

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

)	
In the Matter of)	
)	
Protecting the Privacy of Customers of)	WC Docket No. 16-106
Broadband and Other Telecommunications)	
Services)	
)	
)	

COMMENTS OF AT&T SERVICES INC.

James J.R. Talbot
Gary L. Phillips
David L. Lawson
AT&T SERVICES INC.
1120 20th Street, N.W.
Washington, D.C. 20036
(202) 457-3048

Jonathan E. Nuechterlein
Alan Charles Raul
C. Frederick Beckner III
Clayton G. Northouse
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
(202) 736-8000

May 27, 2016

TABLE OF CONTENTS

EXECUTIVE SUMMARY1

TECHNICAL BACKGROUND.....9

 1. Reading News Websites on a Home PC.....13

 2. Running a Google Search on a Home PC.....18

 3. Using Apps on a Mobile Network21

 4. Using Facebook at a WiFi Hotspot.....25

ARGUMENT.....30

 I. The Proposed Marketing Restrictions Fail Any Reasonable Cost-Benefit Analysis.....35

 A. The Proposed Asymmetric Marketing Burdens Are Irrational and Unnecessary to Serve Consumer Privacy Interests.....35

 1. The NPRM Identifies No Valid Basis for Subjecting ISPs to More Onerous Notice-and-Choice Restrictions than Non-ISPs, and the Proposed Opt-In Rules Are Irrationally Overbroad38

 2. The Proposed Opt-In Rules Would Serve No Genuine Privacy Interest Because Non-ISP Actors Exempt from Those Rules Would Continue Using the Same Information ISPs Would Be Restricted from Using50

 B. The Proposed Marketing Restrictions Would Suppress Competition, Reduce Innovation, and Impose Costs Disproportionate To Any Benefits51

 1. The Proposed Rules Would Raise Broadband Prices and Dampen Broadband Investment Incentives53

 2. The Proposed Rules Would Chill Innovation and Suppress Competition.....55

 3. The Proposed Rules Would Needlessly Confuse Consumers.....56

4.	The Proposed Ban on Commercial Inducements to Opt In to Data Uses Would Be Unlawful and Inimical to Broadband Deployment and Adoption	58
II.	The Commission Should Revise The Proposed Rules To Preserve The Benefits Of Aggregate And Non-Aggregate De-Identified Data	61
A.	Background: the Social and Economic Benefits of De-Identified Data ...	63
1.	Use of AT&T De-Identified Data by Businesses, Research Institutions, and Governmental Bodies Produces Enormous Public Interest Benefits	63
2.	AT&T Takes Significant Steps to Protect Privacy Interests When Creating and Using De-Identified Data.....	66
B.	The Proposed Rules Should Be Revised to Preserve the Benefits of De-Identified Data	67
III.	The Proposed Data-Security Rules Would Radically Overshoot The Mark And Impose Needless And Substantial Costs.....	72
A.	The NPRM’s Definition of Covered Information Would Be Radically Overbroad	75
B.	The Proposed Regulatory Requirements To “Ensure” Data Security Are Excessive and Irrational.....	78
C.	The Proposed Regulatory Requirements Governing Data “Breaches” Are Excessive and Irrational.....	80
IV.	The Proposed Rules Would Be Unlawful.....	87
A.	The Proposed Rules Would Be Arbitrary and Capricious	88
B.	The Proposed Rules Would Violate the First Amendment.....	91
C.	The Commission Lacks Statutory Authority to Address Key Subject Areas in Which the NPRM Proposes Rules.....	100
1.	The Statutory Category of “CPNI” Excludes Any Information Category That Is Widely Accessible to Non-ISP Companies Operating Online.....	100
2.	Section 222 Authorizes the Commission to Regulate Only CPNI, Not Some Broader Category of “Personal Information”	103

3.	Other Miscellaneous Provisions of the Communications Act Do Not Authorize the Commission to Adopt the Regime Proposed in the NPRM	108
D.	The Commission Lacks Authority to Extend Its Rules to Cable Operators and Satellite Providers.....	113
E.	The Proposed Ban on Arbitration Clauses Is Unlawful.....	114
F.	The Proposed Rules Raise Substantial Issues Under the Paperwork Reduction Act	115
G.	The Commission Should Make Clear That Any Rules It Adopts Have No Effect on the Ability of ISPs to Respond to Legitimate Requests By Law Enforcement or National Security Authorities.....	116
	CONCLUSION.....	118

EXECUTIVE SUMMARY

Information is the fuel of the modern economy. Recognizing that fact, federal privacy policy has long struck an important balance that targets potentially harmful uses of consumer data but does not interfere with beneficial data uses that power the commercial Internet. Led by the FTC, this balanced regime stresses two issues: (1) is individually identifiable information unusually sensitive (e.g., financial or medical data), and (2) is it shared with third parties?¹ When the answer to both questions is no, as it is for almost all data uses at issue in this proceeding, federal policy has adopted a permissive approach. For two decades, the FTC has applied this regime to the Internet ecosystem and has protected the privacy interests that consumers value most while fostering the Internet's dynamic growth. And the U.S. government as a whole has staunchly defended this regime as the appropriate regulatory model for all consumer online data.

Nothing has changed to warrant new burdens on the use of *nonsensitive, unshared* information, let alone burdens that apply only to ISPs. The only thing that has changed is that, in 2015, this Commission reclassified ISPs as “common carriers.” At the time, the Commission promised that it would use its new authority to impose “light touch” regulation designed to address only genuine market problems.² Now, to honor that commitment, the Commission should rely on privacy guidelines developed by industry bodies and multistakeholder processes, avoid onerous opt-in requirements for the mere use of nonsensitive data in an ISP's possession,

¹ See, e.g., FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, at 15-16 (Mar. 2012) (“*2012 FTC Privacy Report*”).

² Report & Order on Remand, *Protecting and Promoting the Open Internet*, GN Docket No. 14-28, FCC No. 15-24, ¶¶ 42, 59 (Mar. 12, 2015) (“*Open Internet Order*”).

tailor any data-security requirements to threats of actual consumer harm, and maintain technological neutrality between ISPs and other online companies.

Regrettably, the regulatory regime proposed here would impose unprecedented and unworkable restrictions on the ability of ISPs—and them alone—to collect and use online data for the benefit of consumers. The proposed restrictions are both unnecessary and far more burdensome than the flexible privacy safeguards the FTC has long placed on the Internet ecosystem. Worse yet, they would do nothing to advance the cause of privacy because Internet companies other than ISPs—from Google to Amazon to Acxiom—will go on collecting and using all of the same consumer data, regardless of what the Commission does in this proceeding.

At the heart of this misconceived regulatory proposal is a false analogy to the pre-broadband telephone world.³ The legacy telephone infrastructure was a closed system. The commercial entities with access to CPNI were generally all telecommunications carriers subject to Section 222, and there were no unregulated companies collecting and trading the same information for marketing purposes. In contrast, the Internet owes its explosive growth to the free flow of customer-specific information within a sprawling ecosystem of online companies. ISPs start that flow of information simply by performing basic functions, such as conveying a customer’s IP address and other data to various Internet sites. Once released, that information, along with many other data points the customer shares when communicating with edge providers, is used and exchanged by countless online companies for marketing purposes. The proposed rules, however, would impose absurd and severe constraints on how *ISPs themselves*

³ See, e.g., Statement of Tom Wheeler, Chairman, FCC, Before the Senate Comm. on the Judiciary, Subcomm. on Privacy, Tech. and the Law, at 1 (May 11, 2016) (“For decades, the Commission has steadfastly protected consumers against misuse of their information by [telephone companies] It only makes sense that consumers should enjoy similar privacy protections in the world of broadband.”).

can use the customer-specific information (such as originating and destination IP addresses) that they must share with other companies in this comparatively unregulated ecosystem.

The proposed rules also ignore the basic economic model of the modern Internet. Companies like Google and Facebook provide valuable services for free—yet boast market capitalizations in the hundreds of billions of dollars—only because they track consumers’ online activities and use that information for targeted advertising. That fact not only defines consumer expectations about how their data will be used, but also illustrates the pointlessness of the proposed rules. Those rules could not possibly guarantee the “privacy” of online consumer behavior because they would do nothing to address data collection and use by non-ISPs.

The NPRM also identifies no plausible basis for regulating ISPs more restrictively than all other participants in the Internet ecosystem. ISPs have an unusually strong privacy track record because, unlike many non-ISP actors, they have conventional contractual relationships with their customers and thus have every incentive to treat them fairly. The NPRM nonetheless tries to justify its proposed scheme of asymmetric regulation with familiar talking points about ISPs’ supposedly unequalled visibility into consumer behavior and supposed invulnerability to consumer preferences. But those talking points lack any factual foundation.

First, ISPs have *less*, not more, comprehensive visibility than many edge providers into their users’ online activities. As the FTC has explained, the providers of “operating systems and browsers” such as Android and Chrome “may be in a position to track all, or virtually all, of a consumer’s online activity to create highly detailed profiles,” and consumers “have limited ability to block or control such tracking” unless, for example, they “chang[e] their operating system.”⁴ In contrast, ISPs have less and less ability to track their subscribers’ online activities

⁴ 2012 FTC Privacy Report at 56.

because a clear and rapidly growing majority of Internet traffic is now encrypted. Such encryption blocks ISPs from viewing not only the content of Internet communications, but also the detailed URLs of visited websites. Such encryption has little or no effect, however, on the ability of websites, browsers, operating systems, and other large platform providers to read the contents of Internet communications and send targeted ads in response. In addition, many consumers use multiple ISPs over the course of a day, and each time they switch, they disappear from the view of the ISPs they are not using. In contrast, operating systems, browsers, and mobile apps can keep close track of consumers all day long.

Second, the NPRM is on no firmer ground when it suggests that ISPs should be regulated more because they supposedly face less competition. Indeed, ISPs typically face more competitive pressure than comparable collectors of consumer information. For example, it is easier for a privacy-conscious consumer to switch from one mobile carrier to another (and keep the same phone number) than to cancel his Gmail account or switch to some alternative to Facebook. And it is ironic that the NPRM cites “competition” as a basis for its proposed rules because, in fact, those rules would irrationally shield Google and other incumbents from competition by new entrants—ISPs—in the data marketplace.

Finally, the proposed rules would be affirmatively harmful to consumers, not just unnecessary to protect them. By making it far more difficult for ISPs to do what the rest of the Internet has long done—use nonsensitive customer data to engage in socially productive first- and third-party marketing—the rules would reduce the profitability of broadband services, exert upward pressure on broadband prices, and depress incentives for broadband deployment. The rules would also distort competitive dynamics by hamstringing ISPs’ ability to use existing customer information to market even many of their own services and service bundles. The rules

would needlessly confuse consumers, many of whom will not understand that all the information these rules are designed to “protect” will remain freely accessible on the same liberal terms as before to the providers of their operating systems, browsers, and mobile apps. And the proposed data breach rules would impose needless new compliance costs on ISPs and subject consumers to useless bombardment by premature notifications of “data breaches,” many of which would turn out to pose no genuine threat to anyone.

After a Technical Background section, the remainder of these comments is organized as follows.

Section I addresses the NPRM’s proposed marketing restrictions, with their unprecedented requirements for opt-in consent. Under longstanding federal policy, “most first-party marketing practices are consistent with the consumer’s relationship with the business and thus do not necessitate consumer choice,” even in the form of opt-out consent.⁵ Federal policy has also taken a flexible approach to third-party marketing that involves no transfer of customer-specific information to third-party advertisers. Contrary to the NPRM’s mistaken assumption, most third-party marketing falls into this category, as exemplified by the behavioral third-party advertising that Google sends its users on the basis of their Gmail content.

The proposed rules would break sharply with the notice-and-choice regime applicable elsewhere in the Internet ecosystem. They would subject ISPs to the most speech-restrictive requirement—opt-*in*—for most marketing uses of any consumer information, even where the information is neither sensitive nor shared with third parties. Shifting to opt-in would dramatically reduce the information that can be productively used for marketing purposes and, carried to its logical conclusion, would slam the brakes on the business models of Google,

⁵ 2012 FTC Privacy Report at 40.

Facebook, Amazon, and much of the rest of the Internet ecosystem. Those consequences would follow not because consumers would desire them, but because the transaction costs and negative externalities of a compulsory opt-in regime would create market failures whenever that regime's presumption against data-sharing is misaligned with revealed consumer preferences. Although the proposed rules would recognize a narrow exception for ISP marketing of "communications-related services," the NPRM identifies no basis—and there is none—for limiting the flexibility of opt-out consent to that context alone.

The Commission would likewise ignore the most basic principle of the online economy if, as it contemplates, it banned consumers even from giving their informed consent to marketing uses of their nonsensitive information in exchange for discounted broadband services.

Consumers routinely enable such uses of their individually identifiable data whenever they perform a Google search, sign into a free social-networking site, download a mobile app, or log into a "free" WiFi network. Without such arrangements, the modern Internet would be a more impoverished place: it would have far fewer affordable services for consumers because it would be based more on a subscription model than today's ad-supported model. A paternalistic ban on such arrangements after notice and choice would, by definition, increase the price and lower the output of any affected service, including broadband Internet access.

Section II addresses the proposed restrictions on the ability of ISPs to use and provide anonymous, *de-identified* data (including aggregate data) to third parties, including businesses, universities, and governmental agencies. Use of de-identified data produces enormous social benefits. For that reason, the Commission should remove any suggestion that ISPs are prohibited from taking the necessary first step in the creation of de-identified data: maintaining non-aggregate data and processing it to create de-identified data. The Commission should also avoid

subjecting ISPs to an unprecedented regime of strict liability for third-party actions. And it should not create ISP-specific burdens on the creation, use, or sharing of de-identified data, such as by requiring “opt-in” consent.

Section III addresses the NPRM’s proposed data-security rules. The NPRM adopts patently overbroad definitions of covered data that would saddle ISPs with burdensome regulatory obligations to protect customer information that is not even arguably sensitive or “proprietary.” Unlike any other state or federal breach-reporting regime, the NPRM would extend reporting requirements to widely available information that is routinely disclosed by consumers and poses no genuine privacy risk, such as a customer’s mere name and address. The literal language of the proposed regulation would also irrationally impose strict liability on ISPs for the conduct of third parties, regardless of the reasonableness of the actions they took to secure customer data. And the contemplated rules would implausibly require ISPs to disclose breaches to consumers within ten days, a timetable often too short to allow even the most assiduous investigator to get to the bottom of what has happened and who is at risk.

Section IV addresses the legal infirmities of the Commission’s proposals. Many of the proposed rules would flunk any rational cost-benefit analysis and would thus violate the Commission’s APA obligation to engage in reasoned decision-making. Because the rules would restrict speech, they would also violate the First Amendment. As noted, the rules would require ISPs to adopt opt-in consent mechanisms before using customer information for most first-party and all third-party marketing, even where the information is *nonsensitive* and *is not shared* with third parties. That requirement would fail all three prongs of the applicable *Central Hudson* analysis: (1) it would promote no discernible privacy interest where information is neither sensitive nor shared; (2) it would be radically underinclusive in that it would do nothing to keep

non-ISPs from collecting and using all the same information for their own marketing purposes; and (3) it would not be narrowly tailored because, if the government had any valid interest in “protecting” consumers from unshared uses of nonsensitive information, it could achieve that interest through a less intrusive opt-out mechanism.

The Commission also lacks statutory authority to regulate ISP data practices in the manner it proposes, even if its threshold reclassification decision is upheld. First, much of the customer information the Commission seeks to regulate—all information that is broadly collected and used by non-ISP entities—does not fall within the scope of Section 222 because it is not “proprietary” in any relevant sense of the word. Second, even if such information could be considered “proprietary” and thus “CPNI,” Section 222 grants the Commission no authority to regulate customer data (such as mere names and addresses) that do *not* fall within the statutory definition of CPNI, as the Commission itself recognized until recently. Third, even if Section 222(a) could be read to address non-CPNI information, that provision by its terms addresses only “the confidentiality” of such information and thus could not support the proposed rules to the extent they address the mere *uses* (as opposed to disclosure) of such information.

* * *

In sum, any rules adopted in this proceeding should preserve technological neutrality between ISPs and the rest of the Internet ecosystem, and should narrowly target only those data practices that threaten actual consumer harm.⁶

⁶ These comments are submitted by AT&T Services Inc. on behalf of its affiliates (collectively, “AT&T”).

TECHNICAL BACKGROUND

The NPRM asserts (at ¶ 2) that broadband ISPs “are the most important and extensive conduits of consumer information” and have unique access to information collected about customers online. That assertion rests on a false analogy to the legacy world of circuit-switched telephony, for which Congress designed Section 222. Addressing telephone services in 2002, the Commission found “that telecommunications carriers are in a unique position to collect sensitive personal information—including to whom, where and when their customers call—and that customers maintain an important privacy interest in protecting this information from disclosure and dissemination.”⁷ The Commission now assumes that ISPs occupy the same “unique position” in the Internet ecosystem that telephone companies enjoyed in the telephone world. That factual premise is critical to the NPRM’s proposal to subject ISPs, and them alone, to unprecedented restrictions on their collection and use of consumer data.

That premise, however, is false and indeed unmoored from the realities of the modern Internet. The legacy telephone infrastructure was a closed system: in general, only a limited number of local and interexchange carriers had access to CPNI, and they were all telecommunications carriers subject to Section 222 regulation. There was no ecosystem of unregulated companies harvesting that same information for marketing purposes.⁸ But on the

⁷ Third Report and Order, *Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, 17 FCC Rcd 14860, ¶ 1 (2002) (“2002 CPNI Order”).

