.* at 459 ("Congress' recognition of a regulatory gap with respect to banks is implicitly a recognition of such a gap with respect to common carriers as well.").

[126] Although section 5 exempts enforcement against "common carrier" activities, this exemption does not apply to common carriers' provision of other, non-common carriage services. *See* 15 U.S.C. §§ 44, 45(a)(2) (2006); *see also* FTC v. Verity Int'l, Ltd., 443 F.3d 48, 58–60 & n.4 (2d Cir. 2006) (citing, inter alia, Sw. Bell Tel. Co. v. FCC, 19 F.3d 1475, 1481 (D.C. Cir. 1994) and Nat'l Ass'n of Reg. Util. Comm'rs v. FCC, 533 F.2d 601, 608 (D.C. Cir. 1976)).

sentatives have been publicly outspoken against this result. In the press, FTC Commissioner Maureen Ohlhaussen has made reclassification's effect clear: "If an entity is a common carrier providing common carrier services, [the FTC] can't bring actions against them."[127] Other officials have been more harsh. In a statement before the House of Representatives Committee on the Judiciary titled *Wrecking the Internet to Save It? The FCC's Net Neutrality Rule*, FTC Commissioner Joshua D. Wright cites the FTC's "expertise" and "vigor[ ]" in protecting privacy to argue that reclassification results in "obstacles to protecting consumers . . . by depriving the FTC of its long-standing jurisdiction in [the] area" and "threaten[s] the robust consumer protection efforts that the agency has engaged in over the last two decades."[128] Jessica Rich, director of the FTC's Bureau of Consumer Protection, laments that the FCC's decision "takes an experienced cop off the beat in this important area."[129]

Despite the FTC's opinion to the contrary, some advocates for reclassification view the FCC's newly broadened oversight of Internet service providers as a win for consumers.[130] These proponents posit that the FCC's enforcement approach will benefit consumers more than the FTC's approach does.[131] Though the FTC issues guidance and other notices to inform consumers and indus-

---

[127] *See* Brian Fung, *How to End a Fight Over Who Should Regulate Internet Providers*, WASH. POST (Mar. 26, 2015), http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/26/could-the-ftcs-inability-to-regulate-internet-providers-come-to-an-end/ [https://perma.cc/X5CD-NMGC].

[128] *Wrecking The Internet To Save It? The FCC's Net Neutrality Rule: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 43–44 (2015) (statement of Joshua D. Wright, Commissioner, FTC), www.judiciary.house.gov/index.cfm?a=Files.Serve&File_id=6624EC59-DB2B-45B3-9615-0E689F4CBF37 [http://perma.cc/9VUJ-TLZU] [hereinafter *Wrecking the Internet*].

[129] Brendan Sasso, *Net Neutrality Has Sparked an Interagency Squabble Over Internet Privacy*, NAT'L J. (Mar. 9, 2015), http://www.nationaljournal.com/tech/the-future-of-broadband/net-neutrality-has-sparked-an-interagency-squabble-over-internet-privacy-20150309 [http://perma.cc/L7YN-ZKC4].

[130] *See* Andrea Peterson, *The FCC's Net Neutrality Decision Could Mean Stronger Privacy Rules for Internet Service Providers*, WASH. POST (Feb. 27, 2015), http://www.washingtonpost.com/blogs/the-switch/wp/2015/02/27/the-fccs-net-neutrality-decision-could-mean-stronger-privacy-rules-for-internet-service-providers/ [https://perma.cc/K8CA-4QEM].

[131] *Id.*

try about which practices might trigger enforcement, the agency's enforcement is mostly reactive: that is, it often must wait for a company to engage in a practice that the agency considers unfair or deceptive before initiating investigatory or enforcement action.[132] In the privacy context, this usually involves holding companies to their own broadly defined privacy policies and punishing companies for policy breaches that may occur.[133]

The FCC, on the other hand, has broad rule-making authority that empowers the agency to "set standards that companies will have to abide by before the troubling practices have even taken place."[134] According to Harold Feld, Senior Vice President of Public Knowledge, "[t]he FCC's privacy regulations have worked very well, which is why so many people are unaware of them—because they are so rigid about enforcing them, people don't even have to think about it."[135] So far, the agency has proven to be an aggressive enforcer of current privacy rules as they apply telephone providers.[136] By using its leverage, it is argued, the FCC might be able to take control over some controversial online practices—such as the use of "supercookies"[137]—more effectively than could the FTC.[138]

Proponents also note that despite reclassification, the FTC is not completely barred from regulating online privacy, as the net neutrality rules not foreclose the FTC's ability to police troublesome privacy practices committed by non-common carrier Internet services and websites.[139] Just as the FTC can investigate and bring enforcement actions against telemarketers (even though they

---

132 *See supra* Part I.A.

133 *See generally* Solove & Hartzog, *supra* note 28; *see also* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 (2003).

134 Peterson, *supra* note 130.

135 *Id.*

136 *See, e.g.*, *supra* notes 38–65 and accompanying text.

137 "Supercookies" are persistent unique identifiers that some mobile broadband providers have been inserting onto their customers' devices that allow tracking companies to follow the customers' activity even if they have deleted or disabled cookies. *See* Natasha Singer & Brian X. Chen, *Verizon's Mobile "Supercookies" Seen as Threat to Privacy*, N.Y. TIMES (Jan. 25, 2015), http://www.nytimes.com/2015/01/26/technology/verizons-mobile-supercookies-seen-as-threat-to-privacy.html [http://perma.cc/ZNP6-AVRY].

138 *See* Peterson, *supra* note 130.

139 *See id.*

communicate using phone lines), the FTC will also be able to investigate and bring enforcement actions against Internet services, rather than the carriers of those services.[140] Indeed, actions against services rather than carriers themselves make up the bulk of the FTC's online enforcement to date.[141]

3. What Explains the Interagency Tension Here?

Given the FTC's still-prominent privacy enforcement role even after reclassification, it is somewhat curious that the agency has expressed such discontent at its having a broad swath of companies removed from its enforcement scope. Why is the FTC so sensitive about having its privacy jurisdiction limited in this way?

FTC Commissioner Ohlhaussen has cited consumer protectionism as the primary reason for the FTC's unease with reclassification.[142] She publicly noted that her concern "is really not so much for the FTC, but for the loss to consumers—that they would lose out from having the FTC's active oversight."[143]

In a recent *Forbes* article, former FCC Wireless Bureau Chief Fred Campbell expounds on what such "loss" might entail.[144] He bases his analysis on the recent merger between Verizon and AOL.[145] Through this merger, Verizon hopes to harness AOL's targeted advertising capabilities so that Verizon can expand into the advertising market as the mobile market slows.[146] While the

---

[140] *See id.* ("The FCC will oversee the pipes, while the FTC will be able to wield their enforcement tools against those who operate services that use the pipes.").