⁸ Technology has also transformed the market for voice communications. The public-switched telephone system is undergoing a major transition from legacy circuit-switched technology to a new system that relies on the Internet Protocol for the routing of voice services. Today, a range of VoIP providers collect call-detail records yet remain uncovered by the Commission’s CPNI rules unless they are interconnected (for both originating and terminating calls) with the public switched telephone network. In addition, mobile operating systems such as Android create comprehensive phone and text logs and expose that customer data to app developers. *See, e.g.*, Google Play Help, *Control your app permissions on Android 6.0 and up*, <https://support.google.com/googleplay/answer/6270602?hl=en>. To the extent that the voice marketplace today more closely resembles the Internet than the legacy telephone

Internet, countless entities that are not regulated telecommunications carriers have access to essentially all the same information as ISPs. Anyone using the Internet shares information about his or her usage not only with his or her ISP, but also with his or her operating system, browser, mobile apps, website operators, ad networks, and data brokers, and all of that information becomes part of a widely accessible universe of customer-specific information.

In fact, the leading non-ISP actors in the Internet ecosystem—including search engines (e.g., Google), browsers (e.g., Chrome), ad networks (e.g., DoubleClick), social media (e.g., Facebook), operating systems (e.g., Android), and data brokers (e.g., Acxiom)—have far more visibility than ISPs into the online behavior of individual consumers and often are more difficult to avoid.⁹ A single non-ISP can amass highly personal information collected across different devices on different networks to develop individualized profiles that are in turn used to target advertisements on behalf of third parties.

Google and Facebook alone account for more than 54 percent of the digital advertising market and 67 percent of the mobile advertising market.¹⁰ One out of every five minutes on a mobile device is spent using the Facebook app.¹¹ Sixty percent of all devices exchange traffic with Google every day, and twenty-five percent of all web traffic in North America runs through

network, voice services should be subject to the same light-touch regime that the FTC applies to the Internet ecosystem at large.

⁹ Nothing in these comments should be construed as criticism of the identified edge providers or other non-ISP companies that collect and use online customer information. To the contrary, as discussed below, these companies and their data-oriented business models make valuable contributions to consumer welfare.

¹⁰ See Investor's Bus. Daily (May 3, 2016), <http://www.investors.com/news/technology/google-facebook-digital-duopoly-seen-with-67-of-mobile-ad-market/>; Aleksandra Gjorgievska, *Google and Facebook Lead Digital Advertising Industry to Revenue Record*, Bloomberg Technology (Apr. 21, 2016), <http://www.bloomberg.com/news/articles/2016-04-22/google-and-facebook-lead-digital-ad-industry-to-revenue-record>.

¹¹ Adrienne LaFrance, *Facebook Is Eating the Internet*, The Atlantic (Apr. 29, 2015), <http://www.theatlantic.com/technology/archive/2015/04/facebook-is-eating-the-internet/391766/>.

Google’s servers.¹² Google and Facebook also collect information relating to private messages using their services and web-browsing information from the millions of third-party web pages that contain social media plugins, such as Google’s “Google+” or Facebook’s “Like” button.¹³ And Google and Facebook operate advertising networks that collect web browsing data from hundreds of thousands of popular websites and compile the data into comprehensive profiles of user web browsing activity.¹⁴ Google also operates the Chrome browser that feeds it information, *infra* pp. 13-15, as well as the Android operating system on mobile devices through which Google apps feed it information, *infra* pp. 21-22. The integrated and pervasive online presence of these companies is nearly impossible for consumers to avoid—especially when consumers depend on them for their email, messaging, web searching, and social media.

By contrast, an increasing majority of all web traffic is now obscured to ISPs.¹⁵ As explained below, the rise of encryption has reduced ISPs’ ability to view information about their own customers’ use of Internet services, including those of Google and Facebook. Google and Facebook, meanwhile, have full view of their customers’ use of (1) their own sites and apps (even when these apps are running in the background) and (2) the millions of third-party web

¹² Dara Kerr, *Google Sets Internet Record with 25 Percent of U.S. Traffic*, Cnet.com (July 22, 2013), <http://www.cnet.com/news/google-sets-internet-record-with-25-percent-of-u-s-traffic/>.

¹³ The Center for IT & IP Law at the University of Leuven estimates that more than 13 million websites contain the Facebook “like” button. *From Social Media Service to Advertising Network: A Critical Analysis of Facebook’s Revised Policies and Terms* (Aug. 2015), <https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf>; Google, *Privacy Policy* (Mar. 25, 2016), <https://www.google.com/intl/en/policies/privacy/?fg=1>; Facebook, *Data Policy* (Jan. 30, 2015), <https://facebook.com/about/privacy>.

¹⁴ See Russell Brandom, *Google and Facebook Still Dominate Tracking on the Web*, The Verge (May 16, 2016), <http://www.theverge.com/2016/5/18/11692228/google-facebook-web-tracking-survey-advertising>.

¹⁵ See Peter Swire et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* at 3 (Geo. Tech. Inst. for Infor. Sec. & Privacy, May 2016) (“Swire Report”) (stating that 49 percent of total web traffic was encrypted as of the beginning of 2016, rising to 70 percent by year’s end), <http://apps.fcc.gov/ecfs/document/view?id=60002031928>.

pages where they have placed social media plugins (even when these third-party sites are encrypted). This “visibility gap” between ISPs and other actors is rapidly widening, not only because the increasing prevalence of encryption, but also because many consumers are more continuously connected to the same edge providers (such as Google via Android) than to any given ISP over the course of a day.

None of these developments should come as news to the Commission. For example, they are the subject of a comprehensive February 2016 analysis coauthored by privacy expert Peter Swire, who served as Chief Counselor for Privacy in the Clinton Administration and as Special Assistant to the President for Economic Policy under President Obama.¹⁶ At the Commission’s invitation, Professor Swire also participated in the public workshop the Commission held on broadband consumer privacy.¹⁷

The NPRM ignores these developments and, indeed, nowhere cites Professor Swire’s rigorous and widely publicized analysis. To address that factual deficit, this section reviews in detail how online data is collected and shared in the Internet ecosystem. We examine, with concrete illustrations, which online entities collect what types of user information when a typical consumer (i) accesses news websites on his or her home computer; (ii) runs a Google search on that computer; (iii) watches Netflix on his smartphone while riding a bus; and (iv) checks Facebook on that smartphone while sitting in a coffee shop. In the process, we also describe the basic mechanics of the online advertising ecosystem.

¹⁶ See *id.* Professor Swire was also one of five presidential appointees to the Review Group on Intelligence and Communications Technologies within the Office of the Director of National Intelligence.

¹⁷ Peter Swire, Comments to the FCC on Broadband Consumer Privacy, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (Apr. 28, 2015), <https://transition.fcc.gov/cgb/outreach/FCC-testimony-CPNI-broadband.pdf>.

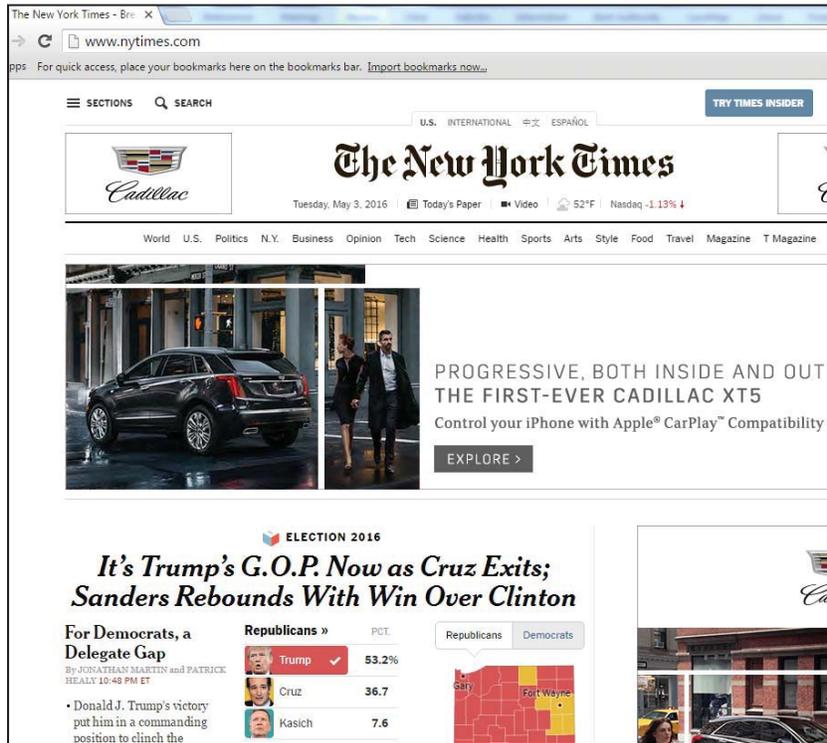
1. Reading News Websites on a Home PC

John Smith subscribes to AT&T U-Verse as his residential ISP. While at home, he decides to read the New York Times online. He opens the Google Chrome browser on his desktop computer and begins typing “www.nyt” into the address box. Chrome’s autofill function proposes “www.nytimes.com,” and John clicks on that URL. When this happens, Chrome may send information about John’s choice to Google.¹⁸ It also sends this information to AT&T, which consults the Domain Name System to determine the relevant IP address for the Times’ web server, and a network session is established within seconds between that server and John’s computer. On John’s end, Chrome resolves the data into a webpage that John can read. Chrome sends Google’s centralized servers various bits of information about John, including the date and time, the destination IP address he visited (“www.nytimes.com”), his IP address, and his location information. Indeed, Chrome may already have sent logging information back to Google from the moment John began entering “www.nyt” into the URL window.¹⁹

¹⁸ See *Google Chrome Privacy Notice*, <https://www.google.com/chrome/browser/privacy/> (“If you accept a predicted query or URL, Chrome may send that information from the browser to your default search engine as well.”).

¹⁹ See *Id.* (“If you use Chrome’s location feature, which allows you to share your location with a web site, Chrome will send local network information to Google Location Services to get an estimated location. ... The local network information may include (depending on the capabilities of your device) information about the wifi routers closest to you, cell IDs of the cell towers closest to you, the strength of your wifi or cell signal, and the IP address that is currently assigned to your device.”); *id.* (“For Chrome browsers and Chrome OS, you may choose to send usage statistics and crash reports to Google.”). Google states that it generally may “use the information we collect from all of our services ... to offer you tailored content—like giving you more relevant search results and ads.” *Google Privacy Policy* (Mar. 25, 2016), <https://www.google.com/intl/en-GB/policies/privacy/>.

Here is what John sees:



For the sake of completeness, we have chosen the New York Times website for this example precisely because, unlike the other websites discussed below, it is (at least for now) one of the few leading websites left that has not yet followed the industry trend towards automatically encrypting its exchanges with visitors. Thus, the content that the Times sends John is not only visible to Google (via Chrome), but also theoretically visible to John's ISP, here AT&T.²⁰ But if John had instead gone to the Washington Post's website, the contents of the webpage would have been invisible to AT&T because the Washington Post uses HTTPS, a protocol that encrypts web traffic on an end-to-end basis between a browser and the destination

²⁰ AT&T uses ISP web-browsing data for customized marketing purposes only when customers have provided opt-in consent after clear notice. AT&T separately uses web-browsing data for *non-*marketing purposes, such as network management, service improvement, and cybersecurity. Significantly, neither deep packet inspection nor any of the other tools available to AT&T (or any other ISP) would permit it to read encrypted communications, as discussed in further detail below.

website. That content would still be visible, however, to Google through its Chrome browser. Today, 42 of the top 50 websites encrypt their communications using HTTPS by default or on user log-in, and nearly 70 percent of global Internet traffic will be encrypted by year-end 2016.²¹

Once John downloads the New York Times homepage, several different entities will already have gathered information about him. The Times itself can associate his IP address with his interests, as revealed by (for example) the articles he chooses.²² The Times also may collect John's geolocation information, browser type, and computer information. John is subject to such data collection whether or not he registers as a paid subscriber to the New York Times, as he might have to do in order to view more than a few articles per month. But if he does register as a subscriber, the Times will collect even more information to fill out his demographic profile, including his "ZIP code, age, sex, household income, job industry and job title."²³ Like many other websites, the New York Times also uses "cookies"—small text files stored on John's browser—to track his browsing history.²⁴

²¹ Swire Report at 3, 29, 36-38; Robert Hackett, *Most Internet Traffic Will Be Encrypted By Year End. Here's Why*, *Fortune* (Apr. 30, 2015), <http://fortune.com/2015/04/30/netflix-internet-traffic-encrypted/>.

²² The New York Times, *Privacy Policy* (June 10, 2015) ("We may collect non-personal information about the computer, mobile device or other device you use to access the NYT Services, such as IP address, geolocation information, unique device identifiers, browser type, browser language and other transactional information."), <http://www.nytimes.com/content/help/rights/privacy/policy/privacy-policy.html>; *id.* ("[W]e gather certain information automatically and store it in log files. This information may include Internet protocol (IP) addresses (the region or general location where your computer or device is accessing the Internet), browser type, operating system and other usage information about the use of the NYT Services, including a history of the pages you view.").

²³ *Id.* ("Registration for the NYT Services may require that you supply certain personal information, including a unique email address and demographic information (ZIP code, age, sex, household income, job industry and job title) to register.").

²⁴ *Id.* ("We use 'cookies,' Web beacons, HTML5 local storage and other similar technologies. These technologies allow us to manage access to and use of the Services, recognize you and provide personalization, and help us understand how people use the NYT Services.").

Third-party advertisers likewise collect information about John when he visits the Times website. The Times' Privacy Policy lists seventeen third parties that may collect such information and "who, in the course of serving or displaying ads on NYTimes.com, may place a cookie on your browser."²⁵ One of these third-party advertisers is Google, which may collect information about John through its ad network, Google Doubleclick. Google may drop or read a cookie on John's browser (which, in this example, is Chrome, also owned by Google) to track his web-browsing history and serve him ads on other websites, after John has left the Times website.²⁶

While John first downloads the Times homepage, Google may use John's browsing history to facilitate a bidding process for third-party advertisers. This bidding process determines, for example, which banner advertisement is placed at the top of John's screen, and it involves many players. Advertisers (such as Cadillac) and publishers (such as the New York Times) rarely negotiate directly with each other. Instead, they rely on middlemen to find platforms to sell products for advertisers and advertising space for publishers; these brokers are commonly known as "demand-side platforms" and "supply-side platforms," respectively.²⁷ Demand-side and supply-side platforms then bid for ad placements in ad exchanges (Google DoubleClick, in this example). Here, Cadillac may have used a demand-side platform, such as

²⁵ See *id.* (listing Atlas Solutions, AdTech, Audience Science, DoubleClick, EyeBlaster, EyeReturn, Eyewonder, Google / DART, Interpolls, Medialets, MediaPlex, Pointroll, Quantcast, Quigo, Spongecell, TremorMedia, and Unicast), <http://www.nytimes.com/content/help/rights/privacy/policy/privacy-information.html>. The Times discloses that, "[i]n the course of serving certain advertisements, an advertiser may place or recognize a unique cookie on your browser in order to collect certain information about your use of the NYT Services." *Id.*

²⁶ *Id.* ("These companies may place or recognize cookies, Web beacons or other technology to track certain non-personal information about our website users. ... In many cases, this information could be used to show you ads on other websites based on your interests.").

²⁷ See generally Swire Report at 82-88.

MediaMath or DataXu, to purchase the most useful placement and target the most relevant users, such as men between 35 and 50 looking to purchase an SUV. At the same time, the New York Times likely worked with a supply-side platform to analyze the demographics of the visitors to its site and market the placement of advertising space. The two platforms then bid on an ad exchange to place Cadillac’s ad on the New York Times homepage.

This advertising marketplace functions efficiently—and has fueled the explosive growth of the modern Internet—only because the free flow of customer information gives companies highly efficient ways to reach the consumers most interested in buying their products. For example, before John visited the Times website, he may have run a Google search for “new SUVs” and visited Car and Driver (<http://www.caranddriver.com/>). Both Google and Car and Driver, among many other sites, may have tracked John’s online behavior and identified him as a potential SUV buyer.

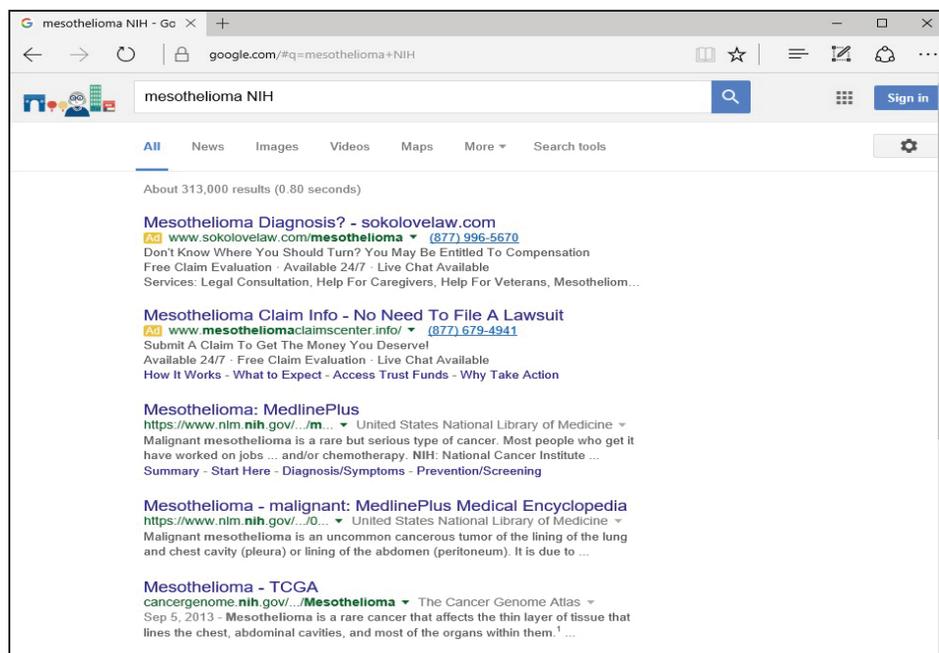
In addition, a third-party data broker such as Acxiom or DataLogix may have bought and sold demographic information about John relating to his income, marital status, and other characteristics. Data brokers trade in consumer information without directly interacting with consumers. They instead collect information from publicly available sources and combine it with customer-specific data they buy from other sources, including websites, mobile app developers, and social media platforms.²⁸ With this comprehensive information set, data brokers assemble profiles of particular consumers, identifying biographical details such as gender, age, education, employment, race, wealth, children, marital status, political affiliation, personal

²⁸ See, e.g., FTC, *Data Brokers: A Call for Transparency and Accountability*, at 46 (May 2014) (“*Data Brokers*”), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

interests, purchase history, and housing information.²⁹ Data brokers then sell this information on the open market to anyone interested in buying it, including the advertisers who wish to reach consumers with demographic profiles like John’s.