[141] *See* Joel R. Reidenberg et al., *Privacy Enforcement Actions*, FORDHAM CTR. ON LAW INFO. POL'Y (June 24, 2014), www.law.fordham.edu/assets/CLIP/CLIP_Privacy_Case_Report_-_FINAL.pdf [http://perma.cc/H8LZ-E8NR] (presenting an "objective and comprehensive survey of the online privacy issues litigated in FTC enforcement actions").

[142] *See* Fung, *supra* note 127.

[143] *See id.*

[144] *See generally* Fred Campbell, *Privacy Concerns About Verizon-AOL Deal Are Really Concerns About Increased Competition*, FORBES (May 18, 2015), http://www.forbes.com/sites/realspin/2015/05/18/privacy-concerns-about-verizon-aol-deal-are-really-concerns-about-increased-competition/ [http://perma.cc/44LA-6XKP].

[145] *See* Clarie Groden, *Verizon Now Officially Owns AOL*, TIME (June 23, 2015), http://time.com/3931793/verizon-now-officially-owns-aol/ [http://perma.cc/DX9H-UV9M].

[146] *See* Kevin Fitchard, *The Real Reason Verizon Bought AOL*, FORTUNE (June 24, 2015), http://fortune.com/2015/06/24/verizon-gains-aol/ [http://perma.cc/S53S-RLHR]

deal is generally viewed as raising no novel privacy issues, some groups oppose it on the basis that the new entity's power to deliver targeted advertising, as well as the substantial data collection that will be required to do so, seriously endangers consumer privacy.[147] This, according to the deal's opponents, should oblige the FCC to "move quickly" to impose strong privacy requirements for broadband Internet access service providers.[148]

However, Campbell argues that opponents' urging that the FCC "interfere[ ]" in Internet privacy amounts to a tactic to help edge providers such as Google and Facebook stave off competition in the advertising market:

> Verizon's [purchase of] AOL for $4.4 billion should be no big deal for regulators. The [FCC] already announced that it won't review the deal and there is no reason to think antitrust regulators will raise concerns. But that hasn't stopped Silicon Valley's advertising giants from attempting to leverage the deal into new regulations that would help them tighten their grip on Internet advertising markets. It's understandable that Internet advertising's market leaders are worried about the deal's potential to increase competition for lucrative ad dollars in mobile and over-the-top markets. Google and Facebook dominate mobile advertising and would undoubtedly like to keep it that way. Though they have little to fear from AOL today, a Verizon-AOL combo would be a credible competitive threat to their monopolistic ambitions. That's why their friends in Washington want the FCC to start interfering in Internet

("From Verizon's standpoint, it needs to find something it can sell via its available networks . . . . That's where AOL comes in[:] . . . it [ ] has put together a sophisticated suite of advertising technologies for online and traditional media that no other company (aside from Google and Facebook) can match.").

147 *See* Shiva Stella, *Public Knowledge Urges FCC to Issue NPRM to Protect Consumer Privacy*, PUB. KNOWLEDGE (May 12, 2015), https://www.publicknowledge.org/press-release/public-knowledge-urges-fcc-to-issue-nprm-to-protect-consumer-privacy [https://perma.cc/MVR9-KP8Q] (citing Senior Vice President Harold Feld, who argues that the deal "raises extremely substantial and urgent privacy concerns").

148 *Id.*

> privacy issues. [The FCC enforcing] new rules prohibiting Internet service providers from tracking consumers online would keep Verizon out of their markets and could have the effect of killing the deal even if antitrust regulators approve it.[149]

Campbell raises a few arguments to support his position. First, he echoes the idea that the Verizon-AOL merger does not raise any novel privacy issues, as Google and Facebook already derive substantial benefit—tens of millions of dollars per year—from targeted advertising empowered by data collection.[150] Moreover, the groups opposing the merger "don't seem to care" about Google and Facebook's data collection practices: they asked the FCC to regulate only Verizon and other ISPs, and not Google or Facebook.[151]

Second, he argues that if opponents were genuinely concerned with consumer privacy, they would have appealed to the FTC instead of the FCC, as the former's enforcement history is much more substantial than the latter's.[152] For example, while the FTC fined Google $22.5 million for misrepresenting its use of cookies in August 2012,[153] the FCC in that same year fined Google a mere $25,000 for its unauthorized collection of highly sensitive consumer Wi-Fi data in relation to its Street View project—even though Google was determined to have had "deliberately impeded and delayed" the FCC's investigation.[154]

Third, Campbell argues that the structure of the net neutrality rules is designed to have a competition-inhibiting effect.[155] Though the FCC could have adopted net neutrality rules that would not

---

[149] *Id.*; *see also* Fitchard, *supra* note 146.

[150] *See* Campbell, *supra* note 144.

[151] *Id.* And not coincidentally, the same groups that oppose the merger advocated that the FCC assume jurisdiction over Internet privacy during the net neutrality debate. *See id.*. *But see supra* note 129 and accompanying text (highlighting the remarks of a Public Knowledge official supportive of the FCC's new privacy reach).

[152] *See* Campbell, *supra* note 144.

[153] *See* Fed. Trade Comm'n, *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, FTC (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented [https://perma.cc/VLK6-EZXT].

[154] *See In re* Google, Inc., Notice of Apparent Liability for Forfeiture, 27 FCC Rcd. 4012, para. 4 (2012); *see also* Campbell, *supra* note 144.

[155] *See* Campbell, *supra* note 144.

have encroached upon the FTC's privacy jurisdiction over Internet service providers, the FCC instead opted to apply "an outdated privacy statute designed for telephone services" that excludes the FTC from governing them.[156] Campbell asserts that "[n]o one should be surprised that Google and Facebook are now attempting to entrench their dominance over Internet advertising by arbitraging this new jurisdictional split over online privacy," and that "[t]he jurisdictional split created by the net neutrality order enables . . . discriminatory result while maintaining a false veneer of consumer protection."[157]

Campbell's theory is subject to criticism. Though he suggests that some edge providers such as Google and Facebook are bedfellows with the FCC, the agency might yet regulate those providers. Professor Daniel Deacon argues that Communications Act section 706, as interpreted by courts, gives the FCC a potentially broad power to regulate services that fall without its core jurisdiction over common carriers.[158]

Section 706(a) of the Communications Act directs the FCC to:

> [E]ncourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans . . . by utilizing, in a manner consistent with the public interest, convenience, and necessity, price cap regulation, regulatory forbearance, measures that promote competition in the local telecommunications market, or other regulating methods that remove barriers to infrastructure investment.[159]

Similarly, section 706(b) requires the FCC to conduct an annual inquiry "concerning the availability of advanced telecommunications capability to all Americans," and, if it finds that such availability is lacking, to "take immediate action to accelerate deployment of such capability by removing barriers to infrastructure

---

156 *See id.*
157 *Id.*
158 *See generally* Deacon, *supra* note 82.
159 47 U.S.C. § 1302(a) (2002).

investment and by promoting competition in the telecommunications market."[160]