2. Running a Google Search on a Home PC

Still using his home computer, John next reads an article on the Times website about new research by the National Institutes of Health (“NIH”) on treatments for mesothelioma. He wonders if his mother—who suffers from this condition—can benefit and decides to run a Google search. John decides to switch his web browser. He opens the Microsoft Edge browser also installed on his computer, accesses Google’s website, enters the key terms “mesothelioma NIH” into the search box, and sees the following results:



Significantly, John’s residential ISP—AT&T U-verse—lacks even the theoretical ability to know what John is asking about in this search because Google uses end-to-end HTTPS

²⁹ See, e.g., <https://www.aboutthedata.com> (revealing the profile information collected by Acxiom that is sold to third parties).

encryption by default (signified by the “lock” icon next to “google.com” in the above screen shot). AT&T knows that John (or someone using his computer) is communicating with Google because AT&T is responsible for transmitting packets between John’s computer and Google’s server. In particular, AT&T can view limited “header information” in those packets—the bare data elements necessary to connect two computers in a web session. But even if AT&T used deep packet inspection, it could not know that John has asked Google to run a search using these search terms (“mesothelioma” and “NIH”), nor does it have any way of reading the search results that Google sends back to John.

In contrast, Google obviously does know what John is asking about (because it receives his data in encrypted format that he and Google alone can decode). In addition to producing search results, Google has also sent John targeted third-party ads, the first on behalf of a law firm specializing in mesothelioma-related legal representation.³⁰ Also, if John is signed into his Google account, Google can associate these searches explicitly with him (i.e., an individually identifiable “John Smith”).³¹ Finally, in addition to Google, Microsoft also has potential visibility into John’s inquiry.³² Depending on John’s settings, Microsoft’s personal assistant Cortana, which is integrated with the Edge browser, may see the full URL of the page, the search

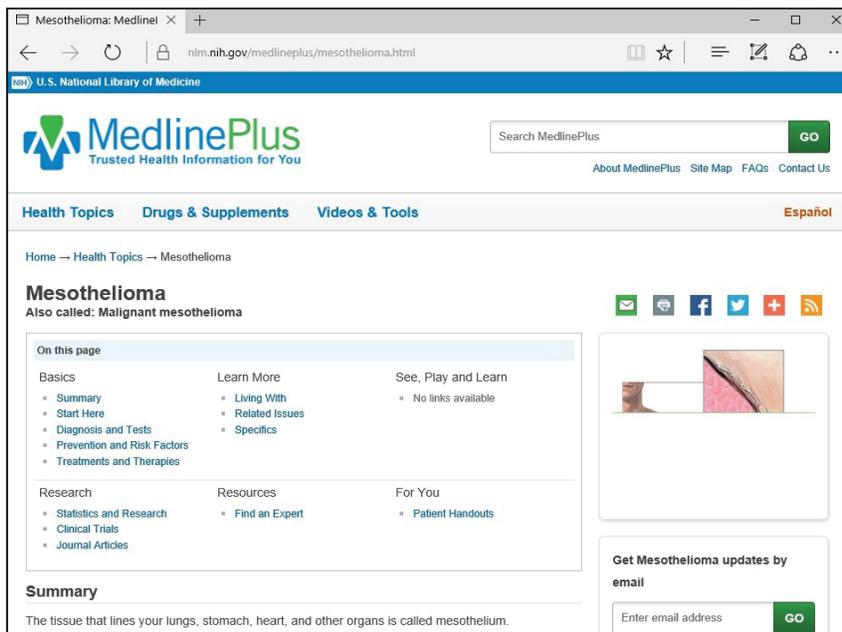
³⁰ See, e.g., *Google Terms of Service*, (Apr. 14, 2014) (“Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection.”), <https://www.google.com/policies/terms/>. However, Google states that it will not “associate an identifier from cookies or similar technologies with sensitive categories, such as those based on race, religion, sexual orientation or health.” Google, *Privacy Policy* (Mar. 25, 2016), <https://www.google.com/policies/privacy/>.

³¹ Swire Report at 53.

³² Two operating systems account for virtually all of the desktop market: Apple’s Mac OS X and Microsoft’s Windows. See Emil Protalinski, *Windows 10 Hits 9% Market Share, El Capitan Takes First Among OS X Versions*, VentureBeat (Dec. 1, 2015) (reporting Mac OS X and Windows account for more than 98% of worldwide market share), <http://venturebeat.com/2015/12/01/windows-10-hits-9-market-share-el-capitan-takes-first-among-os-x-versions/>.

terms, and the results. And it may transmit this information back to centralized Microsoft servers for further analysis and use.³³

John clicks on the first result below the advertisements—the one for NIH:



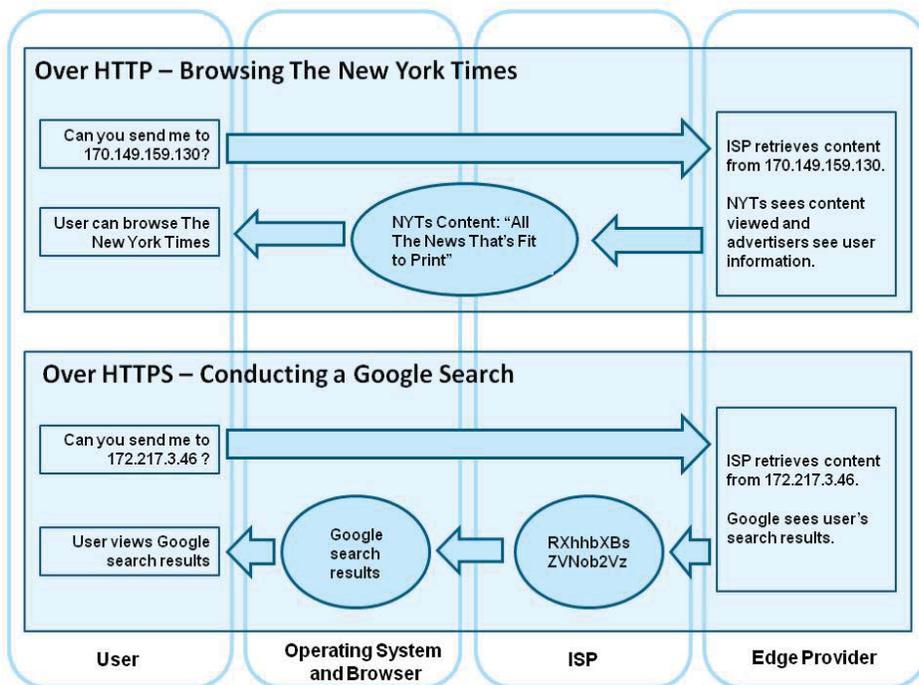
Like Google, NIH uses HTTPS for end-to-end encryption of web sessions with its site's visitors.³⁴ Thus, while John's browser and the website know exactly what webpage John is visiting, AT&T does not. Instead, it can see only the domain name ("www.nlm.nih.gov/"), not

³³ See *Microsoft Edge and Privacy: FAQ* ("If you're using Cortana with Microsoft Edge, your browsing history will be sent to Microsoft to help Cortana personalize your experience."), <http://windows.microsoft.com/en-us/windows-10/edge-privacy-faq>; *id.* ("If the Use page prediction setting is on, it sends your browsing history to Microsoft, uses aggregated browsing history data to predict which pages you're likely to browse to next, and then loads those pages in the background for a faster browsing experience.").

³⁴ The federal government has encouraged the use of encryption. See e.g., Federal Financial Institutions Examinations Council, *IT Examination Handbook* 45 (2006) (directing firms to "secure remote access to and from their systems by . . . [u]sing strong authentication and encryption to secure communications"); 12 C.F.R. pt. 364, App. B, at III.C.1 ("Each [institution] must consider whether . . . [e]ncryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access [is appropriate]."); 45 C.F.R. § 164.312(a)(2)(iv) ("Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.").

the more detailed URL (“www.nlm.nih.gov/medlineplus/mesothelioma.html”) showing that John has visited the NIH page dealing with mesothelioma.³⁵

The following chart sums up by illustrating how encryption affects what various ISP and non-ISP entities can see when they process a Google search.³⁶



3. Using Apps on a Mobile Network

To this point, we have focused on web activity on a desktop computer; we now turn to the world of mobile devices, apps, and operating systems. In that mobile ecosystem, too, non-ISP actors have access to a much broader and more continuous range of information about individual consumers than ISPs do.

Suppose John gets on a bus and watches a video using the Netflix app on his Samsung smartphone. His phone is connected to the Verizon Wireless network and runs on Google’s

³⁵ Swire Report at 27.

³⁶ A similar diagram appears in the Swire Report at 26.

Android operating system. John’s use of the Netflix app gives Netflix a variety of information about him that can be used for marketing purposes. Netflix collects John’s unique device ID, device and software characteristics, connection information, IP address, general and precise locations, and other data.³⁷ In addition to Netflix, other third parties also collect a wealth of information about John. For starters, the mere use of his phone gives Google significant insights into his user profile. The Android operating system can see that John has downloaded and is using his Netflix app. Depending on the phone’s settings, various Google apps—such as Google Maps or the Google search app—also enable Google to learn John’s precise geolocation, what apps he has been using, and what IP addresses he has visited.³⁸

While John is watching a video on his phone, other apps are also collecting his information. Before John got on the bus, he may have considered hiring a car and opened the Uber app. Though John stopped actively using that app when he saw the bus coming, the app is still running in the background and is collecting John’s precise location as he moves through town on the bus.³⁹ John also plays the game Words with Friends—one of the more popular apps available for Android devices or iPhones. This app, developed by Zynga, collects John’s

³⁷ Netflix, *Privacy Statement* (disclosing the collection of “device IDs or unique identifiers, device and software characteristics (such as type and configuration), connection information, statistics on page views, referral URLs, IP address and standard web log information” and the collection of “your general geographic location”), <https://help.netflix.com/legal/privacy>.

³⁸ See Google, *Privacy Policy* (disclosing the collection of “Internet protocol address[es]”; “device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL”; and “information about your actual location. We use various technologies to determine location, including IP address, GPS, and other sensors that may, for example, provide Google with information on nearby devices, WiFi access points and cell towers”), <http://www.google.com/policies/privacy/>.

³⁹ See Uber, *Privacy Statement* (“If you permit the Uber app to access location services through the permission system used by your mobile operating system (‘platform’), we may also collect the precise location of your device when the app is running in the foreground or background.”), <https://www.uber.com/legal/privacy/users/en/>.

telephone number, device type information, operating system, mobile device ID, specific geolocation, mobile contacts stored on John’s phone, and information about other apps stored on John’s phone.⁴⁰ In Zynga’s words, it uses the information to “manage and deliver contextual and behavioral advertising,” among other things.⁴¹ It also allows advertisers and ad networks to place ads on the app.⁴² When it does so, advertisers “may collect or we may share” performance data (relating to the number of clicks on advertisements); “aggregated and/or de-identified information”; IP address information and de-identified persistent device identifiers; social network IDs; and information relating to the use of the app.⁴³

Such marketing practices are routine on the modern Internet. Mobile operating systems enable third-party app developers to collect a range of valuable information about consumers, including:

- their unique device ID and IP address;
- their location information, including their location derived from GPS, cell towers, WiFi hotspot locations, and their use of Bluetooth;
- their call log and SMS text message history; and
- their photos, videos, contacts, and calendar.⁴⁴

The collection of such information—as noted in the examples above—can remain largely hidden from consumers, as such information is commonly collected even when an app runs only in the background.⁴⁵

⁴⁰ Zynga, *Privacy Policy*, <https://www.zynga.com/privacy/policy>.

⁴¹ *Id.*

⁴² *Id.*

⁴³ *Id.*

⁴⁴ Swire Report at 70.

⁴⁵ See Julia Angwin & Jennifer Valentino-Devries, *Apple, Google Collect User Data*, Wall St. J.

App developers often monetize such information by selling it to third-party advertisers and data brokers.⁴⁶ Unlike ISPs (*see* Section I.A.1.d, *infra*), most app developers give consumers only the most cursory notice that they are sharing such information with anyone. Their privacy notices are often included within lengthy terms of service that most consumers are unlikely to read, and they also often appear in take-it-or-leave-it form: people cannot use the app without agreeing to the terms.

Nonetheless, the information-sharing that consumers implicitly authorize when using mobile apps is a boon for consumers generally. The revenues that app developers earn from monetizing consumer data offset their costs and enable them to offer their apps to consumers either for free or at very low prices. Without a market for consumer data, consumers would likely have a much smaller and more expensive set of online services to choose from.⁴⁷ Google, for example, generates 90 percent of its total revenue from ads.⁴⁸ Without such revenue, Google would almost certainly have to charge subscription fees for services that are now free.⁴⁹

The information collected by Google and app developers dwarfs the information that Verizon—John’s mobile ISP—could even theoretically collect. Verizon is of course aware of

(Apr. 22, 2011), <http://www.wsj.com/articles/SB10001424052748703983704576277101723453610>.

⁴⁶ *Id.*

⁴⁷ *See* Joshua D. Wright, *An Economic Analysis of the FCC’s Proposed Regulation of Broadband Privacy*, at 16, 20-28 (May 27, 2016) (submitted by USTelecom in this proceeding) (“Wright White Paper”). Researchers at Cambridge University found that 77 percent of the top free applications in the Android marketplace were ad-supported. Ilias Leontiadis, *Don’t Kill My Ads! Balancing Privacy in an Ad-Supported Mobile Application Market*, Proceedings of 13th ACMM Sigmobility Workshop on Computing Systems and Applications (2012).

⁴⁸ Alphabet Inc. and Google Inc., Form 10-K, at 7 (Dec. 31, 2015) (“We generated 90% of total Google segment revenues from advertising in 2015.”).

⁴⁹ The online advertising market is only getting bigger and is projected to grow to \$220.38 billion by 2019. *See* MarketsandMarkets, *Online Advertising Market by Search Engine Marketing, Display Advertising, Classifieds, Mobile, Video, Lead Generation, Rich Media - Global Advancements, Forecasts & Analysis (2014 - 2019)*, <http://www.marketsandmarkets.com/PressReleases/online-advertising.asp>.

John’s general location with respect to its cell sites, and it likely also knows that he is communicating with Netflix servers because it must connect those servers to his phone. But Verizon has no way of knowing what John is watching because the Netflix app encrypts content with HTTPS. Nor can Verizon read the texts that John sends his friends over WhatsApp or the emails he sends over the Gmail app because those, too, are encrypted and are thus potentially visible only to Facebook and Google, respectively.⁵⁰ And of course, AT&T—John’s wireline ISP at home—has no idea where John is, what he is doing, or whether he is even online because it is no longer handling his connection to the Internet.

4. Using Facebook at a WiFi Hotspot

John heads to a local coffeehouse and connects to the WiFi network there. The coffeehouse manages that network and uses Comcast as its ISP. John accesses the Facebook app from his smartphone and posts a status update. Because he has an Android phone (and also because he has installed various Google apps), Google’s operating system can see that John has accessed the Facebook app.⁵¹ Facebook, of course, knows the contents of his post; it also has access to his device information, geolocation, and various forms of data about him collected by third-party apps and websites that have Facebook social plug-ins—including every website that has a Facebook “like” button or other plug-ins.⁵² Facebook may use any and all of this information to target ads to John based on its informed assumptions about his interests and preferences.⁵³

⁵⁰ See, e.g., Electronic Frontier Foundation, *WhatsApp Rolls Out End-to-End Encryption to its Over One Billion Users* (Apr. 7, 2016) (“End-to-end encryption has just gone massively mainstream.”), <https://www.eff.org/deeplinks/2016/04/whatsapp-rolls-out-end-end-encryption-its-1bn-users>.

⁵¹ See p. 22, *supra*.

⁵² See *supra* note 13; Facebook, *Data Policy*, <https://www.facebook.com/policy.php>.

⁵³ Facebook, *Data Policy*, <https://www.facebook.com/policy.php>.

Again, the ISP—this time Comcast—can see only that John is communicating with Facebook. It cannot see the contents of the pages he views, the status updates he posts, or the messages he sends, because Facebook—like Google, NIH, and Netflix in the examples above—encrypts its users’ communications.⁵⁴ And the other ISPs that sometimes carry John’s traffic see even less. AT&T (John’s wireline ISP) still does not know where John is or whether he is online. And because John is on a public WiFi network, Verizon is no longer responsible for connecting John to the sites he visits, although it may receive limited information from his phone simply to ensure that he can seamlessly reconnect to Verizon’s mobile network once he leaves the coffeehouse.