The FCC relied on section 706—a non-Title II basis—as justification for the no-blocking and nondiscrimination net neutrality rules it proposed in its 2010 Open Internet Order.[161] There, the FCC explained that the rules in that Order promoted the policies outlined in section 706 because they supported "virtuous cycle of innovation."[162] Upon a challenge to this Order, the D.C. Circuit determined that the FCC's conclusion that section 706(a) "constitutes an affirmative grant of regulatory authority" was a reasonable one.[163] Additionally, the court upheld the FCC's determination that section 706(b) "empower[ed] it to take steps to accelerate broadband deployment if and when it determines that such deployment is not reasonable and timely."[164] And both sections, the court concluded, authorize the FCC to directly regulate broadband providers (instead of merely to promote infrastructure deployment via other means).[165] Although it agreed with the FCC's jurisdictional arguments, the D.C. Circuit in the end vacated the Order's no-blocking and nondiscrimination rules.[166] Nevertheless, the court's decision is significant to the extent that it affirmed the FCC's section 706 authority to regulate companies—namely, broadband Internet access providers—that were the same as, or closely allied with, those telephone and cable operators the FCC has traditionally regulated.[167]

According to Professor Deacon, this decision contributes to the FCC having "a malleable and potentially broad jurisdiction over Internet Protocol-based networks and services."[168] He notes that

---

160 *Id.* § 1302(b).

161 *See In re* Preserving the Open Internet, Report and Order, 25 FCC Rcd. 17905, para. 1 (2010) [hereinafter 2010 Open Internet Order].

162 *See id.* para. 123. Under the "virtuous cycle," "new uses of the [broadband] network—including new content, applications, services, and devices—lead to increased end-user demand for broadband, which drives network improvements, which in turn lead to further innovative network uses." *Id.* para. 14.

163 Verizon v. FCC, 740 F.3d 623, 637–40 (D.C. Cir. 2014).

164 *Id.* at 641 (internal quotations omitted).

165 *See id.* at 643.

166 *See id.* at 650–59.

167 *See* 2010 Open Internet Order, *supra* note 161, para. 49.

168 Deacon, *supra* note 82, at 134.

"there is nothing inherent in the nature of [section] 706 that would limit the reach of that section to those particular providers."[169] Consequently, Deacon argues, the FCC could cite the section's potentially expansive authority to regulate entities that fall outside the FCC's traditional jurisdictional bounds.[170] To exemplify his theory, Professor Deacon builds a hypothetical involving Google and Facebook that could be read as a direct response to former Wireless Bureau Chief Campbell's argument:

> Take, as the most prominent example, edge providers such as Google or Facebook. The Open Internet Order regulated broadband Internet access providers in order to promote innovation by edge providers. But there is no reason that FCC could not use its [section] 706 power instead to regulate edge providers directly, at least as long as it could tell a credible story regarding why such regulation enabled innovation at the edge (in turn spurring consumer demand for broadband and, with it, broadband infrastructure deployment, under the "virtuous cycle" theory).[171]

Professor Deacon further argues that such a prospect is "not fanciful."[172] He considers a case from 2012 in which the FTC investigated Google over allegations that the company manipulated search results to favor its own services.[173] Professor Deacon explains that the issue in that case was "conceptually similar" to issues in the net neutrality dispute, and that in such cases, the FCC may find intervention to be appropriate.[174]

Given Professor Deacon's argument, it may be difficult to rationalize Mr. Campbell's theory that reclassification and strong privacy rules for broadband Internet providers suggest an attempt

---

169 *Id.* at 173.

170 *See id.*

171 *Id.*

172 *See id.* at 173–74.

173 *See id.* at 174; *see also* Steve Lohr, *Drafting Antitrust Case, F.T.C. Raises Pressure on Google*, N.Y. TIMES (Oct. 12, 2012), http://www.nytimes.com/2012/10/13/technology/ftc-staff-prepares-antitrust-case-against-google-over-search.html [http://perma.cc/F9ZS-UZ8Y].

174 *See* Deacon, *supra* note 82, at 174.

to promote anticompetitive behavior, and that this has stirred the FTC's ire. Though Deacon's argument does not necessarily defeat Campbell's, it posits a theory that potentially weakens it. If anything, the combination of theories raises more questions than it does provide answers about the true reasons for the FTC's discontent with the FCC's decision making. But whether or not we have a full explanation, a tension remains between the two agencies. How might it be resolved?

IV. POSSIBILITIES FOR RESOLVING THE INTERAGENCY TENSION

Despite differences between the agencies, the possibility for a robust and effective Internet privacy enforcement regime persists. For example, new privacy rules for broadband Internet service providers might delineate enforcement responsibilities between the FCC and the FTC, while clarifying industry's obligations and consumers' expectations under the new enforcement regime. Alternatively, congressional action could remove the statutory bar that prohibits the FTC from enforcing against common carriers. Alternatively, or in addition to a repeal of the common carrier exception, the FCC and FTC could share cooperative privacy enforcement authority, as they share authority in other non-privacy areas. In this Part, I explore these possibilities.

A. New Rules

New CPNI rules, as devised through rulemaking proceeding, will clarify how section 222 applies to broadband Internet access service provider. Unlike the Order, these rules could address and suggest a remedy for the FCC's capture of the FTC's authority to police providers' privacy practices.

The FCC states in its Order that rulemaking proceedings to this end will take place, but it leaves unclear when such proceedings might occur, or when the rules they produce might take effect.[175] However, in a late June 2015 speech, FCC Chairman Tom

---

[175] *See* 2015 Open Internet Order, *supra* note 1, para. 467.

Wheeler confirmed that the agency would commence privacy rulemaking in the fall of that year.[176]

In April 28, 2015, the FCC hosted a public workshop on consumer broadband privacy that could potentially provide a preview of how Internet-specific rules might appear.[177] The FCC's purposes for hosting the event were to "explore the [FCC's] role in protecting the privacy of consumers that use broadband Internet access service," "provide an opportunity for diverse stakeholders to explore a range of matters associated with the application of statutory privacy protections to broadband Internet access service," and "address whether and to what extent the [FCC] can apply a harmonized privacy framework across various services within [its] jurisdiction."[178]

Members of the workshop's second panel discussed section 222's application to broadband Internet access services.[179] Panelists agreed that this application is complicated;[180] some panelists debated about the extent to which section 222 is suitable to accommodate a privacy framework for Internet service providers, as well as the extent to which it is appropriate for the FCC to impose an obligation to protect "proprietary information" in the Internet context.[181] Similarly, the panelists grappled with how to best define "customer proprietary network information" in that context.[182]

One panelist argued that anti-fraud, cybersecurity, and research-enabling principles should guide the FCC's revised applica-

---

176 *See* Mario Trujillo, *FCC to Start Work on Broadband Privacy in Fall*, HILL (June 26, 2015), http://thehill.com/policy/technology/246259-fcc-to-start-work-on-broadband-privacy-in-fall [http://perma.cc/V3MX-TVPV].

177 *See Public Workshop*, *supra* note 85.

178 *Id.*

179 *See id.*; *see also* Morgan Kennedy, *FCC's Broadband Consumer Privacy Public Workshop*, NAT'L L. REV. (May 5, 2015), http://www.natlawreview.com/article/fcc-s-broadband-consumer-privacy-public-workshop [http://perma.cc/X6UV-8WB5] (summarizing the workshop's discussions).

180 *See* Kennedy, *supra* note 179.

181 *See id.*

182 Panelist Jim Halpert of DLA Piper argued that many of section 222's provisions do not apply smoothly to ISPs, and noted that "personally identifiable information" is not part of section 222's definition of CPNI. *See id.* Similarly, panelist Nancy Libin of Wilkinson Barker Knauer cautioned against defining CPNI too broadly. *See id.*

tion of section 222.[183] Another panelist argued that the FCC should mimic the FTC's approach and issue guidance documents and hold workshops that provide standards and encourage strong privacy practices so that industry can keep step with a rapidly evolving landscape.[184] Some panelists similarly argued that the FCC should adopt an FTC-like set of criteria so one set of rules fulfills both consumer and industry expectations.[185]

Later, in a May 2015 web conference organized by the International Association of Privacy Professionals, FCC Wireline Competition Bureau Deputy Chief Matthew DelNero stated that the agency is looking to gather "creative" input from stakeholders about how to best integrate its broadened privacy authority within existing enforcement regimes.[186] DelNero stressed that the agency is "really very much in an information-gathering mode and [is] really trying to hear from all the different stakeholders about what the important areas are."[187] He noted that though "[t]he [April] workshop was a good start, [the agency's] doors are very much open, and [the FCC] hope[s] that the workshop gets people thinking good and creative thoughts about where [it] go[es] from here."[188]

According to DelNero, FCC Commissioner Tom Wheeler and his colleagues have taken care to point out that the April workshop was only the "beginning of a process," and that the FCC intends to take a "careful and deliberative approach" toward privacy.[189] As part of this approach, the FCC will likely implement further informal steps for hearing stakeholder input before official rulemaking begins.[190]

During the web conference, DelNero noted that some stakeholders have expressed a preference for rules that create a harmo-

---

183 *See id.*
184 *See id.*
185 *See id.*
186 *See* Allison Grande, *FCC Approaching Privacy Rules Cautiously, Official Says*, LAW360 (May 7, 2015), http://www.law360.com/articles/653163/fcc-approaching-privacy-rules-cautiously-official-says [http://perma.cc/F72W-H7G8].
187 *Id.*
188 *Id.*
189 *Id.*
190 *See id.*

nized enforcement approach.[191] For example, fellow panelist Debbie Matties, Vice President of iPrivacy CTIA, argued that the FCC must find a way to regulate privacy in a manner that does not intrude upon existing regulations or active regulators, including the FTC.[192] This, DelNero concludes, suggests that "maybe broadband providers are less concerned with uncertainty per se and more concerned that when [the FCC] does rulemaking, it keeps in mind the broader ecosystem and how [s]ection 222 interacts with other statutory authorities."[193]

Though new rules would likely clarify industry's privacy obligations and give consumers a clear framework for their privacy expectations with respect to how broadband providers handle their information, it is yet unclear whether or how such rules might respond to FTC and stakeholders' concerns about privacy enforcement. Though DelNero's statements suggest that the FCC may consider these concerns during its rulemaking process, it is unclear whether such is likely to occur. If rulemaking fails to supply a resolution, means other than formal rulemaking might be more effective for loosening the interagency tension.

B. Repeal of the Common Carrier Exception

As an alternative to, or as an addition to new CPNI rules, Congress might repeal the common carrier exception to eliminate the bar that keeps the FTC from regulating common carriers. Some stakeholders have called on Congress to do just that.[194] According to FTC Chairwoman Edith Ramirez, the common carrier exception is "outdated" and unnecessarily shackles the FTC's ability to protect consumers.[195]

---

191 *See id.*

192 *See id.*

193 *Id.*

194 *See Ramirez Urges Repeal of Common Carrier Exemption*, FTC:WATCH (Feb. 13, 2015), http://www.ftcwatch.com/ramirez-urges-repeal-of-common-carrier-exemption/ [http://perma.cc/YW84-2G94] (subscription required); *see also* Letter from Mike Ananny, et. al to FTC Commissioners (Jan. 29, 2015), http://www.pijip.org/wp-content/uploads/2015/01/Net-Neutrality-Prof-Letter-01292015.pdf [http://perma.cc/Q762-LJNX].

195 *See Ramirez Urges Repeal of Common Carrier Exemption*, *supra* note 194. In 2003, then-FTC Chairman Timothy Muris similarly argued that the exemption "dates from a period when telecommunications services were provided by government-authorized,

Recently, officials from both agencies have endorsed the idea of eliminating the common carrier exception.[196] In a March 2015 House Judiciary Committee hearing, FCC Chairman Tom Wheeler said that "[the] idea is definitely worthy of review," and that "[the FCC] should work in tandem with the FTC."[197] He further noted that the partnership would amount to "a great one-two punch."[198] FTC Commissioner Terrell McSweeny echoed this sentiment, arguing that because "[t]here are slightly different tools in the FCC toolbox and in the FTC toolbox," she supports repeal.[199]

If the common carrier exception is successfully repealed, the agencies would have wider authority to police consumer harms, as the resulting legal landscape would empower both the FTC and the FCC to regulate common carriers whose activities warrant investigation and enforcement. A repeal of the common carrier exception would likely lead to greater cooperation between the two agencies.[200]

C. Co-Governance

In 2003, Professor Christopher Yoo wrote that "technological convergence" would require a farewell bid to the days in which varying communications services in use could "occupy[ ] a separate regulatory silo."[201] He suggested that "the ultimate destiny . . . that the various communications platforms will serve as complements, rather than substitutes . . . raises the possibility that new types of regulation that would allow the sharing of each network might have to be created."[202]

---

highly regulated monopolies." Fed. Trade Comm'n, *FTC Commissioners Testify on Agency's Reauthorization Request*, FTC (June 11, 2003), https://www.ftc.gov/news-events/press-releases/2003/06/ftc-commissioners-testify-agencys-reauthorization-request [https://perma.cc/LM6N-HGN9].

196 *See* Fung, *supra* note 127.

197 *Wrecking The Internet*, *supra* note 128, at 89.

198 *Id.*

199 *Id.* at 77.

200 *See infra* Part IV.C.

201 *See* Christopher S. Yoo, *New Models of Regulation and Interagency Governance*, 2003 MICH. ST. DCL L. REV. 701, 714 (2003).

202 *Id.* at 715.

In modern times, this "new type of regulation" may be co-governance. Co-governance regulatory regimes already in place suggest that the FCC and FTC might adopt a similar regime for online privacy governance. As it stands, each agency participates in co-governance schemes already, both with other agencies and with each other.