* * *

The above discussion illustrates why ISPs have access to a diminishing fraction of the information available to major edge providers in the Internet ecosystem: (i) the increasing tendency of consumers to switch among several ISPs over the course of the day, and (ii) the deepening prevalence of encryption. Several points warrant further emphasis before we turn to an analysis of the NPRM’s proposals.

Multiple ISP platforms per user. As the John Smith example illustrates, a typical consumer today uses several different ISPs in the course of a day, and he goes dark for each ISP when he moves from one connection to another. Like encryption, this use of multiple ISP networks substantially limits what any given ISP can learn about a given customer and belies any claim that an ISP has uniquely “comprehensive” insights into that customer’s online activities.

⁵⁴ See, e.g., Robert Hackett, *Most Internet Traffic Will Be Encrypted by Year End. Here’s Why*, Fortune (Apr. 30, 2015), <http://fortune.com/2015/04/30/netflix-internet-traffic-encrypted/>; Rachael King, *Facebook Is Working on Self-Protecting Mobile Apps*, Wall St. J. (Sept. 24, 2015), <http://blogs.wsj.com/cio/2015/09/24/facebook-is-working-on-self-protecting-mobile-apps/>.

And like encryption, this is a new and growing phenomenon, which arises mainly from consumers' increasing reliance on smartphones and the accelerating proliferation of WiFi hot spots. In 2014, an estimated 46 percent of all cellular traffic was offloaded to WiFi networks,⁵⁵ and that figure is projected to increase to 60 percent by 2020.⁵⁶

In contrast to ISPs, edge providers like Google and Facebook can track users across devices and networks because users routinely log into the same accounts on different devices and across different ISP networks.⁵⁷ Just as important, even Internet companies that (unlike Google) cannot directly track customers across the Internet can still acquire comprehensive information about those same customers from third-party data brokers like Acxiom, Epsilon and Datalogix.⁵⁸ As discussed, brokers acquire highly detailed, customer-specific information from a variety of commercial, government, and other publicly available sources. For example, they collect information relating to customer-specific “purchase data” and “web browsing activities” in addition to “bankruptcy information” and “voting registration.”⁵⁹ Data brokers combine this information to “form a composite of the consumer’s life” and then sell this information to edge providers, ad networks, and anyone else who may be interested.⁶⁰

⁵⁵ Swire Report at 25 (citing Cisco, *Cisco Visual Networking Index, Forecast and Methodology, 2014-2019 Working Paper* (May 27, 2015), http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html).

⁵⁶ *Id.* (citing Juniper, *Juniper Mobile Data Onload & Offload Report* (June 2015), <http://www.juniperresearch.com/researchstore/enablingtechnologies/mobile-data-onload-offload/wifi-small-cell-network-strategies>).

⁵⁷ The average American checks his or her social media account 17 times per day and regularly does so across different ISP networks. Swire Report at 43.

⁵⁸ *See, e.g.,* FTC, *Data Brokers* at 11-18.

⁵⁹ *Id.* at 46.

⁶⁰ *Id.*

Customer churn. ISPs' visibility into any given user's online behavior is obstructed not only because of encryption and WiFi offloading, but also because ISPs face strong competition from one another and thus continuously lose existing customers while gaining new ones. From 2012 to 2015, the reported monthly churn rate for mobile ISPs ranged from 1.44% to 1.85%, meaning that between 17.28% and 22.2% of customers switch mobile broadband ISPs *in any given year*.⁶¹ These high churn levels limit each ISP's ability to track any given consumer over time even apart from that consumer's use of multiple ISPs' networks over the course of a typical day.⁶² Contrary to the NPRM's suggestion (at ¶¶ 4, 128), this churn phenomenon affects ISPs more than leading edge providers. For example, webmail services (e.g., Gmail) and social networks (e.g., Facebook) are "stickier" from a user's perspective, tend to retain users for longer than any given ISP does, and thus have greater longitudinal visibility into their users' online profiles. See Section I.A.1.d, *infra*.

VPNs. As discussed, HTTPS encryption blocks ISPs from viewing the *content* (and detailed URLs) of a growing majority of web traffic today and enables the ISP to see only the top-level *destination* of the traffic in the form of IP addresses. But consumers increasingly use still-deeper encryption technologies that keep ISPs (as well as government agencies and hackers) from seeing even which IP addresses those consumers are visiting. The most prevalent example is "virtual private network" (VPN) technology, familiar to employees of the many organizations

⁶¹ Federal Communications Commission, *Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless, Including Commercial Mobile Services: Eighteenth Report*, ¶ 20 (Dec. 23, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DA-15-1487A1_Rcd.pdf.

⁶² As we discuss further below, the Commission has acknowledged that high churn is a "reasonable proxy" for determining that switching costs are low. See, e.g., Federal Communications Commission, *Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless, Including Commercial Mobile Services: Fifteenth Report*, ¶ 260 (June 24, 2011), https://apps.fcc.gov/edocs_public/attachmatch/FCC-11-103A1_Rcd.pdf.

that use VPNs for work-at-home applications.⁶³ An estimated 30 million people in the United States will use a VPN this year.⁶⁴ VPN technology is growing increasingly pervasive, not only because many companies require their employees to use it, but also because more and more security-conscious consumers are signing up on their own with mass-market VPN services.⁶⁵ Indeed, the FTC recommends that consumers use VPNs whenever they log onto public WiFi hotspots.⁶⁶

When someone uses a VPN, his ISP can see only his initial request for a connection to the Internet site hosting that VPN.⁶⁷ The VPN provider then holds that connection open while handling—and encrypting—all communications with other Internet destinations. In the industry jargon, VPN traffic is sent in a “secure tunnel,” which means that all such traffic, including even the user’s requests to visit particular IP addresses, is encrypted and thus unintelligible to the ISP.

⁶³ See Swire Report at 34.

⁶⁴ *Id.*

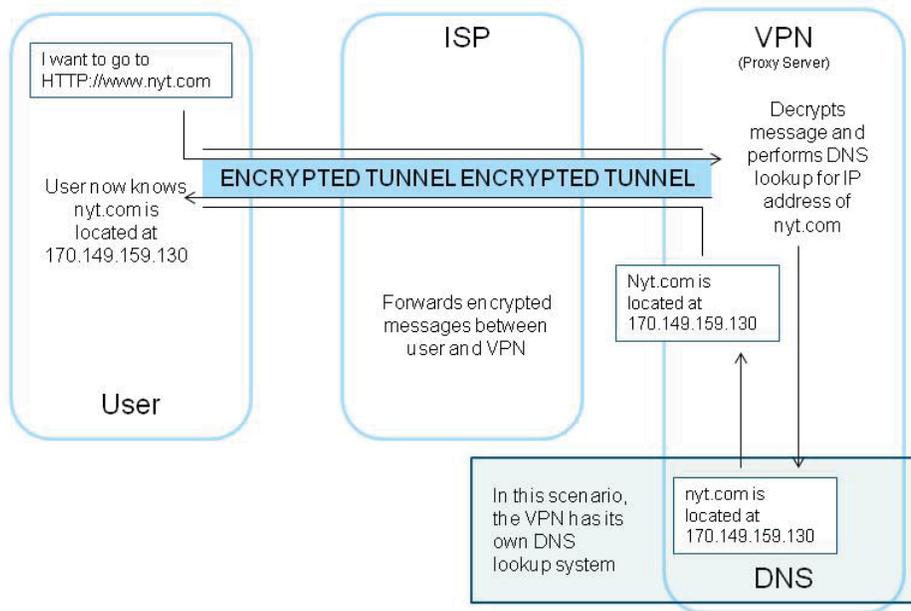
⁶⁵ See James Vincent, *Opera Just Added a Free VPN to Its Browser for Anonymous Internet Access*, The Verge (Apr. 21, 2016), <http://www.theverge.com/2016/4/21/11477036/free-vpn-opera-web-browser>; Electronic Frontier Foundation, *HTTPS Everywhere* (discussing the HTTPS Everywhere extension for Firefox, Chrome, and Opera browsers that “encrypts your communications with many major websites, making your browsing more secure”), <https://www.eff.org/HTTPS-everywhere>.

⁶⁶ See FTC, *Tips for Using Public Wi-Fi Networks* (Mar. 2014), <https://www.consumer.ftc.gov/articles/0014-tips-using-public-WiFi-networks>.

⁶⁷ See generally Swire Report at 31-35.

The ISP “sees” only that its user is making continued use of a VPN.⁶⁸

Virtual Private Networks DNS Lookup



As these technologies grow increasingly popular, they will further widen the considerable gap between what ISPs and edge providers can see in typical Internet traffic.

ARGUMENT

Since the dawn of the commercial Internet, the FTC—with the support of the federal government as a whole—has enforced a flexible but highly effective regime to govern online privacy and data security. As discussed below, that regime relies on industry best practices, avoids burdensome opt-in requirements for the mere use of nonsensitive data for marketing purposes, tailors data-security requirements to threats of actual consumer harm, and maintains technological neutrality between similarly situated providers.⁶⁹ Until a year ago, the FTC

⁶⁸ A similar diagram appears in Swire Report at 32.

⁶⁹ See generally *2012 FTC Privacy Report* (discussing FTC regime); Letter from Jon Leibowitz to the Commission, No. 16-106 (May 23, 2016) (letter from former FTC Chairman describing flexible FTC regime and urging the FCC to ensure consistency with it); Daniel J. Solove & Woodrow Hartzog, *The*

applied that regime to the Internet ecosystem at large. When this Commission reclassified broadband Internet access as a Title II “common carrier” service, however, it asserted the authority to regulate the privacy practices of broadband ISPs as common carriers.

So long as that decision stands, the Commission should ensure that any rules it adopts preserve as much substantive consistency as possible with the FTC’s longstanding regime—not only because that regime has defined the rules of the road for two decades, but also because it is a case study in regulatory success. The FTC’s regime has protected consumers from genuine privacy abuses while freeing companies like Google and Facebook to build the modern Internet ecosystem on the efficient exchange of customer information for deeply discounted (or “free”) services. It thus reflects the basic insight that, in the words of the PCAST Big Data Report, “[t]he beneficial uses of near-ubiquitous data collection ... fuel an increasingly important set of economic activities” and that any “policy focus on limiting data collection” would not strike “the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth).”⁷⁰

That is why the U.S. government, including the Obama Administration, has staunchly defended the FTC’s regime as the appropriate regulatory model for all consumer online data and has supported the development of a consistent and flexible online-privacy regime administered by the FTC. As the White House explained in proposing its 2012 Consumer Privacy Bill of

FTC and the New Common Law of Privacy, 114 Colum. L. Rev. 583, 585-86 (2014) (explaining how “FTC privacy jurisprudence is the broadest and most influential regulating force on information privacy in the United States—more so than nearly any privacy statute or common law tort”).

⁷⁰ PCAST *Big Data Report* at x-xi; Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* 39-40 (May 2014) (“*White House Big Data Report*”) (“For consumers, big data is fueling an expansion of products and services that impact their daily lives.”); 2012 *FTC Privacy Report* at 2 (noting that “the collection and use of consumer data has led to significant benefits in the form of new products and services”).

Rights, privacy law should not “treat similar technologies within the communications sector differently,” and thus “the Administration supports simplifying and clarifying the legal landscape and making the FTC responsible for enforcing the Consumer Privacy Bill of Rights against communications providers” along with all other participants in the Internet ecosystem.⁷¹ Like the U.S. government, the international community also recognizes the need for greater consistency in the regulation of communications platforms. In the words of the European Commission, regulators should “[e]nsur[e] a level playing field for comparable digital services,” subject “comparable digital services ... to the same or similar rules, duly considering opportunities for reducing the scope and extent of existing regulation,” and “simplify, modernize, and lighten existing regulation.”⁷²

The White House further endorsed the FTC’s longstanding reliance on “general principles that afford companies discretion” in how they design their privacy practices, as well as “multistakeholder process[es] to produce enforceable codes of conduct” that industry can voluntarily incorporate into privacy policies.⁷³ The White House added that such multistakeholder processes are not only “different from traditional agency rulemakings,” but superior to them in this context because, unlike regulations prescribed by “a single, centralized authority,” multistakeholder processes “provide the flexibility, speed, and decentralization necessary to address Internet policy challenges.”⁷⁴ And the White House similarly emphasized

⁷¹ The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at 39 (2012) (“*White House Consumer Privacy Bill of Rights*”) (footnote omitted).

⁷² European Commission et al., *Online Platforms and the Digital Single Market* (May 25, 2016), <https://ec.europa.eu/digital-single-market/en/news/communication-online-platforms-and-digital-single-market-opportunities-and-challenges-europe>.

⁷³ *White House Consumer Privacy Bill of Rights* at 2.

⁷⁴ *Id.* at 23-24.

that command-and-control privacy regulation would ultimately harm consumers because it would deprive industry of needed flexibility and initiative, and “both companies and consumers benefit when companies commit to the task of innovating privacy practices.”⁷⁵

Nothing has changed to justify either a departure from the FTC’s time-tested regime or substitution of top-down regulation in place of the private initiative and multistakeholder processes the White House has lauded. The NPRM, however, proposes to reinvent much of federal privacy policy from scratch and radically increase the level of regulatory micromanagement while paying mere lip service to the FTC’s approach. Unless substantially revised, the new rules would impose needless costs on broadband providers, reduce the profitability of broadband service to ISPs, and exert upward pressure on broadband prices. And they would accomplish nothing to protect consumer privacy because, under the FTC’s more flexible regime, all non-ISP actors will continue collecting and using all the same customer information the Commission’s rules would irrationally hamstring ISPs from using. The proposed rules would thus violate a cardinal principle of administrative law: they would reject a well-functioning regulatory regime in favor of a radically more burdensome one without any empirical basis for concluding that any industry problem required the shift.⁷⁶

Two threshold points encompass many of the issues in this proceeding and thus warrant emphasis up front. First, the relevant question here is not whether ISP privacy and data-security

⁷⁵ *Id.* at 24.

⁷⁶ *See, e.g., Nat’l Fuel Gas Supply Corp. v. FERC*, 468 F.3d 831, 843 (D.C. Cir. 2006) (“Professing that an order ameliorates a real industry problem but then citing no evidence demonstrating that there is in fact an industry problem is not reasoned decisionmaking.”); *Fox TV Stations v. FCC*, 280 F.3d 1027, 1051 (D.C. Cir. 2002) (“A single incident . . . —and one that seems to have been dealt with adequately under [existing] rules—is just not enough to suggest an otherwise significant problem”); *Associated Gas Distribs. v. FERC*, 824 F.2d 981, 1019 (D.C. Cir. 1987) (agency lacks any basis for fashioning “an industry-wide solution for a problem that exists only in isolated pockets,” and “the disproportion of remedy to ailment” is therefore arbitrary and capricious).

practices should be subject to oversight at all. AT&T supports the substantive principles outlined in the Industry Framework, which would subject ISPs to a regime similar to the FTC's.⁷⁷ The Commission also should recognize the well-established body of state privacy laws as well as general privacy guidelines developed by industry bodies and multistakeholder processes.⁷⁸ Instead, the relevant question is whether—as the NPRM proposes—ISPs should be subject to *much more burdensome* regulation than the FTC and states apply to all other actors in the Internet ecosystem. Precisely framed, therefore, the basic cost-benefit question here is this: what benefits, if any, can be gained from subjecting ISPs to the major incremental burdens that the proposed regime would add to the baseline FTC-type regime; and would the costs of those incremental burdens outweigh those asserted benefits? On a wide range of issues, the NPRM's proposals flunk that cost-benefit analysis.

Second, many—but by no means all—of the proposed rules' flaws stem from their overbroad application to almost all of the customer information in an ISP's possession, not just the sensitive information. Part IV below explains why the statutory scheme does not permit the Commission to sweep non-CPNI information within its proposed regime. But quite apart from that legal constraint, the proposed rules defy common sense because they would treat nonsensitive information categories, such as simple subscriber names and addresses unaccompanied by any sensitive context, as though they were in fact highly sensitive data. No other agency has ever treated such information that way under any other U.S. privacy regime. Including such information within the Commission's proposed privacy framework would give

⁷⁷ See NPRM ¶¶ 280-282.

⁷⁸ See generally Digital Advertising Alliance, *Self-Regulatory Principles for Online Behavioral Advertising Implementation Guide* (Oct. 2010); Network Advertising Initiative, *2015 Update to the Code of Conduct* 3 (2015).

rise to a host of absurd policy consequences, from restricting ISPs from marketing on the basis of their own customer lists to characterizing millions of innocuous events as reportable “data breaches.”

I. THE PROPOSED MARKETING RESTRICTIONS FAIL ANY REASONABLE COST-BENEFIT ANALYSIS

A. The Proposed Asymmetric Marketing Burdens Are Irrational and Unnecessary to Serve Consumer Privacy Interests

Any new proposal to restrict innovative uses of customer data for marketing purposes must confront several realities about the American economic and legal landscape. First, information is the lifeblood of the modern American economy. As with “other essential factors of production such as hard assets and human capital, ... much of modern economic activity, innovation, and growth simply couldn’t take place” without the collection and use of consumer data.⁷⁹ Second, the genie is out of the bottle. No matter what the Commission does in this proceeding, major actors in the Internet ecosystem will continue to track and use all of the same information the proposed rules would keep ISPs from efficiently tracking and using. Third, Supreme Court precedent forbids either excessive or underinclusive provider-specific burdens on commercial speech.