1. FTC and FCC Co-Governance with Other Agencies

Both the FTC and the FCC already engage in complementary co-governance schemes with other government agencies. For example, the FTC along with the Food and Drug Administration ("FDA") and U.S. Department of Agriculture ("USDA") regulate food labeling. Similarly, both the FTC and the FCC join forces with the U.S. Department of Justice ("DOJ") to enforce against anticompetitive behavior by reviewing mergers and acquisitions.

a) Food Labeling (FTC/FDA/USDA)

The FTC, FDA, and USDA share jurisdiction over claims that food manufacturers make about their products pursuant to a complementary statutory scheme. In this context, the FTC relies on section 5 of the FTC Act to police "unfair or deceptive acts or practices" and sections 12 and 15 of the Act prohibit "any false advertisement" that is "misleading in a material respect."[203] Similarly, the FDA derives its authority in this context from the Federal Food, Drug, and Cosmetic Act section 403(a), which prohibits "labeling [that] is false or misleading in any particular."[204] The USDA authority stems from the Federal Meat Inspection Act, which prohibits labeling of meat or meat products that is "false or misleading in any particular,"[205] and the Poultry Products Inspection Act, which prohibits labeling of poultry products that is "false or misleading in any particular."[206]

---

[203] 15 U.S.C. §§ 45, 52, 55 (1980).
[204] 21 U.S.C. § 343(a) (2010).
[205] *Id.* § 601(n)(1) (2015).
[206] *Id.* § 453(h)(1).

Since 1954, the FTC and the FDA have cooperated under a Memorandum of Understanding.[207] Under this agreement, the FTC regulates food advertising, while the FDA regulates food labeling.[208] In addition, the agreement affirms the agencies' shared commitment to: (1) prevent public deception; (2) coordinate their work to eliminate duplicative effort; and (3) promote consistency in handling matters of mutual concern.[209]

b) Anticompetitive Behavior (FTC/DOJ)

Both the FTC and the DOJ Antitrust Division enforce federal antitrust laws.[210] While they share some overlapping jurisdiction, in practice the two agencies' efforts complement one another by relying on their expertise in different markets.[211] For example, the FTC often regulates in economic spaces that involve high consumer spending, such as health care, pharmaceuticals, professional services, food, energy, and technology.[212] Before either agency begins an investigation, it consults with the other to avoid duplicative enforcement of the same transaction; this way, each agency may conserve staff resources and avoid placing the same party in a form of double jeopardy.[213]

---

[207] *See* Working Agreement Between FTC and Food and Drug Administration, 4 Trade Reg. Rep. (CCH) ¶ 9,850.01 (1971).

[208] *See id.*

[209] *See id.* ¶¶ 9,850.01–.02.

[210] *See The Enforcers*, FTC (June 26, 2015), https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/enforcers [https://perma.cc/HBY8-PB9J] [hereinafter *The Enforcers*].

[211] *Id.*; *see also Mission*, DEP'T JUST., http://www.justice.gov/atr/about/mission.html [http://perma.cc/9HQE-6VVP] (last updated July 20, 2015). Under the FTC/DOJ Hart-Scott-Rodino Premerger Program, FTC and DOJ merger review is formalized: this "clearance process" gives the agencies a nine-day window to decide which, based on its expertise, will review a particular merger. *See* James R. Weiss & Martin L. Stern, *Serving Two Masters: Dual Jurisdiction of the FCC and the Justice Department Over Telecommunications Transactions*, 6 COMMLAW CONSPECTUS 195, 209 (1998).

[212] *See The Enforcers*, *supra* note 210.

[213] *See id.*; *see also* Harold Furchtgott-Roth, *The Failure of FCC Merger Reviews: Communications Law Does Not Necessarily Perform Better than Antitrust Law*, AMERICAN ENTERPRISE INST. (Dec. 9, 2002), http://www.aei.org/publication/the-failure-of-fcc-merger-reviews/print/ [http://perma.cc/2A4H-7YEW].

The initiation point for the federal antitrust review process for mergers is the Hart-Scott-Rodino filing.[214] The Hart-Scott-Rodino Antitrust Improvements Act provides that parties may not complete certain mergers, acquisitions, or types of asset transfers until they have made a detailed filing with the FTC and DOJ, and have waited for those agencies to determine that the proposed transaction does not violate antitrust law.[215] After a preliminary review of filed materials, antitrust regulators may make a "second request" for additional information.[216] Based on precedent, antitrust lawyers can predict when a second request will be made in relation to a particular transaction.[217] Consequently, the Hart-Scott-Rodino procedure is considered to be "clear, predictable, [and] lawful . . . ."[218]

If antitrust authorities deem that a proposed merger presents anticompetitive problems, the authorities have power to challenge the merger in federal court.[219] However, actual court challenges are "extremely rare," as parties whose proposed mergers face anticompetitive problems often modify or withdraw altogether their proposals.[220] This tidy process eliminates the need for "redundant" federal merger review.[221]

Over the years, the FTC and DOJ agencies have developed and published multiple revisions of the *Horizontal Merger Guidelines*, which describe the analytical framework the agencies follow when reviewing horizontal mergers.[222] The *Horizontal Merger Guidelines*,

---

214 Hart-Scott-Rodino Antitrust Improvements Act of 1976, 15 U.S.C. § 18a (2000).

215 *See id.* § 18a(a)–(b).

216 *See id.* § 18a(e).

217 *See* Furchtgott-Roth, *supra* note 213.

218 *See id.*

219 *See* 15 U.S.C. § 18a(f).

220 *See* Furchtgott-Roth, *supra* note 213.

221 *See id.*

222 *See* DEP'T JUST. & FED. TRADE COMM'N, HORIZONTAL MERGER GUIDELINES (2010), http://www.justice.gov/sites/default/files/atr/legacy/2010/08/19/hmg-2010.pdf [http://perma.cc/MPX4-WB85] [hereinafter 2010 Horizontal Merger Guidelines]. The 2010 guidelines replace those issued in 1992 and 1997, as they "reflect the ongoing accumulation of experience at the Agencies." *Id.* at 1 n.1; *see also* DEP'T JUST. & FED. TRADE COMM'N, HORIZONTAL MERGER GUIDELINES (1992, rev. 1997), http://www.justice.gov/atr/public/guidelines/hmg.pdf [http://perma.cc/7Z6A-CCJ6].

revised in 2010, "are the product of an extensive team effort" between the agencies.[223] As Carl Shapiro[224] describes:

> The process for revising the Guidelines was lengthy, collaborative, and open: the [a]gencies posted a series of questions, inviting public comment on possible revisions; numerous useful public comments were received and reviewed; the [a]gencies sponsored five public workshops at which panelists discussed possible revisions to the Guidelines; subsequently, the FTC made public a draft of the proposed Guidelines, again inviting additional public comments; numerous thoughtful comments were again received and reviewed; and in response to those comments, the proposed Guidelines were further clarified.[225]

Additionally, the agencies collaborated to produce a *Commentary on the Horizontal Merger Guidelines*.[226] In that document, the agencies provide specific examples of how they have applied the Guidelines' analytic principles in previously reviewed mergers.[227]

c) Anticompetitive Behavior (FCC/DOJ)

Though the FTC generally has authority to review mergers and acquisitions under sections 1 and 6 of the FTC Act,[228] the Clayton Act strips the FTC of its jurisdiction to review mergers and acquisitions between common carriers (in accordance with the common

---

[223] Carl Shapiro, *The 2010 Horizontal Merger Guidelines: From Hedgehog to Fox in Forty Years*, 77 ANTITRUST L.J. 701, 701 (2010).

[224] Deputy Assistant Attorney General for Economics, Antitrust Division, U.S. Department of Justice, on leave from his position as Transamerica Professor of Business Strategy, Haas School of Business, University of California at Berkeley. *See id.* at 701 n.1. Shapiro was also a member of the joint DOJ/FTC Horizontal Merger Guidelines working group. *See id.*

[225] *Id.* at 701–02.

[226] *See* DEP'T JUST. & FED. TRADE COMM'N, *Commentary on the Horizontal Merger Guidelines* (2006), http://www.justice.gov/sites/default/files/atr/legacy/2006/04/27/215247.pdf [http://perma.cc/6K7U-GT4D] [hereinafter *Commentary*]. Though it predates the 2010 guidelines, the Commentary "remains a valuable supplement" to them. *See* 2010 Horizontal Merger Guidelines*, supra* note 222, at 1 n.1.

[227] *See generally Commentary*, *supra* note 226.

[228] *See* 15 U.S.C. §§ 41, 46 (1994).

carrier exception) and vests that authority in the FCC instead.[229] Just as other types of mergers require approval by the FTC and the DOJ, telecommunications mergers require approval from both the FCC and the DOJ.[230]

Under this co-governance scheme, the agencies' statutory mandates differ.[231] Per section 7 of the Clayton Act, the DOJ may prohibit any acquisition that would "substantially . . . lessen competition, or . . . tend to create a monopoly."[232] The Hart-Scot-Rodino Antitrust Improvements Act of 1976[233] provides for a merger preclearance process that ensures timely DOJ review of any proposed merger.[234] A DOJ challenge to a proposed merger requires that the DOJ bear the burden of proof that the proposed merger violates antitrust laws.[235] As William J. Rinner notes, this is a "crucial" procedural posture, as DOJ-reviewed mergers are "presumed not to substantially lessen competition absent a contrary showing."[236] As a result, the DOJ's merger analyses lead to predictable standards on which companies can rely.[237]

The FCC, on the other hand, reviews mergers according to a broad "public interest" standard for license transfers, as articulated in the Communications Act sections 214 and 310.[238] Under

---

[229] *See id.* § 21(a).

[230] Rachel E. Barkow & Peter W. Huber, *A Tale of Two Agencies: A Comparative Analysis of FCC and DOJ Review of Telecommunications Mergers*, 2000 U. CHI. LEGAL F. 29, 29 (2000).

[231] *Compare* 15 U.S.C. § 18 (2000) *with* 47 U.S.C. § 214 (1997), *and* 47 U.S.C. § 310 (1996).

[232] *See* 15 U.S.C. § 18; Barkow & Huber, *supra* note 230, at 37.

[233] 15 U.S.C. § 18a.

[234] *See generally id.* § 18.

[235] *See id.*; Barkow & Huber, *supra* note 230, at 37; *see also* United States v. Citizens & S. Nat'l Bank, 422 U.S. 86, 120 (1975).

[236] William J. Rinner, *Optimizing Dual Agency Review of Telecommunications Mergers*, 118 YALE L.J. 1571, 1573–74 (2009).

[237] *See id.* at 1574; *see also supra* Part IV.C.1.b.

[238] *See* 47 U.S.C. § 214 (1997); 47 U.S.C. § 310 (1996). Under this standard, the FCC determines whether the proposed transaction works to promote "the public interest, convenience and necessity." 47 U.S.C. § 310(d); *see also* Weiss & Stern, *supra* note 211, at 197–98. The FCC has no specific statutory authority to review mergers except that under Clayton Act section 7, which is reserved for communications carriers and which the FCC has never used. *See* Furchtgott-Roth, *supra* note 213.

this "amorphous"[239] standard, the parties must affirmatively prove that the proposed transaction would serve the public interest, or alternatively, that "any likely anticompetitive effect is more than offset by other benefits."[240] Though the FCC views itself as a "shadow DOJ" that analyzes mergers to determine how they will influence telecommunications industry competition, the two agencies' approaches are, in reality, "markedly different."[241]

FCC merger review follows similarly the informal adjudication model the agency uses to review new license applications.[242] But in other aspects, it retains some elements of rulemaking.[243] Unlike the DOJ, the FCC faces no statutory deadline for completing its review.[244] The FCC rarely follows a self-imposed 180-day review deadline,[245] which leads to "long delays that risk undermining the very reasons for a merger."[246]

Before it approves a merger, the FCC may request concessions—conditions the merging parties must meet to win approval.[247] In cases where the FCC does this, the merging parties must either negotiate the conditions requested by the FCC or otherwise risk participation in a rare formal adjudicatory hearing, the prospective costs of which are "sufficiently high to deter any proposed

---

[239] Lawrence M. Frankel, *The Flawed Institutional Design of U.S. Merger Review: Stacking the Deck Against Enforcement*, 2008 UTAH L. REV. 159, 201 n.42 (2008).

[240] *See id.* at 201.

[241] Barkow & Huber, *supra* note 230.

[242] *See* Weiss & Stern, *supra* note 211, at 197 n.23 ("Section 308 of the Communications Act . . . requires the [FCC] to consider the same factors in reviewing a license transfer as in granting a license in the first place."); *see also* Rinner, *supra* note 236, at 1574.

[243] For example, parties who seek to transfer a license through a merger often must submit supporting materials; other stakeholders may submit remarks through a notice-and-comment process, and the FCC may request additional documentation. *See In re* Applications of Ameritech Corp., Transferor, and SBC Commc'n, Transferee, Memorandum Opinion and Order, 14 FCC Rcd. 14712, paras. 47–49 (1999).

[244] *See id.* paras. 39–45 (describing the FCC's review process).

[245] *See Informal Timeline for Consideration of Applications for Transfers or Assignments of Licenses or Authorizations Relating to Complex Mergers*, FCC (July 10, 2015), http://www.fcc.gov/transaction/timeline.html [https://perma.cc/RCR9-XB4F]; *see also* Barkow & Huber, *supra* note 230, at 31–32 ("The average merger takes two to four months to conclude. Telecommunications mergers, however, take between nine and twelve months to conclude.").

[246] *See* Barkow & Huber, *supra* note 230, at 33.