The FTC—long the federal government’s preeminent privacy enforcer—has taken these concerns to heart by developing a flexible privacy regime that is based on consumer welfare principles and thus emphasizes two key variables of particular importance to consumers: (1) is the consumer information at issue especially *sensitive* (e.g., financial or medical data), and (2) is it *shared* with third parties?⁸⁰ That context-specific approach targets objectionable and

⁷⁹ McKinsey Global Institute, *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, at iv (2011).

⁸⁰ *2012 FTC Privacy Report* at 15-16.

potentially harmful uses of consumer data while avoiding interference with the efficient, value-generating use of consumer data in contexts that do *not* involve sensitive data and third-party sharing.⁸¹

For example, under the FTC’s longstanding practice, “most first-party marketing practices are consistent with the consumer’s relationship with the business and thus do not necessitate consumer choice,” even in the form of opt-out consent.⁸² As a result, when a company such as Amazon, Google, or Apple seeks to expand the range of branded services it offers its own existing customers, it does not trigger any consent requirement at all under the FTC’s framework (although such companies may well offer opt-out as a matter of company

⁸¹ Unless otherwise indicated, the term “third party” in these comments means third-party advertisers and similar non-agent third parties. At a minimum, the Commission should amend its proposed Rule 64.7002(e)(2) to clarify that it does not intend to prohibit ISPs from sharing customer PI with its agents, as is currently permitted by its existing CPNI rules. *See* 47 C.F.R. § 64.2007(3)(b) (“A telecommunications carrier may, subject to opt-out approval or opt-in approval, disclose its customer’s individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, *to its agents* and its affiliates that provide communications-related services.”) (emphasis added). Failing to allow ISPs to share information with agents (based on opt-out approval) would be arbitrary and irrational because it would hamper ISPs’ ability to market their services on a cost-effective basis. Indeed, ISPs and their agents would need to engage in even more sharing than before of information covered by the Commission’s privacy rules if, as proposed, that category is expanded to include customer name and address (e.g., mailing vendors) and other non-sensitive information. At the same time, prohibiting ISPs from sharing information with agents is not necessary to protect the confidentiality of customer information, as those agents will have the same obligation to protect the customer information and ISPs are subject to vicarious liability for the acts of their agents. *See* Section III.C, *infra*.

⁸² *2012 FTC Privacy Report* at 40 (emphasis added). Section 222 exempts carriers from any need to obtain consumer consent (either opt-in or opt-out) when, *inter alia*, they “use, disclose, or permit access to” individually identifiable CPNI in the provision of “the telecommunications service from which the information is derived” or of “services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.” 47 U.S.C. § 222(c)(1); *see also* *NPRM* ¶¶ 111-121 (discussing circumstances where customer consent is implied). To the extent the proposed rules would permit an ISP only to “use” information in this category, and not also “disclose” or “permit access to” it, they would flatly violate Section 222(c)(1). *See NPRM* p. 108 (Proposed Rule 64.7002(b)). Apart from that observation and other respects in which the proposed rules would violate Section 222(c)(1), *see* Section I.B.4, *infra*, these comments do not focus on the category of information for which consent is implied. Instead, these comments focus on whether consent mechanisms should take the form of opt-in or opt-out.

policy). And the FTC takes a similarly flexible approach to third-party marketing that, like most of the ISP third-party marketing at issue here, involves no sharing of customer-specific information with third-party advertisers (see below).⁸³ These background rules have worked well for two decades. They have informed the corporate policies of companies throughout the Internet ecosystem, including any ISPs to which they applied until last year’s reclassification decision. And they have both reflected and shaped consumer expectations about the handling of personal information on the modern Internet.

The NPRM now proposes a radical break from those two decades of consensus. The proposed rules not only would require notice-and-choice for first-party ISP marketing, but also would subject most such marketing to the most speech-restrictive notice-and-choice regime—opt-in—even when an ISP merely *uses* (without sharing) *nonsensitive* customer-specific data already in its possession. To that general opt-in requirement for marketing uses, the Commission would recognize only a single exception for the first-party marketing of “communications-related services,” which the Commission proposes to construe narrowly. This is a radical proposal. Shifting to opt-in slashes the amount of data that can be productively used for pro-consumer purposes, not because that is what consumers want, but because the transaction costs and externalities of an opt-in regime create market failures where the presumption against data-sharing is misaligned with consumer values. *See* Section I.B, *infra*.⁸⁴ As discussed below, any generalized opt-in requirement would stop the Internet economy in its tracks if it were broadly applied, and the NPRM’s single-minded “focus on limiting data collection” strikes exactly the

⁸³ Specifically, the FTC does not require any consent mechanism (opt-in or opt-out) when non-sensitive consumer information is used for third-party marketing, except where users are tracked on third-party websites. *See 2012 FTC Privacy Report* at 59-60.

⁸⁴ *See also* Wright White Paper at 14, 19-20.

wrong “balance between beneficial results and unintended negative consequences (such as inhibiting economic growth).”⁸⁵

In short, with very limited exceptions, the NPRM proposes to subject ISPs to much more restrictive opt-in requirements for the use of *any* customer-specific information for *any* marketing of new products, even where the information is nonsensitive and is shared with no third parties. That proposal is as irrational as it is irreconcilable with two decades of consensus federal policy. It would create no discernible consumer benefit, as discussed in this subsection, and it would nonetheless inflict substantial costs in the form of consumer confusion, competitive distortions, and lost efficiency and innovation, as discussed in Section I.B below. Finally, as discussed in Section IV, it would also violate core First Amendment protections for commercial speech.

1. *The NPRM Identifies No Valid Basis for Subjecting ISPs to More Onerous Notice-and-Choice Restrictions than Non-ISPs, and the Proposed Opt-In Rules Are Irrationally Overbroad*

The NPRM acknowledges that, by requiring opt-in consent for most ISP marketing activities, its proposed notice-and-choice regime would single ISPs out for special regulatory burdens and that those burdens must be justified. In its words, “edge providers, who may have access to some similar [consumer data], are not subject to the same regulatory framework [as proposed in the NPRM], and . . . this regulatory disparity could have competitive ripple effects.”⁸⁶ The NPRM nonetheless cites several “important factors” that, it says, would “mitigate” the ISP-specific burdens its asymmetric regulation would impose.⁸⁷ And the NPRM likewise contends (*id.* ¶ 128) that considerations of market power and “switching costs” justify

⁸⁵ *PCAST Big Data Report* at x-xi.

⁸⁶ *NPRM* ¶ 132.

⁸⁷ *Id.*

special burdens for ISPs. But all of these cited factors in fact illustrate why, to the contrary, it would make no sense to regulate ISPs more restrictively than all other actors in the Internet ecosystem.

a. Continued FTC oversight of non-ISP actors. Among its “mitigat[ing]” factors, the NPRM first observes that “the FTC actively enforces the prohibitions in its organic statute ... against companies in the broadband ecosystem that are within its jurisdiction and that are engaged in practices that violate customers’ privacy expectations.” *Id.* ¶ 132. But that is a reason to subject ISPs to the same basic principles that, for decades, the FTC has enforced against all other “companies in the broadband ecosystem.” It is not a basis for subjecting ISPs to much more onerous rules than the FTC applies to everyone else. Again, the central question in this proceeding is not whether ISP privacy practices should be overseen at all, but whether they should be regulated far more intrusively than every other online company’s privacy practices.

b. Industry consensus on the use of opt-in for the sharing of sensitive information. As its second “mitigat[ing]” factor, the NPRM notes that “the industry has developed guidelines recommending obtaining express consent before sharing some sensitive information” and that “large edge providers are increasingly adopting opt-in regimes for sharing of some types of sensitive information.” *Id.* But that observation cuts sharply against the proposed rules, not for them. It underscores the broad consensus that different consent rules should apply to the “sharing of sensitive information” than to the use of all other information. In contrast, the proposed rules would impose a one-size-fits-all approach to most ISP uses of any customer information, whether or not the information is sensitive or shared with third parties.

No one disputes that an opt-in mechanism is generally appropriate for sharing information the FTC has long flagged as particularly sensitive—“information about children,

financial and health information, Social Security numbers, and precise, individualized geolocation data” (as opposed to the less granular geolocation data available through cell tower triangulation or subscriber zip codes).⁸⁸ By the same token, no one has seriously contended until now that opt-in, with all its attendant social costs (discussed in Section I.B below), is appropriate for the vast majority of information that is not sensitive, particularly if it is not even shared with third parties. That is why, under the FTC’s approach, companies face no opt-in requirements at all when, on the basis of nonsensitive but customer-specific information, they engage in any type of first-party or third-party marketing that involves no disclosure of such information to third-party advertisers.⁸⁹ The proposed rules, however, would subject ISPs to an opt-in requirement for any use of customer data, no matter how nonsensitive, for (1) any first-party marketing of services deemed “non-communications-related” and (2) any third-party marketing of any kind, even where the ISP shares no information with the third-party advertiser. The NPRM even asks (at ¶ 165) whether the Commission should require “opt-in” when an ISP uses completely de-identified data. These proposals are breathtaking in their scope; are indefensible as both a policy and a legal matter (see also Section IV, *infra*); and, for good reason, have no precedent in any other U.S. agency’s privacy regime.

As an initial matter, the proposed distinction between “communications-related” and “non-communications-related” services is an anachronism and should be abolished. The

⁸⁸ 2012 *FTC Privacy Report* at 58; see also *The Two Towers: The Abuse of Mobile-Phone Data*, *The Economist* (Sept. 6, 2014) (“Routinely collected tower data can place a mobile phone in a broad area, but it cannot ‘pinpoint’ it.”), <http://www.economist.com/news/united-states/21615622-junk-science-putting-innocent-people-jail-two-towers>.

⁸⁹ 2012 *FTC Privacy Report* at 55-57, 58-60. For simplicity of discussion, we use the term “ISP” to denote an ISP and its corporate affiliates and “third party” to denote a company unaffiliated with an ISP. All corporate affiliates should qualify as such, particularly if the affiliate relationship is made clear to consumers, whether through branding, marketing activities, or otherwise. See *NPRM* ¶ 19.

Commission first drew that distinction in 2002 to reflect its intuitions about what ads consumers expected to receive from conventional telephone companies.⁹⁰ But whatever merit that distinction might have had for subscription-oriented telephone industry of 2002, it has no basis in consumer expectations about today’s broadband Internet ecosystem, which is dominated by ad-supported services. Countless consumer-facing participants in that ecosystem routinely contact their existing customers with a range of first-party and third-party ads. Consumers are accustomed to seeing such online ads whenever they use the Internet. And a consumer would be no more surprised to see an ad promoting his or her ISP’s home-alarm ad system than a Gmail user would be to see an ad for the Google Photos cloud-storage service.⁹¹

Inexplicably, however, the NPRM proposes not only to retain the limiting category of “communications-related services” but to narrow it further—and thus enlarge the scope even of first-party advertising that is subject to the opt-in requirements.⁹² For example, depending on how the proposal is implemented, ISPs might be subject to opt-in consent requirements whenever they wish to use their customers’ names and email addresses simply to market their own branded home-alarm system, their own branded mobile applications, a newly introduced smartphone offered in conjunction with their wireless plans, and perhaps even their branded

⁹⁰ 2002 CPNI Order ¶¶ 36, 51, 66. Specifically, the Commission found that “telecommunications consumers expect to receive targeted notices from their carriers about innovative telecommunications offerings that may bundle desired telecommunications services and/or products, save the consumer money, and provide other consumer benefits.” *Id.* ¶ 36.

⁹¹ Consumers may opt out of receiving marketing messages from AT&T by clicking an “unsubscribe” link in emails or texting “stop” in response to a text message. *AT&T Privacy Policy* (July 24, 2015), https://www.att.com/Common/about_us/privacy_policy/print_policy.html. Consumers may opt out of receiving targeted online advertisements, as with Google, through their accounts. *Id.*; see also Google, *Privacy Policy* (Mar. 25, 2016), <https://www.google.com/policies/privacy/>.

⁹² See NPRM ¶¶ 18, 71.

over-the-top VoIP or video-streaming services.⁹³ The NPRM does not actually try to justify this proposal; instead, it notes only (at ¶ 72) that the Commission does not wish to allow ISPs to offer “a broad array of services” on an opt-out basis and thus “seek[s] comment on how we might ... narrow the scope of services we would treat as ‘communications-related services.’” But that is no explanation at all; it is simply a declaration of animus toward ISPs and their ability to market their own products.

In fact, no plausible explanation exists. The proposal to require restrictive opt-in rules for first-party advertising of “non-communications-related” services rests on an untenable premise: that consumers are somehow more surprised or distressed when a company with whom they already do business sends them first-party ads for branded services that are (arguably) unlike—rather than similar to—the services they already buy from that company. But the NPRM cites no evidence that consumers react this way to different types of first-party marketing, whether by ISPs or anyone else. In particular, the two Pew Research Center reports cited repeatedly by the NPRM supply no such evidence.⁹⁴ Instead, they show at most that consumers sometimes object when they learn that their existing providers *share* their personal information with third-party advertisers. By definition, that is not what happens in first-party advertising. That is why the FTC exempts first-party advertising from its notice-and-choice framework altogether unless it involves the otherwise unnecessary collection of sensitive information.⁹⁵

⁹³ See *id.* ¶ 18 (proposing to exclude “edge services” from the “communications-related” category); *id.* ¶ 71 (asking whether to “limit communications-related services to telecommunications, cable and satellite services regulated by the Commission”).

⁹⁴ See *id.* ¶¶ 109, 123, 129 (citing Mary Madden & Lee Rainie, Pew Research Center, *Americans’ Attitudes About Privacy, Security and Surveillance*, at 4 (2015); Lee Rainie & Dana Page, Pew Research Center, *Privacy and Information Sharing*, 5-6, 20, 23-25 (Jan. 14, 2016)).

⁹⁵ See *2012 FTC Privacy Report* at 40-48.

For similar reasons, the NPRM is on no firmer ground when it proposes a categorical opt-in requirement for all *third-party* marketing as well. The NPRM appears to overlook a key feature of such marketing (*e.g.*, ¶ 129): it often does not involve any sharing of individually identifiable customer information with the third-party advertiser. Consider the typical third-party ad a user might see after he logs into Gmail from a desktop computer and sends a friend an email asking whether she’s enjoying the Prius she just bought. Based on the words in that email, Google might deliver, on the user’s Gmail homepage, an ad for a local Toyota dealership.⁹⁶ But Google has not told the dealership who is sending this email and therefore receiving the ad. Instead, it has simply contracted to deliver ads to specific customers who use designated keywords in their emails. The dealership might receive aggregate customer information so that it knows (for example) how many people received its ads, but it could not trace that information to specific potential customers.

Like countless edge providers, AT&T and other ISPs conduct or plan to conduct analogous (but even less intrusive) third-party advertising, which does not involve transferring individually identifiable customer information to third-party advertisers. For example, an ISP might contract to send ads to its customers who have billing addresses in zip codes near a local merchant, and it might tell the merchant how many customers it reached without disclosing their individual identities.⁹⁷ Such practices are even more benign than Google’s use of Gmail for

⁹⁶ Google offers an opt-out for targeted advertisements. But even for users that opt out, “Google will still scan ... your email with our automated processing.” See *How Gmail Ads Work*, <https://support.google.com/mail/answer/6603?hl=en>.

⁹⁷ An ISP might also obtain information about its customers from third parties (*e.g.*, data brokers) and combine it with its own customer data to increase the relevance of its first- and third-party advertising. There is no discernible basis for restricting an ISP’s ability to use third-party information in that manner: that information is already freely available on the market, and the ISP’s use of it does not result in any sharing of ISP-derived information with third parties. *Cf. NPRM* ¶ 138 (seeking comment on this issue).

behavioral third-party advertising. Google scans its users' private emails and targets third-party ads to them on the basis of *those emails' actual content*, whereas the ISP in our example uses more general information to convey its own third-party ads. But the important point is that neither Google nor the ISP has shared any of this information with the advertisers, and neither has triggered the third-party sharing concern highlighted in either the Pew reports or the FTC's privacy regime. Against that backdrop, it would make no sense to subject the ISP, but not Google, to a categorical opt-in requirement for uses of customer data for third-party advertising.

c. Breadth of Access to Customer Information. In its next effort to justify the proposed "regulatory disparity," the NPRM argues (at ¶ 132) that "edge providers only have direct access to the information that customers choose to share with them," whereas broadband providers supposedly "have direct access to potentially *all* customer information[.]" As discussed at length in the Technical Background, however, this claim gets the facts exactly backwards. Even if they try to use deep packet inspection, ISPs cannot read encrypted communications, which account for a rapidly increasing majority of Internet traffic, and thus have no way of seeing the information that users send to encrypted Internet sites or which particular webpages or other content they receive back. *See* Tech. Background, *supra*. For example, when someone types "how can I avoid opiate addiction" into Google's search engine or browser, or emails that same question to a friend from his Gmail account, Google knows the person asking the question is concerned about opiate addiction, but the ISP can know only that he has used one of Google's services.

On top of that, and contrary to the NPRM's assumption, any given ISP today handles only a portion of a typical subscriber's Internet traffic and can know nothing at all about a subscriber's online activities handled by some other ISP. *See* Tech. Background, *supra*. Again,

a home Internet provider cannot see what a customer does over a cellular network or a public WiFi network, and the providers of those other networks have similarly limited visibility. In contrast, Google (much like other edge providers) can track someone's activities continuously if she remains logged into one of Google's services, such as Gmail or Google Maps, or if she uses Google Chrome as her Internet browser, or insofar as she uses an Android phone, whose operating system may report a variety of user information back to Google. *See* pp. 21-25, *supra*. The Commission cannot plausibly justify regulating ISPs more stringently than Google on the theory that they have access to "all customer information" (*NPRM* ¶ 132), for that is likely true of Google but not of them.