[247] *See id.* at 64.

merger."[248] Through these negotiations, which are guided by the overseeing commissioners' sense of whether pro-competitive factors and benefits to the public interest outweigh any perceived costs that the merger might impose, the FCC molds the transaction into a form that meets its approval.[249] Agreement to the FCC's conditions often results in merging parties' sacrificing most avenues for judicial review of the merger's final approval order.[250]

To determine the range and scope of any conditions, the FCC conducts an antitrust analysis that closely mirrors the steps outlined in the DOJ/FTC's *Horizontal Merger Guidelines*.[251] This analysis focuses more intensely on the proposed merger's effect on *potentially relevant* market participants than does the DOJ's prospective competition review.[252]

The FCC's antitrust authority has been widely criticized. The FCC/DOJ dual-standard regime for reviewing telecommunications mergers, it is argued, is inefficient and unworkable: the process results in no written rules, precedents, or guidance; it imposes unnecessary, difficult-to-calculate costs on merging parties; and it fails to yield consistent, predictable results across industry sectors.[253] As a result, the viability of FCC merger review co-governance faces much skepticism.[254]

---

248 Rinner, *supra* note 236, at 1575.

249 *Id.* at 1576.

250 *See id.*; Barkow & Huber, *supra* note 230, at 78.

251 *See* Barkow & Huber, *supra* note 230, at 44–45; Rinner, *supra* note 236, at 1575; *see also* 2010 Horizontal Merger Guidelines, *supra* note 222.

252 *See* Barkow & Huber, *supra* note 230, at 44–45.

253 *See* Furchtgott-Roth, *supra* note 213

254 *See, e.g.*, Lawrence M. Frankel, *The Flawed Institutional Design of U.S. Merger Review: Stacking the Deck Against Enforcement*, 2008 UTAH L. REV. 159, 255 (2008); Laura Kaplan, *One Merger, Two Agencies: Dual Review in the Breakdown of the AT&T/T-Mobile Merger and a Proposal for Reform*, 53 B.C. L. REV. 1571, 1612 (2012) ("Concurrent FCC and DOJ review of telecommunications mergers simply does not make sense."); Rinner, *supra* note 236; Philip J. Weiser, *Reexamining the Legacy of Dual Regulation: Reforming Dual Merger Review by the DOJ and the FCC*, 61 FED. COMM. L.J. 167, 198 (2008) ("The current state of merger review and merger remedies in the telecommunications industry is a second-best world where antitrust authorities encroach on the turf of the regulatory authorities and vice versa."); Furchtgott-Roth, *supra* note 213, at 7 ("The FCC's review of license transfers has made a mockery of the Clayton Act review of mergers and acquisitions by the federal antitrust agencies. Merging parties are subjected to various forms of regulatory

2. The FCC and FTC Already Co-Govern in Some Areas

The FCC and FTC share complementary jurisdiction in other areas already. The two agencies have successfully cooperated on issues involving special telephone services such as "900-numbers" and "dial-around" services, as well as in the context of "cramming."

a) 900-Numbers

The FCC and FTC, along with the U.S. Postal Service, share jurisdiction over the 900-number telephone services industry.[255] The FCC assigns the 900 area code, which designates that a certain type of call is being made rather than designating a call's geographic location.[256] Consumers can call 900-numbers to purchase information or service via phone.[257]

In this context, the FCC monitors long-distance carriers who provide 900-numbers, and shares jurisdiction with individual states over billing and collection services.[258] In tandem, the FTC investigates the complaints of consumers who allege that they were overcharged for 900-number services or did not receive those services as advertised.[259] U.S. Postal Service inspectors have authority to investigate 900-number-related fraud in cases where consumers' use of the services involves mail delivery.[260]

b) Dial-around Services

Another example of FCC and FTC collaboration is the agencies' *Joint FCC/FTC Policy Statement For the Advertising of Dial-Around and Other Long-Distance Services To Consumers* ("Joint Ad-

---

double jeopardy not faced by merging parties in other industries. Peculiar and potentially unlawful results are reached leading to a patchwork quilt of company-specific rules.").

255 *See* Nancy D. Galvez, *900 Numbers: A Controversial Industry*, 10 J. CONSUMER EDU. 1, 3–4 (1992).

256 *See* AT&T Commc'ns of Maryland, Inc. v. Comptroller of the Treasury, 176 Md. App. 22, 25–26 (Md. Ct. Spec. App. 2007), *rev'd sub nom.* AT&T Commc'ns of Maryland, Inc. v. Comptroller of Treasury, 950 A.2d 86, 87 (Md. Ct. Spec. App. 2008).

257 *See id.*

258 *See* Galvez, *supra* note 255, at 3–4.

259 *See id.* at 4.

260 *Id.*

vertising Guidelines").[261] To protect consumers from improper statements and disclosures contained in certain advertisements for dial-around long-distance services, the agencies jointly developed the Joint Advertising Guidelines to address which dial-around advertising approaches are permissible and which are misleading.[262] These services, which include "10-10-XXX" numbers, enable customers to bypass, or dial-around their pre-selected long-distance service provider for a given telephone to use a different service provider.[263] The March 1, 2000 Guidelines establish basic principles to which dial-around advertisers must adhere, including truthfulness, disclosure, clarity, and conspicuousness.[264]

Concurrent with the Joint Advertising Guidelines, the FCC announced that it fined MCI WorldCom Inc., a dial-around services company, $100 thousand for making misleading statements about its rates in advertisements.[265]

c) "Cramming"

The FTC and FCC join efforts to protect against "cramming"—the term given to the placing of unwanted or more-frequently-than-expected extra charges to customers' telephone bills.[266] Often, cramming results from scammers' attaching difficult-to-spot charges to text message services such as text-based ho-

---

[261] *See In re* Joint FCC/FTC Policy Statement For the Advertising of Dial-Around and Other Long-Distance Services To Consumers, Policy Statement, 15 FCC Rcd. 8654, para. 1 (2000) [hereinafter Joint Advertising Guidelines]; *see also* Furchtgott-Roth & Tramont, *supra* note 114, at 219–20.

[262] *See* Joint Advertising Guidelines, *supra* note 261, para. 10.

[263] *See id.* para. 3.

[264] *See id.* paras. 11–14.

[265] *See In re* MCI WorldCom, Inc., Order, 15 FCC Rcd. 4545 (2000); Peter S. Goodman, *FCC Fines MCI WorldCom for "Dial-Around" Ads*, WASH. POST (March 1, 2000), http://www.washingtonpost.com/archive/business/2000/03/01/fcc-fines-mci-worldcom-for-dial-around-ads/5a97d5e2-9817-45d5-8c7e-d4fe6cdb0897/ [http://perma.cc/6T77-4RY4].