The *NPRM* is also flatly wrong to suggest (at ¶ 256) that the FTC's *2012 Privacy Report* supports the proposition that ISPs are "uniquely situated" for these purposes. In fact, the FTC there explained that "ISPs are just one type of large platform provider" with access to customer information; that "operating systems and browsers" such as Android and Chrome are also large platform providers and "may be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles"; and that consumers "might have limited ability to block or control such tracking" unless, for example, they take the extraordinary step of "changing their operating system."⁹⁸ The FTC made those observations four years ago, even before the rapid rise of default encryption blocked ISPs, but not operating systems and browsers, from access to most user activity on the Web. Equally important, the FTC emphasized "that any privacy framework should be technology neutral" as between these types of "large platform

⁹⁸ *2012 FTC Privacy Report* at 56.

provider[s].”⁹⁹ In short, the FTC’s *Privacy Report* warns against, rather than supports, the very type of asymmetrical regulatory scheme proposed here.

d. Competition, switching costs, and responsiveness to customer preferences. Finally, the NPRM suggests that ISPs should be subject to asymmetrically burdensome privacy rules on the theory that they, unlike edge providers, face a “lack of competition,” enjoy “high switching costs,” and thus have insufficient business “incentives” to respond to customer privacy preferences.¹⁰⁰ In these respects, too, the Commission has turned the realities of the modern Internet on their head.

AT&T and others have submitted voluminous broadband competition data to the Commission in a variety of recent proceedings.¹⁰¹ As these submissions explain, both fixed and mobile ISPs face substantial competition for retail customers, and that competition is particularly intense in the mobile broadband marketplace. This is not surprising. As anyone with a television knows, mobile providers such as T-Mobile, Sprint, Verizon, and AT&T bombard consumers with heavily marketed inducements to defect from one to another. They spend hundreds of millions of dollars annually on advertising precisely because consumers routinely switch providers and find it easy to do so. In fact, the churn rates for mobile ISPs are quite high:

⁹⁹ *Id.*

¹⁰⁰ NPRM ¶ 128; *see also id.* at ¶ 262 (citing “lack of competition” among ISPs and “switching costs” as proposed bases for denying consumers the right to accept lower broadband prices for greater information uses).

¹⁰¹ *See, e.g.,* Comments of AT&T, *In the Matter of Expanding Consumers’ Video Navigation Choices*, MB Docket No. 16-42 (Apr. 22, 2016); Comments of AT&T, *Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993*, WT Docket No. 15-125 (June 29, 2015); Comments of AT&T, *In the Matter of Protecting and Promoting the Open Internet Framework for Broadband Internet Services; Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless, Including Commercial Mobile Services*, GN Docket No. 14-28 (July 15, 2014). We incorporate those filings by reference and are submitting them in this docket.

as discussed, between 17.2 and 22.2 percent of mobile customers switch providers in any given year. *See* p. 28, *supra*.¹⁰²

In contrast, consumers may find it much more difficult to abandon leading edge providers if they dislike some aspect of *their* privacy policies. First, switching operating systems typically means switching devices (e.g., replacing an Android-based Samsung with an iOS-based iPhone), and that not only costs money, but often requires the consumer to abandon many of the apps and much of the data on the old phone. Second, unlike physical telecommunications networks, social networks are not typically interconnected with one another, which means that the largest ones benefit from enormous network effects. A typical consumer would find it far easier to switch from Sprint to another mobile provider than to cancel his Facebook account in favor of some other social network because doing the latter would require severing virtual connections with hundreds of friends and acquaintances. Third, unlike telephone numbers, email addresses are non-portable. As a result, a customer that has used a Gmail address for any length of time may encounter switching costs if she contemplates canceling that service because she dislikes some aspect of Google’s privacy policy.¹⁰³ Among other things, she will need to reach out to her contacts to inform them that her email address has changed, and they may continue sending emails to her at the “wrong” address and assume that she received them.

¹⁰² The NPRM suggests that an ISP’s supposed “position as gatekeeper” for Internet traffic may have some bearing on the issues presented here. *See NPRM* ¶ 128 n.223 (quoting *Open Internet Order* ¶ 81). It does not. Even in the limited contexts where it applies, this “gatekeeper” (or “terminating access monopoly”) concept addresses only the supposed ability of carriers to charge high interconnection rates to entities that are *not* its customers: interconnecting carriers. *See* Jonathan Nuechterlein & Christopher Yoo, *A Market-Oriented Analysis of the “Terminating Access Monopoly” Concept*, 14 COLO. TECH. J. 21 (2015). That concept has nothing to do with the retail competition that forces any carrier to deal fairly with *its own customers*.

¹⁰³ *Open Internet Order* ¶ 330 (recognizing “subscribers today rely heavily on third-party services, such as email and social networking sites, even when such services are included as add-ons in the broadband Internet access provider’s service”).

Fourth, Google and other major edge providers have far more market power in a range of relevant markets than any given ISP does in the mobile broadband marketplace. For example, Google accounts for approximately two-thirds of the U.S. search market¹⁰⁴ and more than half of the U.S. mobile operating system market,¹⁰⁵ whereas the largest mobile ISP—Verizon—accounts for only 38% of mobile consumers nationwide.¹⁰⁶ Finally, Google not only controls large shares of various individual markets—search, webmail, browsers, and mobile operating systems—but assembles all of the information it obtains from each of those markets to maintain its current role as the world’s unrivalled observer and collector of consumer information.¹⁰⁷

In short, there is no plausible basis for finding that, in general, consumers have less choice among ISPs than among leading edge providers or that switching from one ISP to another is more difficult than switching from one leading edge service to its closest rival. In a variety of familiar contexts, the opposite is true, and consumers motivated by privacy concerns have, if anything, far greater opportunities to defect to their ISP’s rival than to their edge provider’s rival.

That is a key reason why ISP privacy policies rank among the most robust and consumer-friendly in the Internet ecosystem—and why the NPRM’s proposed notice requirements (¶¶ 82-102) are thus unnecessary to promote transparency. Unlike many edge providers, ISPs maintain explicit, long-term contractual relationships with their customers, and their privacy policies are

¹⁰⁴ ComScore, *August 2015 U.S. Desktop Search Engine Rankings* (Sept. 16, 2015), <https://www.comscore.com/Insights/Market-Rankings/comScore-Releases-August-2015-U.S.-Desktop-Search-Engine-Rankings>.

¹⁰⁵ ComScore, *December 2015 U.S. Smartphone Subscriber Market Share* (Feb. 4, 2016), <https://www.comscore.com/Insights/Rankings/comScore-Reports-December-2015-US-Smartphone-Subscriber-Market-Share>.

¹⁰⁶ Federal Communications Commission, *Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless, Including Commercial Mobile Services: Eighteenth Report*, tbl.II.C.2 (Dec. 23, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DA-15-1487A1_Rcd.pdf.

¹⁰⁷ See Comments of AT&T, Decl. of Michael Kearns, *In the Matter of Expanding Consumers’ Video Navigation Choices*, MB Docket No. 16-42, at 4-9 (Apr. 22, 2016).

central to those relationships.¹⁰⁸ These ISP privacy policies clearly set forth what information ISPs collect and how it is used.¹⁰⁹ And whereas many edge providers present consumers with take-it-or-leave-it privacy notices,¹¹⁰ ISPs give consumers real choice and entitle them to opt out of particular information-use practices and nonetheless receive service. AT&T, for example, enables its customers to opt out of relevant advertising; receipt of marketing mail, emails, or calls; and use of anonymous and aggregate data for marketing purposes.¹¹¹

Finally, even if the Commission had some plausible basis for singling out ISPs on the basis of competition or high switching costs, it would still have no logical reason to subject ISPs to different *substantive privacy standards*. If ordinary market pressures were insufficient to make ISPs respect the privacy standards that prevail elsewhere in the Internet ecosystem, the proper regulatory response would be to ensure that ISPs do in fact follow those standards, not to subject ISPs to different and more burdensome standards. By analogy, when local exchange competition is inadequate to keep rates at competitive levels, the Commission has concluded that the proper regulatory response is to cap rates at those levels—not to force rates below those levels.¹¹²

¹⁰⁸ See, e.g., AT&T, Inc., *AT&T Privacy FAQ* (July 24, 2015), <http://www.att.com/gen/privacy-policy?pid=2506>; Comcast Cable Communications, LLC, *Privacy Policy* (Oct. 2015), <http://my.xfinity.com/privacy/2015-10/#full>; Verizon, *Privacy Policy* (Dec. 2015), <http://www.verizon.com/about/privacy/full-privacy-policy>.

¹⁰⁹ See, e.g., AT&T, Inc., *AT&T Privacy FAQ*, <http://www.att.com/gen/privacy-policy>.

¹¹⁰ See, e.g., eBay, User Privacy Notice (May 1, 2015) (“By using our Services and/or registering for an account with us, you are accepting the terms of this Privacy Notice and our User Agreement, and you are consenting to our collection, use, disclosure, retention, and protection of your personal information as described in this Privacy Notice.”), <http://pages.ebay.com/help/policies/privacy-policy.html>.

¹¹¹ See, e.g., AT&T, Inc., *AT&T Privacy FAQ*, <http://www.att.com/gen/privacy-policy>.

¹¹² See First Report & Order, *Implementation of the Local Competition Provisions of the Telecommunications Act of 1996*, 11 FCC Rcd 15,499, ¶ 679 (1996) (subsequent history omitted) (designing network-element leasing rates to “replicate[], to the extent possible, the conditions of a competitive market”).

2. *The Proposed Opt-In Rules Would Serve No Genuine Privacy Interest Because Non-ISP Actors Exempt from Those Rules Would Continue Using the Same Information ISPs Would Be Restricted from Using*

Even if asymmetric regulation could be justified by some relevant distinction between ISPs and non-ISP actors, such regulation would still accomplish nothing for consumers because all of those unregulated non-ISP actors would still be subject to the same flexible FTC-style regime as before and would go on collecting and using all of the same information the rules would inefficiently restrict ISPs from using.

As discussed in the Technical Background, edge providers such as Google have extensive information that ISPs lack about any given individual's online activities, whereas ISPs have little or no information about their users that edge providers do not also have. In other words, the user information that ISPs can even theoretically "see" is essentially a subset of the user information that edge providers "see." Thus, even if the proposed opt-in rules could be justified in a hypothetical world where ISPs were the only ones collecting and using online information, the rules still cannot be justified in *this* world, where, no matter what this Commission does, every non-ISP participant in the online advertising marketplace will continue collecting and using exactly the same information that the rules would restrict ISPs from using.

Against this backdrop, it is puzzling that the NPRM asks (at ¶ 213) whether the Commission "should require mobile [ISPs] to use their contractual relationship with mobile device or mobile operating system (OS) manufacturers" to obtain broad confidentiality guarantees on behalf of end users, including "limit[s] on] the use and disclosure of customer PI." Is the NPRM proposing to force mobile ISPs to exclude Android devices from their networks until Google abandons the data-fueled business model underlying the Android platform and its

1.6 million apps?¹¹³ If so, the proposal would severely disrupt the Internet ecosystem. Simply by performing their assigned functions, ISPs give operating systems, edge providers, and app developers (among others) access to a broad range of user-specific information, such as originating and destination IP addresses, call and text logs, and, in the case of mobile ISPs, cellsite-based geolocation information. The Commission would destabilize the commercial Internet if, through the contemplated contractual requirements, it used its asserted authority over ISPs to keep Google and other third-party providers from collecting and using this information on the same terms as before. On the other hand, if the NPRM is *not* proposing to alter the data practices of non-ISP entities, its overall proposal achieves nothing. Once released into the broader ecosystem, ISP-conveyed customer information is used and exchanged by countless online companies for marketing purposes, and it would make no sense to constrain how *ISPs themselves* can use that information once they set it loose to keep the Internet functioning as designed.

B. The Proposed Marketing Restrictions Would Suppress Competition, Reduce Innovation, and Impose Costs Disproportionate To Any Benefits

The proposed marketing restrictions not only would fail to create any appreciable privacy benefits, but would affirmatively harm consumers by disrupting the basic economics of the Internet ecosystem. As discussed, information is the lifeblood of the modern economy. Google, Facebook, and other Internet pathbreakers have created immeasurable value by offering their billions of customers free access to vast quantities of shared information. Google and Facebook could not offer consumers the free and widely available services they do if, by imposing a general opt-in rule, regulators had created systemic friction between consumers and efficient

¹¹³ See Statista, *Number of Apps Available in Leading App Stores as of July 2015*, <http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/>.

marketing uses of their information. Either those services would not exist at all or they would exist only in more limited forms and for substantial fees, used by only a tiny fraction of the customer base each company now boasts.¹¹⁴ As former FTC Commissioner (and now Professor) Joshua Wright explains in a white paper submitted today in this proceeding, if the government now imposed on the Internet ecosystem at large the type of notice-and-consent rules the NPRM contemplates here, it would slam the brakes on the modern Internet ecosystem, causing the economy incalculable damage in the process.¹¹⁵ Again, in the words of the PCAST Big Data Report, “a policy focus on limiting data collection will not be ... likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth).”¹¹⁶

Obviously, consumers as a whole would not intend these consequences even though their individual failures to opt in would have produced them. That fact illustrates the market failure that flows from any opt-in regime that is misaligned with consumer expectations.¹¹⁷ Such a regime inaccurately presumes, as its explicit default rule, that most consumers do *not* wish to have their information used for marketing purposes, no matter how nonsensitive that information may be. That default rule creates a systemic bias against efficient information-sharing. It requires that, before data can be shared, consumers must first stop what they are doing and digest

¹¹⁴ See Wright White Paper at 6-9; 2014 White House Big Data Report at 50 (“There are enormous benefits associated with the rise of profiling and targeted advertising and the ways consumers can be tracked and offered services as they move through the online and physical world. Advertising and marketing effectively subsidize many free goods on the Internet, fueling an entire industry in software and consumer apps.”); see also Deepa Seetharaman, *Facebook Revenue Soars on Ad Growth*, Wall St. J. (Apr. 28, 2016), <http://www.wsj.com/articles/facebook-revenue-soars-on-ad-growth-1461787856>.

¹¹⁵ See Wright White Paper at 25-28.

¹¹⁶ PCAST *Big Data Report* at x-xi.

¹¹⁷ See Wright White Paper at 13-14, 17-18 .

technical information about data collection and use. These transaction costs are non-trivial from a consumer’s perspective. Thus, unless consumers receive a discount or perceive some other affirmative benefit to reading, digesting, and opting in, they will generally take the path of least resistance and *do nothing*, thereby foreclosing—under an opt-in regime—any use of their information. And in making that non-choice, individual consumers do not fully internalize the broader social costs of their nonparticipation in the information economy.¹¹⁸

These are the reasons—and not any widespread predisposition to keep nonsensitive information “private”—why opt-in regimes impose enormous obstacles to the efficient and unobjectionable use of consumer information.¹¹⁹ That systemic bias against information-sharing would inflict several major categories of costs on the broadband ecosystem.

1. *The Proposed Rules Would Raise Broadband Prices and Dampen Broadband Investment Incentives*

First and most obviously, the proposed marketing restrictions would exert upward pressure on broadband prices by hamstringing ISPs from doing what many other non-ISP actors routinely do: subsidize affordable consumer services by using customer data to engage in profitable first- and third-party marketing.

By restricting the mere use of customer-specific information, the proposed rules would not enable consumers to see *fewer* ads; they would simply cause consumers to see *less relevant* ads and, in the process, deprive ISPs of the revenues they could earn by making third-party ads more relevant. Similarly, because the rules would restrict ISPs even from using their own customer data (including names and addresses) to promote many of their own services, ISPs would have to spend more money on less efficient advertising mechanisms, such as television

¹¹⁸ *Id.* at 18-20.

¹¹⁹ *See id.*

advertisements to the public at large. In short, the proposed restrictions would reduce the profitability of broadband services in several key respects: they would (1) decrease revenues from third-party advertising, (2) reduce each ISP's ability to use information from existing customer relationships to market its own products, and (3) subject ISPs to substantial new operational costs, such as the costs of systems changes and recordkeeping requirements.¹²⁰

These effects would undermine the Commission's primary mission, set forth in Section 706 and elsewhere: increasing broadband deployment and adoption. All else held equal, regulation tends to raise the price (and lower the output) of a service if it increases the cost of providing that service or reduces the incremental revenues a provider can earn in adjacent markets. As Professor Wright explains, the proposed rules would have precisely those effects on broadband service because they would impose new costs on ISPs, hamstringing their ability to sell new services to their own customers, and all but preclude them from earning revenues for third-party marketing in the double-sided online marketplace.¹²¹ By analogy, if the government told

¹²⁰ Under the approach discussed in the NPRM, those costs would skyrocket (at ¶ 142), because ISPs would constantly have to solicit "just-in-time" approvals whenever they collect customer information or put that information to new uses. Indeed, in many cases, that requirement would simply deter ISPs even from seeking opt-in consent because the cumbersome steps needed to prepare and transmit notices to the customers at issue and wait for their responses would often make "just-in-time" approval a practical impossibility in the fast-paced world of Internet commerce. Consistent with those concerns, the FTC has recommended just-in-time notice and consent *only* with respect to a narrow range of sensitive data. See FTC, *Mobile Privacy Disclosures FTC Staff Report: Building Trust Through Transparency* (Feb. 2013) (recommending that companies "[p]rovide just-in-time disclosures to consumers and obtain their affirmative express consent before allowing apps to access sensitive content like geolocation; [and] [c]onsider providing just-in-time disclosures and obtaining affirmative express consent for other content that consumers would find sensitive in many contexts, such as contacts, photos, calendar entries, or the recording of audio or video content"), <https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf>.

¹²¹ See Wright White Paper at 20-22. For a discussion of the "seesaw principle" applicable to pricing in two-sided markets, see generally M. Armstrong, *Competition in Two-Sided Markets*, 37 RAND J. Econ. 668 (2006); J. Rochet & J. Tirole, *Two-Sided Markets—A Progress Report*, 37 RAND J. Econ. 645 (2006).

magazine publishers that they must limit the ad space they sell to third-party merchants, subscription rates for magazines would increase and fewer magazines would be sold. Broadband services are no different in this respect.

2. *The Proposed Rules Would Chill Innovation and Suppress Competition*

The irrational distinction between “non-communications-related” and “communications-related” services would not only contradict consumer expectations about data use (see Section I.A.1.b above), but also chill ISP innovation and distort competitive dynamics between ISPs and over-the-top rivals.

The NPRM proposes (at ¶ 18) to exclude all “edge services offered by a broadband provider” from the “communications-related” category. Under that approach, an ISP’s innovative mobile app may be deemed a “non-communications service” subject to opt-in requirements. ISPs would thus face severe impediments in trying to use their own customer data to market those services, whereas non-ISP providers would remain free to use all existing customer data however they wish to promote their equivalent services. This opt-in requirement for “non-communications-related” services would thus place ISPs at a substantial competitive disadvantage whenever they do offer over-the-top “edge services” in competition with non-ISP providers of those same services, such as Google or Amazon. And that regulatory asymmetry would irrationally suppress competition and thus disserve the very consumers these rules are designed to protect.

More generally, the proposed rules would erect an arbitrary distinction between (1) preferred (non-ISP) participants in the Internet ecosystem, which could continue collecting the same types of personal information as before, and (2) ISPs, which would be restricted in their ability to collect the same information. And the proposed regime would not only tilt the competitive playing field for the delivery of targeted advertising, but do so in favor of entrenched

incumbents (edge providers, such as Google) and against new entrants (ISPs). As economists Thomas Lenard and Scott Wallsten explain, “[t]reating ISPs differently from edge companies would put ISPs at a competitive disadvantage in the large and growing digital advertising market, which had revenues of approximately \$60 billion in 2015. This disadvantage would pose an entry barrier to ISPs, denying them a source of revenues and therefore helping to ensure that they continue to cover all their costs from direct payment by end users.”¹²²

Indeed, as soon as the Commission announced its proposed rules, the rating agency Moody’s immediately issued a downgrade for ISPs, explaining that “this proposal will have a negative impact on both fixed and mobile broadband providers. If approved, the ability to compete with digital advertisers such as Facebook and Google . . . , who are able to collect the same type of data from consumers who access their websites and those of others, will be severely handicapped in the future as the old guard ecosystem evolves to become more competitive.”¹²³ Again, that regulatory bias is particularly unjustifiable not only because ISPs are new entrants in the relevant market, but also because, in this era of encryption and multiple connections per user, edge providers already enjoy substantial and rapidly increasing benefits over ISPs in the collection and use of consumer data. *See* Tech. Background, *supra*.

3. *The Proposed Rules Would Needlessly Confuse Consumers*

In addition to these other harms, the proposed regulations would generate consumer confusion about exactly what is, and what is not, subject to particular privacy protections. Most

¹²² Thomas Lenard & Scott Wallsten, *An Economic Analysis of the FCC’s Privacy Notice of Proposed Rulemaking* at 3 (May 25, 2016) (“Lenard & Wallsten”) (submitted by the Tech. Policy Inst. in this proceeding).

¹²³ Moody’s Investor Service, *FCC’s Broadband Privacy Proposal Credit Negative for Linear TV and Wireless Providers* (Mar. 14, 2016), <http://www.netcompetition.org/wp-content/uploads/FCC%E2%80%99s-broadband-privacy-proposal-credit-negative-for-linear-TV-and-wireless-providers.pdf>.

consumers do not sharply distinguish among the various interdependent actors in the Internet ecosystem, and all but the savviest will assume that the same general privacy rules apply to their mobile operating system (or web browser or coffee-shop WiFi operator) as apply to their mobile ISP. Asymmetric regulation of different segments of the online marketplace would thus needlessly confuse consumers, who are unlikely to understand the nuances in the different privacy regimes and may wrongly assume that the Commission’s rules apply to all of their Internet activities.¹²⁴ A consumer reading about the supposed benefits of the proposed rules would be surprised to learn that, even though AT&T must obtain opt-in consent before making most uses of personally identifiable information it collects as an ISP, Google need follow no such requirement in arranging for the Android operating system to transmit all of the same information (and more) back to Google’s centralized servers for the same types of uses.

The proposed rules would confuse consumers in a second respect as well. Like other ISPs, AT&T obtains customer information not only when it acts as an ISP, but also when it acts in any non-ISP, non-Title II capacity—for example, as an edge provider. To keep its customer communications as user-friendly as possible, AT&T has developed a unified privacy policy applicable to all such services, and its customer privacy notices are accordingly simple and easy to follow. AT&T can maintain that approach, however, only if the Commission’s privacy rules for ISPs are consistent with the FTC’s privacy regime for every other Internet participant. If the Commission radically departs from that regime, as it proposes to do, AT&T (like other ISPs) will have to complicate their user notifications. One set of rules governing opt-in and opt-out would

¹²⁴ Although AT&T agrees that, as a matter of best practices, ISPs should offer some form of “privacy dashboard” (*NPRM* ¶ 205), the Commission should not impose any regulatory obligation to that effect. Among other concerns, any privacy dashboard designed to reflect the NPRM’s proposed rules would sow extraordinary confusion among consumers, given the complexity of those rules and the deeply counterintuitive distinctions they would draw. The Commission should instead allow industry to continue developing best practices in this area to ensure an optimal combination of transparency and usability.

address information gathered by AT&T as an ISP; a different set of rules would address information gathered by AT&T in a non-ISP capacity; and the latter set of rules would also properly apply to AT&T *qua* ISP so long as it purchased the information from third parties (such as data brokers) and not directly by virtue of providing service. AT&T also would have to obtain separate permission to use customer data for first-party marketing, even though customers already can opt out of receiving any marketing material at all from AT&T through choices such as Do Not Call, do not email and do not direct mail. These disparate regimes would mystify consumers for the same reason they would make irrational public policy: the distinctions they draw would make no sense.

4. *The Proposed Ban on Commercial Inducements to Opt In to Data Uses Would Be Unlawful and Inimical to Broadband Deployment and Adoption*

The NPRM asks (at ¶ 259) whether the Commission should prevent consumers—even via the clearest opt-in mechanism—from agreeing to “financial inducements, such as lower monthly rates, for their consent to use and share” customer-specific information for marketing purposes, apparently whether or not the information is sensitive or shared with third parties. That paternalistic proposal runs headlong into the basic premise of the modern economy.

Whenever someone performs a Google search, or uses a Gmail account, or buys an Android phone, or signs into a Facebook account, or downloads a mobile app, or even logs into a WiFi network operated at a coffee shop or in New York City, that person is choosing to share information about his or her online activities in exchange for free or discounted service.¹²⁵

¹²⁵ The NPRM notes (at ¶ 260) that, in various *non*-ISP-related contexts, it is not always “clear that consumers generally understand that they are exchanging their information as part of those bargains.” That is because not all companies are as clear as ISPs in explaining to consumers what information will be shared and for what purposes, and many edge providers obtain consumer consent through take-it-or-leave-it mechanisms. In contrast, AT&T could not be clearer in explaining the types and uses of the

Indeed, using such information to subsidize high-value but affordable services is the basic bargain of the Internet ecosystem, and it has fueled the technology sector’s explosive growth with widespread consumer support.¹²⁶ Until now, no U.S. governmental body has seriously suggested that the companies on the information-receiving end of this bargain are using “coercive tools to force consumers to give up their statutory rights” or are “unfairly disadvantage[ing] low income or other vulnerable populations who are unable to pay for more expensive, less-privacy invasive service options.”¹²⁷ In fact, the reality is exactly the opposite of those characterizations. Banning discounts in exchange for information-sharing would, by definition, increase the price and lower the output of any affected service, including broadband Internet access. The contemplated ban would thereby disadvantage precisely those low-income populations about whom the NPRM expresses concern. Again, moreover, the question is not whether any consumer’s data will be collected, because non-ISP actors will continue to collect and use the same data anyway. The question is whether ISPs will be able to put that data to

information at issue when offering customers a discount on GigaPower services, discussed below. AT&T, Inc., *U-verse with AT&T GigaPower Internet Preferences*, <https://www.att.com/esupport/article.html#!/u-verse-high-speed-internet/KM1011211>.

¹²⁶ According to a recent Zogby poll, “[m]ore than 85 percent of respondents said they preferred an ad-supported Internet model instead of paying for online content, and three-quarters said they would reduce their online activities ‘a great deal’ if they had to pay for those services and content.” Digital Advertising Alliance, *Zogby Poll: Americans Say Free, Ad-Supported Online Services Worth \$1,200/Year; 85% Prefer Ad-Supported Internet to Paid* (May 11, 2016), <http://www.prnewswire.com/news-releases/zogby-poll--americans-say-free-ad-supported-online-services-worth-1200year-85-prefer-ad-supported-internet-to-paid-300266602.html>.

¹²⁷ *NPRM* ¶ 261 (internal quotation marks omitted). The NPRM badly mischaracterizes the FTC’s 2016 Big Data Report as somehow supporting the latter proposition. *See id.* ¶ 261 n.407 (citing *2016 FTC Big Data Report* at 2, 9-11). The FTC Report merely cautions against the use of Big Data—no matter how it is obtained—to make prejudicial assumptions about consumers who fall into particular demographic categories. *See 2016 FTC Big Data Report* at 2, 9-11. It does *not* suggest that low-income consumers are somehow harmed simply by accepting discounted (or free) services in exchange for allowing their information to be used.

productive use and share a portion of the ensuing value with their customers—including low-income customers.

The contemplated ban on opt-in discounts would also be deeply anticompetitive. As the NPRM notes, AT&T offers a discount on the ultra-fast 1GB-speed tier of its GigaPower service when a customer expressly agrees to allow the information he or she shares online to be used for marketing purposes (which do not involve sharing customer-identifiable data with third-party advertisers). AT&T generally deploys GigaPower in areas where other providers, such as Google Fiber or a cable incumbent, have already deployed their own ultra-high-speed fiber networks. Google can cross-subsidize the deployment of its networks by making use of the additional consumer data it will obtain through the higher-level services in which it exercises substantial market power, such as search and Gmail. Forbidding AT&T to make use of the same data to fund its broadband rollout *even after obtaining explicit consumer consent* would once again tip the competitive scales in favor of Google, which has more than twice AT&T’s market capitalization precisely because of the value it derives from ad-based revenue.

The contemplated ban on opt-in discounts would also be unlawful for all the same constitutional and administrative law reasons that the NPRM’s proposed opt-in requirements would be unlawful, *see* Section IV.A & IV.B, *infra*, and several others as well. In particular, such a ban would violate Section 222(c)(1), which presupposes that informed consumer consent is always sufficient to justify such data use. That provision restricts the specified data uses “[e]xcept ... with the approval of the customer,” which signifies Congress’s intent to remove the restrictions whenever a customer does approve.¹²⁸

¹²⁸ 47 U.S.C. § 222(c)(1).

In addition, the contemplated ban would be particularly arbitrary and capricious if the Commission adopted it while failing to make rigorous findings of market power for each of the affected companies and broadband markets. A necessary (but not sufficient) premise of that ban is that “customers’ broadband choices are limited by lack of competition” or “switching costs.” *NPRM* ¶ 262. Whenever there is competition, consumers concerned about privacy can vote with their feet if any provider’s undiscounted price for broadband service is excessive. Again, consumers have exactly that choice in the areas where AT&T has deployed GigaPower, where AT&T faces intense competition from Google Fiber or similar services offered by cable incumbents. AT&T is certainly not a dominant provider in any of those markets. Consumers have similarly broad choices in choosing among mobile ISPs, and switching costs are minimal. *See p. 28, supra*. In all of these contexts, the contemplated ban on discounted opt-in arrangements would be arbitrary and capricious because they would accomplish no discernible public benefit and would instead simply deny consumers any opportunity to share in the value created by innovative uses of customer information.

II. THE COMMISSION SHOULD REVISE THE PROPOSED RULES TO PRESERVE THE BENEFITS OF AGGREGATE AND NON-AGGREGATE DE-IDENTIFIED DATA

The previous section focused on the Commission’s proposed restrictions on how ISPs may use information in their possession to conduct both first-party and third-party marketing that involves no transfer of individually identifiable information to third-party advertisers. This section addresses the Commission’s proposed restrictions on an ISP’s ability to perform data analytics and use or share with third parties non-individually identifiable information—aggregate or non-aggregate de-identified data, which Section 222 categorically exempts from CPNI

regulation.¹²⁹ Like the NPRM’s proposed restrictions on marketing, the NPRM’s proposed restrictions on non-individually identifiable information could impose substantial harms while furthering no legitimate public policy benefits.

The NPRM focuses on proposed regulations for the use and disclosure of a particular category of de-identified information: *aggregate* customer proprietary information. It defines aggregate information as “*collective* data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.” *NPRM* ¶ 72 (emphasis added). The NPRM proposes a four-factor test for determining when an ISP can use or share aggregate customer proprietary information without consumer consent: the ISP must obtain consent unless it (1) determines that the aggregate information is not “reasonably linkable” to an individual or device; (2) publicly commits to maintain and use the data in non-individually identifiable format and not to attempt to re-identify the data; (3) contractually prohibits entities to which the provider discloses information from attempting to re-identify the data; and (4) exercises “reasonable monitoring” to ensure such contracts are not violated. *Id.* ¶ 154. The NPRM, however, does not propose to apply the four-part standard to de-identified but *non-collective* customer information, even though those data, too, reveal no personal information.¹³⁰ Instead, the NPRM asks whether providers should be prohibited from using or disclosing such de-identified data absent express customer consent. *Id.* ¶ 165. As explained below, the answer is clearly no.

¹²⁹ Section 222 authorizes the Commission to restrict the disclosure and use *only* of “individually identifiable” CPNI, 47 U.S.C. § 222(c)(1), and affirmatively authorizes carriers to “use, disclose, or permit access to aggregate customer information,” *id.* § 222(c)(3). As used here, the term “de-identified data” is a generic category that encompasses aggregate data and non-collective de-identified data as separate subcategories.

¹³⁰ As explained in greater detail below, even apart from aggregation, statistical techniques can be reasonably used to ensure that specific data cannot be linked to an individual.

The Commission should also clarify a number of points in connection with its four-part standard to preserve the ability to use de-identified data in socially beneficial ways. Several restrictions contemplated by the NPRM would unlawfully preclude ISPs from using de-identified data in ways that would provide substantial public benefits yet pose no privacy concerns. The specific changes recommended by AT&T are set forth in subsection B below. But to put those proposed regulatory changes in the proper context, we first discuss the major social benefits derived from the use and dissemination of de-identified information as well as the steps AT&T takes to ensure those benefits are delivered without compromising customer privacy.

A. Background: the Social and Economic Benefits of De-Identified Data

1. *Use of AT&T De-Identified Data by Businesses, Research Institutions, and Governmental Bodies Produces Enormous Public Interest Benefits*

AT&T makes many types of de-identified customer information available to business customers, research institutions, and government entities.¹³¹ First, AT&T sells business customers such information in the form of commercial reports that enhance economic efficiency in countless respects, helping companies market and deliver products and services in a manner that most effectively meets their customers' interests and needs. For example, using such data, a retailer may estimate the number of customers at or near its stores by time of day and day of week and decide to increase the number of sales representatives during certain peak business hours and ship products to certain locations based on expected demand.

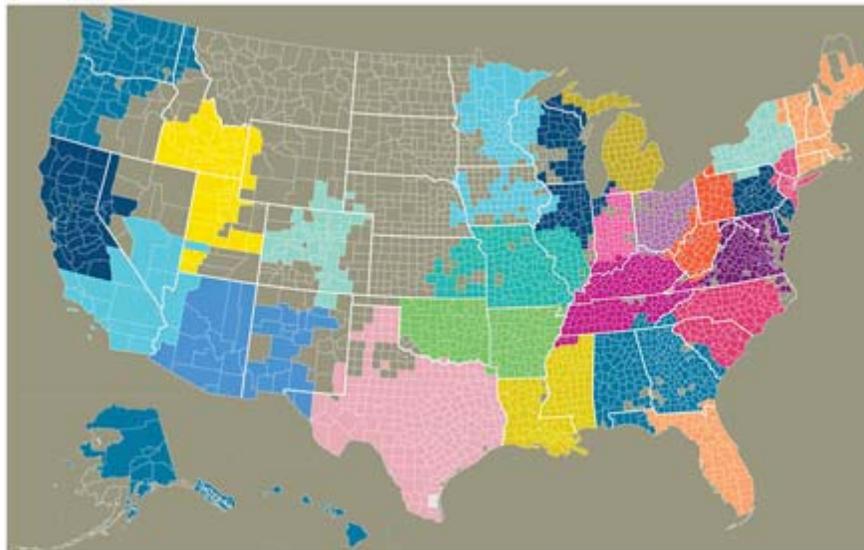
Second, AT&T provides de-identified aggregate and non-aggregate information to universities, laboratories, think tanks, and other institutions for research purposes focused on social networking, behavioral sciences, environmental policy, public policy, and other fields.