[266] *See* FED. TRADE COMM'N, MOBILE CRAMMING: AN FTC STAFF REPORT 7, 11 (2014), https://www.ftc.gov/system/files/documents/reports/mobile-cramming-federal-trade-commission-staff-report-july-2014/140728mobilecramming.pdf [https://perma.cc/66TP-EKVF]; *Cramming—Unauthorized Charges on Your Phone Bill*, FCC (May 12, 2015), https://www.fcc.gov/guides/cramming-unauthorized-misleading-or-deceptive-charges-placed-your-telephone-bill [http://perma.cc/49MF-H6XS].

roscopes or trivia games.[267] Phone service carriers often take a cut of these extra fees.[268]

In May 2015, Verizon Wireless and Sprint were forced to pay $90 million and $68 million, respectively, to settle joint investigations by the FCC and FTC that revealed that both companies profited from cramming.[269] A similar joint investigation in 2014 resulted in AT&T's having to pay $105 million to settle cramming charges.[270] In its statement on the settlement, the FCC cited the investigation as "a prime example of government agencies working together on behalf of American consumers."[271]

3. Is There Opportunity for FCC/FTC Cooperation in the Online Privacy Context?

Just as the FCC and FTC collaborate and co-govern in the 900-number and the dial-around service contexts, the two agencies might cooperate similarly in the Internet privacy context. In the April 28, 2015 Public Workshop on Broadband Consumer Privacy, FCC and FTC officials expressed a desire to work together to regulate and enforce new rules governing how CPNI data will be collected, shared, used, and stored.[272] The FTC expressed a similar sentiment in a 2014 Comment to the FCC on Internet deployment.[273] FCC Enforcement Bureau Chief Travis LeBlanc has

---

[267] *See* Alex Fitzpatrick, *T-Mobile and the FTC: What Is Text Message "Cramming?*," TIME (July 2, 2014), http://time.com/2950184/what-is-text-message-cramming/ [http://perma.cc/9F3P-3MBZ].

[268] *See id.*

[269] *See* Fed. Comm. Comm'n, *Verizon & Sprint to Pay $158 Million to Settle Mobile Cramming Investigations*, FCC (May 12, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-333427A1.pdf [https://perma.cc/GLV7-8JAX]. The Consumer Financial Protection Bureau and various states' attorneys general joined in the effort. *See id.*

[270] *See* Fed. Comm. Comm'n, *AT&T Mobility to Pay $105 Million to Settle Wireless Cramming and Truth-In-Billing Investigation*, FCC (Oct. 8, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-329830A1.pdf [https://perma.cc/SQ53-9MTY].

[271] *Id.*

[272] *See Public Workshop*, *supra* note 85; *see also* Lydia Beyoud, *FCC, FTC Promise to Work in Concert on Consumer Privacy Rules in Broadband*, BLOOMBERG BNA (Apr. 28, 2015), http://www.bna.com/fcc-ftc-promise-n17179925915/ [http://perma.cc/9N22-9JY4].

[273] *See* Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of

stated that the FCC "has to start to think hard about data" after its decision to reclassify broadband Internet service providers as common carriers.[274] In an August 2015 *Wall Street Journal* commentary, FTC and FCC commissioners noted that they are "disturbed" that their respective agencies are on a "collision course."[275]

Neither the FCC nor the FTC have defined how their cooperation might take shape here. But the FTC's 2014 comment to the FCC may prove instructive: "as the FCC explores the laws and standards applicable to broadband providers . . . the FTC encourages the FCC to consider the [agencies'] well-established legal standards and best practices," such as those outlined in the Joint Advertising Guidelines.[276] A cooperative FTC/FCC privacy enforcement regime could mirror the agencies' approach to dial-around service enforcement. For example, the agencies could issue joint privacy guidance documents, such as those described above.[277] Additionally, the agencies could develop a set of consistent substantive principles for enforcing privacy jointly.[278] Or simi-

---

1996, as Amended by the Broadband Data Improvement Act, Comment of the FTC, GN Docket No. 14–126 at 12 (Sept. 19, 2014), https://www.ftc.gov/system/files/documents/advocacy_documents/federal-trade-commission-comment-federal-communications-commission-regarding-privacy-security/140919privacybroadband.pdf [https://perma.cc/9QRJ-GWTF] [hereinafter FTC Comment] ("The FTC welcomes the opportunity to share its experience promoting consumer privacy and data security with the FCC and looks forward to working with the FCC to ensure a consistent, efficient, and effective approach to enforcement and oversight in the broadband area.").

[274] Angelique Carson, *Regulators To Collaborate More, But How?*, IAPP (Mar. 11, 2015), https://iapp.org/news/a/regulators-to-collaborate-more-but-how [https://perma.cc/F6VY-7AWH].

[275] *See* Michael O'Rielly & Maureen K. Ohlhausen, *The Consequences of a Washington Internet Power Grab*, WALL ST. J. (Aug. 6, 2015), http://www.wsj.com/articles/the-consequences-of-a-washington-internet-power-grab-1438903157 [http://perma.cc/SM3G-LRYV] ("[W]e are disturbed to see our agencies on a collision course that could disrupt the country's thriving Internet providers and businesses, with little or no added benefit for consumers.").

[276] *See* FTC Comment, *supra* note 273, at 12. *See generally* Joint Advertising Guidelines, *supra* note 261.

[277] *See supra* notes 251–52, 261–64 and accompanying text; *see also supra* note 184 and accompanying text.

[278] *See generally* Joint Advertising Guidelines, *supra* note 261 (discussing substantive principles that the FTC and FCC apply to false or misleading advertising practices considered "deceptive" under section 5 of the FTC Act and "unjust and unreasonable" under section 201(b) of the Communications Act).

larly, the agencies could carve out expertise-specific areas for privacy enforcement, such as the FTC and DOJ do in the antitrust context.[279]

When considering co-governance as a viable option for Internet privacy regulation, we should remember the criticisms that the FCC's current co-governance scheme face.[280] For FCC/FTC privacy co-governance to be effective, it is important the regime would be free from any of the problems inherent in the FCC/DOJ's antitrust co-governance scheme. That is, a privacy co-governance regime should produce and rely upon clear, efficient, predictable rules and standards. Otherwise, the same inefficiencies that plague the FCC/DOJ antitrust co-governance regime would render any complimentary privacy governance scheme unworkable and ineffective.

CONCLUSION

Internet privacy is at a crossroads.[281] As consumer privacy and data security grow in interest to both consumers and regulators, rapid and aggressive changes to regulation in these areas are taking place. As businesses, consumers, and regulators adapt to these changes, they will inevitably face complications and tensions. Such is the way of progress.

But complications and tensions are less tolerable in some areas than in others. Generally speaking, we hope that our government functions effectively and efficiently; this is especially true when the government's function is to protect something as sacrosanct as personal privacy.

In this Note, I have attempted to provide an account of one tension that has arisen in the Internet privacy context. Though I have offered a few potential solutions for resolving this tension, it is

---

[279] *See, e.g.*, *supra* Part IV.C.1.b. Indeed, the FTC suggests this in its 2014 Comment. *See* FTC Comment, *supra* note 273, at 12 n.43 (citing Joint Advertising Guidelines, *supra* note 261, paras. 4–8).

[280] *See supra* Part IV.C.1.c.

[281] The author tips his hat to Professor Dan Deacon for inspiring this simple summary. *See* Deacon, *supra* note 82, at 183 ("Communications policy is at a crossroads.").

difficult to predict how resolution will occur—if it occurs at all. It will be interesting to wait and see.