¹³¹ See AT&T, Inc., *AT&T Privacy FAQ*, <http://www.att.com/gen/privacy-policy>.

For example, researchers at AT&T Labs – Research, IBM Research, and MIT SENSEable City Laboratory used de-identified cell phone data from millions of customers to map the communities that people form through personal communications.¹³² Specifically, the researchers identified connections and commonalities in personal interactions that crossed state lines by analyzing cell phone calling and texting records and mobile location data. No personally identifiable information was used; rather, AT&T provided these researchers with de-identified aggregate customer data.

Applying a modularity algorithm to the de-identified aggregate data, the researchers identified regional links that crossed state lines, but in other instances, individual States were comprised of multiple, distinct communities. This research is important to understanding how economic and social communities form and the role that geography and political boundaries can play in community development. The figure below provides an example of this research.

(Counties with strong connections were assigned a similar color.)



¹³² Alexandre Gerber, Deirdre W. Paul, James R. Rowland, & Christopher A. Rath, *The Connected States of America Maps Communities*, AT&T Researchers (July 3, 2011), http://www.research.att.com/articles/featured_stories/2011_06/201106_connected_states_America_project_no_links.html.

This, of course, is just one example. Such uses of de-identified data have a range of applications across communications, business, public policy, sociology, anthropology, biology, environmental science, medicine and health care, and numerous other fields. As noted in another research paper, de-identified customer information “provide[s] to researchers and city planners an unprecedented opportunity to understand the presence and movement of physical communities.”¹³³ Researchers are just beginning to explore the full potential and range of applications of de-identified data derived from broadband use.

Third, AT&T provides de-identified information to local, state, and federal governmental bodies. Governments may use this data for municipal development, business development, transportation planning, emergency and disaster response coordination, and other public policy purposes. For example, AT&T’s de-identified customer information may be used to assist a municipality in its efforts to design a more efficient public transportation system. By collecting and analyzing de-identified data from its customers, AT&T can give a municipality the data it needs about its residents’ daily commutes and enable city planners and government officials to analyze the data to pinpoint key areas of public policy concern.

For example, AT&T collaborated with the California Department of Transportation on a research project that analyzed traffic and commuting patterns in Los Angeles and San Francisco. A team of researchers at the University of California at Berkeley developed a traffic model simulation using AT&T non-aggregate de-identified location data from mobile devices.¹³⁴ The

¹³³ Fabien Girardin, et al., *Towards Estimating the Presence of Visitors from the Aggregate Mobile Phone Network Activity They Generate*, 11th International Conference on Computers in Urban Planning and Urban Management (2009), http://www.research.att.com/export/sites/att_labs/techdocs/TD_7KDR9B.pdf.

¹³⁴ See David Z. Morris, *How AT&T Is Using Drivers’ Cellular Data to Help Fix California Traffic*, *Fortune* (Oct. 16, 2015), <http://fortune.com/2015/10/16/att-using-big-data-to-fix-traffic/>.

researchers then briefed the Department by producing outputs of the simulated data to help improve traffic flows and reduce congestion. With such use of de-identified information, a municipality may attempt to design a more efficient transportation system (roads, highways, and bridges) or public transportation infrastructure (buses, subways, and light rails).

2. *AT&T Takes Significant Steps to Protect Privacy Interests When Creating and Using De-Identified Data*

For each of the uses of de-identified data described above, AT&T offers substantial privacy protections to reasonably ensure the anonymity of the customer data it shares with third parties. *First*, AT&T uses statistical techniques and operational controls to de-identify customer data before it discloses any customer information to third parties.¹³⁵

Second, AT&T fully discloses the use of de-identified information to its customers. AT&T states that it may share anonymous information with other companies and entities, including “[u]niversities, laboratories, think tanks and other entities that conduct networking, social, behavioral, environmental and other types of scientific research, for the purpose of creating fundamental new knowledge”; and “[m]unicipalities, government or other entities that may use this data for purposes such as municipal and transportation planning, and emergency and disaster response coordination.”¹³⁶ AT&T also discloses its use of “aggregate information to create External Marketing & Analytics Reports that we may sell to other companies for their own marketing, advertising or other similar uses.”¹³⁷

Third, AT&T offers opt-out opportunities for its customers if they wish to be excluded from External Marketing and Analytics Reports, even though no such choice is required under

¹³⁵ See AT&T, Inc., *AT&T Privacy FAQ*, <http://www.att.com/gen/privacy-policy>.

¹³⁶ *Id.*

¹³⁷ *Id.*

the FTC’s privacy framework.¹³⁸ AT&T also provides opt-outs for relevant advertising and online behavioral advertising that apply to the use of customer data—whether in identified or de-identified form—to target advertisements to AT&T customers.¹³⁹

B. The Proposed Rules Should Be Revised to Preserve the Benefits of De-Identified Data

The NPRM’s approach to de-identified data should be revised in key respects to preserve the benefits of de-identified data.

As an initial matter, the NPRM contemplates (at ¶ 165) a piecemeal regulatory approach that would erect formidable and needless practical barriers to socially beneficial uses of de-identified data. Specifically, the NPRM proposes to apply its four-part test only to aggregate data, but not de-identified data generally, and to subject non-collective de-identified data to far more burdensome restrictions, including potentially an “opt-in” requirement. But there is no policy justification for treating aggregate and non-collective de-identified data under different regulatory frameworks. Aggregation and statistical de-identification are both effective approaches to removing personally identifiable information. Indeed, as the NPRM acknowledges (at ¶ 154), its four-part standard is drawn from the FTC’s regulatory framework, but the FTC applies the same regulatory approach to *all* de-identified data, even data used and shared in non-collective form.¹⁴⁰

The Commission also lacks any legal authority to impose the types of restrictions the NPRM contemplates for non-collective de-identified data. As AT&T has previously

¹³⁸ *Id.*

¹³⁹ *Id.*

¹⁴⁰ *2012 FTC Privacy Report* at 20-21. To the extent the Commission’s concern is that aggregation may be more effective in preventing re-identification, the solution is to not require opt-in for de-identified data, but to require the type of “best practices” that AT&T currently uses to produce non-collective data that cannot reasonably be re-identified.

explained,¹⁴¹ Section 222(c)(1) authorizes the Commission to restrict only the use of “individually identifiable” CPNI, and the Commission must give effect to those terms. Under no plausible reading of the statute could information that has been purged of personal identifiers be considered “individually identifiable.” Any such prohibition also would violate the First Amendment, whether the communication it suppresses is viewed as commercial speech or, depending on the circumstances, as noncommercial speech entitled to full constitutional protection. *See* Section IV.B, *infra*. There is no valid justification for preventing ISPs from using and disclosing data that has been de-identified to prevent the disclosure of personally identifiable information.

In addition, the Commission should, in several respects, clarify or modify its four-part test to preserve the full array of social benefits of de-identified data.

First, ISPs often cannot create de-identified data unless they can first take identifiable customer data and anonymize it to create aggregate or otherwise de-identified data sets. The Commission has previously recognized this essential step of producing aggregate data and has expressly extended the exemption from CPNI’s requirements to the anonymization process. In prior orders, the Commission has recognized that Section 222 and CPNI regulations authorize a carrier to “aggregate its CPNI to develop profiles of its customers”¹⁴² and that, when CPNI is transformed into aggregate customer information, “carriers are free to use aggregate information

¹⁴¹ Comments of AT&T, *In the Matter of Petition of Public Knowledge for Declaratory Ruling that Section 222 of the Telecommunications Act Prohibits Telecommunications Providers from Selling Non-Aggregate Call Records Without Customers’ Consent*, WC Docket No. 13-306 (Jan. 17, 2014). We incorporate this filing by reference and are submitting it in this docket.

¹⁴² Second Report and Order and Further Notice of Proposed Rulemaking, *In the Matter of Implementation of the Telecommunications Act of 1996*, 13 FCC Rcd 8061, ¶ 149 (1998) (“1998 CPNI Order”), vacated on other grounds by *U.S. West, Inc. v. F.C.C.*, 182 F.3d 1224 (10th Cir. 1999).

‘to assist in product development and design, as well as in tracking consumer buying trends, without customer approval.’”¹⁴³

The same clarification is required here. To create de-identified data, AT&T and other providers will need to strip away personal characteristics from identifiable data. Providers then will need to match these data sets by means of a unique identifier with other information to produce aggregate reports. Without an express clarification that the de-identification requirement applies only to the ultimate use or sharing of data, the Commission might inadvertently ban the creation of de-identified data. Providers must be permitted to *maintain and use* customer information to create de-identified data, without any “opt-in” restriction; otherwise, much de-identified data could never be created.¹⁴⁴

Second, the NPRM proposes (at ¶ 154) to ban ISPs from using aggregate data without consent if it is reasonably linkable to “a specific individual *or device*.” But information about a *device* can raise privacy concerns only to the extent that it can in turn be linked to a *person*. Where that connection is strong, the individual has a cognizable privacy interest. There is no significant privacy interest, however, where that connection to an identifiable person is too weak to be reasonably made. The Commission should thus revise its proposal to focus on the true privacy interest at stake: the linkability of data *to persons*.

¹⁴³ Declaratory Ruling, *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information & Other Customer Information*, 28 FCC Rcd 9609, 9621 ¶ 34 (2013).

¹⁴⁴ *NPRM* ¶ 165. On a similar note, the Commission should clarify that the second part of its four-part standard—that ISPs should make a public commitment to maintain de-identified data they create in non-individually identifiable format and not attempt to re-identify the data—does not affect in any way ISPs’ ability to use the underlying data from which such de-identified data was drawn. In other words, the Commission should clarify that the public commitment it seeks from ISPs applies only to the data that has gone through the de-identification process.

Third, the Commission should clarify that not all aggregate data should be subject to the requirement (*NPRM* ¶ 154) that any ISP “contractually prohibit[] any entity to which it discloses or permits access to the aggregate data from attempting to re-identify the data.” An ISP might well be expected to include a contractual requirement prohibiting re-identification when the de-identified data provided to a third party is drawn from particularly sensitive customer information and where there is some objective concern about re-identification. But the Commission cannot reasonably require ISPs to impose such contractual requirements in all circumstances—for example, where there is little reasonable possibility that the data could be re-identified or, alternatively, where the underlying data at issue is not sensitive. Such an inflexible requirement could create illogical and counter-productive consequences: re-identifying individual data from some highly abstract aggregate data is far more difficult and, in many circumstances, simply impossible. The FTC implicitly acknowledges this when it suggests that one method to ensure that data is sufficiently de-identified is through “the use of aggregate or synthetic data.”¹⁴⁵ Thus, to follow “existing best practice guidance from the FTC,” *NPRM* ¶ 154, the Commission should categorically exempt certain highly aggregated data from any requirement to include contractual provisions against attempted reidentification.

Taken to its illogical extreme, the Commission’s proposal would make it impossible for ISPs to provide important statistical information that has been commonly published in the industry and that raises no conceivable privacy concerns. For example, commonly disclosed aggregate data—such as the total number of broadband subscribers—would technically constitute aggregate data derived from CPNI. There is no reasonable possibility that such aggregate data can ever be used to re-identify individuals, and ISPs obviously could not impose

¹⁴⁵ 2012 *FTC Privacy Report* at 21.

contractual limitations on all parties that receive such data. Indeed, AT&T discloses the total number of broadband subscribers in its quarterly reports, as well as the percentage of customers that have plans that deliver high Internet speeds, the total number of mobile broadband subscribers, and other information that constitutes aggregate “customer proprietary information,” as the Commission would define that term.¹⁴⁶ This is the type of information that the Commission should seek to encourage, not suppress with unnecessary and burdensome regulatory requirements. Indeed, the Commission itself produces an annual report that consists of aggregate CPNI and customer PI.¹⁴⁷

Fourth, for similar reasons, the Commission should not impose a blanket requirement to monitor performance of third parties’ compliance with their contractual obligations. To begin with, any monitoring rule could logically apply only where the Commission has subjected an ISP to a threshold requirement to impose contractual obligations on third parties, and as just discussed, it would make no sense to impose that threshold requirement in a variety of circumstances. More generally, there is no basis for imposing any monitoring requirement in any circumstances, given that the third party at issue will have every incentive both to comply with its contractual obligations and to avoid civil liability as well as enforcement actions by the FTC or this Commission (depending on whether the third party is a common carrier).

Finally, the Commission should make clear that in no circumstances will ISPs be held strictly liable for the actions of third parties to whom they provide aggregate or otherwise de-

¹⁴⁶ These concerns apply with particular force given the broad sweep of the definitions the NPRM proposes for CPNI and PII, which would treat data raising no legitimate privacy concerns as “proprietary.” Any concerns about sharing aggregated data are particularly attenuated when the underlying data do not implicate any privacy interest.

¹⁴⁷ See Federal Communications Commission, *Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless, Including Commercial Mobile Services: Eighteenth Report* (Dec. 23, 2015) (reporting, for example, the total number of broadband customers).

identified data. Like any other actor in the Internet ecosystem, an ISP may face a risk of liability if it transfers sensitive data to third parties without taking reasonable steps to avoid foreseeable privacy harms.¹⁴⁸ But the Commission would create irrational disincentives against socially productive uses of aggregate or de-identified data if it subjected ISPs to strict liability for harm caused by third parties after the ISPs *do* take whatever steps are reasonable under the circumstances. Instead, it should establish a “reasonableness” standard that is consistent with the FTC’s approach.

III. THE PROPOSED DATA-SECURITY RULES WOULD RADICALLY OVERSHOOT THE MARK AND IMPOSE NEEDLESS AND SUBSTANTIAL COSTS

Data breaches are a source of serious concern in today’s Internet environment, and that is why AT&T and other ISPs are industry leaders in protecting customer data from hackers. When a company does sustain a breach, it must scramble to investigate what happened and which data may have been compromised. In general, if, after gathering the facts, it concludes that the breach may have compromised specified categories of consumer data, it will notify affected consumers (as well as law enforcement) to allow them to take appropriate steps to avoid or mitigate possible harm. Except in a few specialized contexts relating to particularly sensitive information (such as health or financial records), the timing and contents of such data-breach notifications have been governed mainly by state law, and 47 states (as well as the District of Columbia, Puerto Rico, Guam, and the Virgin Islands) have so far adopted detailed rules addressing those issues.

Against this backdrop, the NPRM proposes data-breach and data-security requirements that would extend well beyond those established by state and other federal regulators, even with

¹⁴⁸ See, e.g., *FTC v. Sitesearch Corp.*, No. 14-cv-2750 (D. Ariz. Dec. 11, 2015) (Final Judgment and Order) (settling allegations that data broker unreasonably sold the sensitive personal information of consumers to third parties who foreseeably used the information to commit fraud).

respect to broadband customer data that is not particularly sensitive, such as name and address information. The proposed requirements would not only exceed the Commission's statutory authority (*see* Section IV.C, *infra*), but also subject ISPs to irrational, duplicative, and counterproductive requirements without precedent under any other regulatory scheme.

To be sure, on some issues, the NPRM acknowledges the practical dimensions of its proposals. For example, on the question of triggering criteria for customer notification, the NPRM appropriately asks (at ¶¶ 237-238) whether those criteria “[s]hould ... be calibrated to the sensitivity of the information” and, similarly, whether no notification should be required “if, after an appropriate investigation, the [ISP] determines that there is not a reasonable likelihood that harm to the consumers will result from the breach.” The answer to both questions is yes, as should be obvious from any rational application of a cost-benefit analysis. An affirmative answer to those questions is also necessary to avoid the well-recognized risks of over-notification. As discussed, below, customer notifications are costly to implement and often confusing to consumers, particularly if consumers receive too many of them, and those costs should be incurred only if the notification could serve some real consumer benefit.

On several other issues, however, the NPRM jumps the rails. Of particular concern, it proposes extraordinarily broad definitions of the information subject to various data-security obligations, such as the obligation to report breaches to the Commission itself. *See* Section III.A, *infra*. The covered information would include virtually all of the customer data contained in an ISP's systems and files. That proposal is unprecedented precisely because it would make no sense. No existing state or federal breach notification standard applies to *all* personal information a company holds. Rather, those state and federal notification standards target categories of *sensitive* information whose exposure could place affected individuals at risk of

identity theft, embarrassment, or other serious harm. In contrast, the one-size-fits-all regime proposed in the NPRM would extend data-security and breach-related requirements to widely available information that poses no genuine privacy risk, such as a customer's name, address, and type of service (e.g., fixed or mobile). That approach would expose ISPs to substantial enforcement penalties whenever the Commission decides that they took inadequate measures to safeguard this innocuous information or had otherwise breached Commission rules regarding it, even where "disclosure" risks no harm at all. Regulations that treat all personal information the same would further contradict widely accepted risk-management principles and impair the ability of ISPs to focus their resources on the most serious cyber threats.

The NPRM also proposes a variety of other unprecedented data security and data breach requirements. For example, a literal reading of those rules would arguably make ISPs strictly liable for any data breach resulting from information they shared, no matter how reasonable the steps they took to protect the data. *See* Section III.B, *infra*. Likewise, in the event of a data breach (or suspected data breach), the contemplated rules would require ISPs to disclose the breach to customers on a 10-day timetable, which is far less time than necessary for even the most assiduous investigator to get to the bottom of what has happened and who is at risk. *See* Section III.C, *infra*.

Each of these requirements would further no legitimate policy goal and would merely impose enormous costs on broadband providers while hamstringing their ability to focus on the greatest cyber threats. If the Commission ultimately adopts rules in this area, it should therefore adopt a framework that requires only "reasonable" data security measures, and it should require breach notification on a reasonable timetable and only where there is a reasonable risk of harm to customers.

A. The NPRM's Definition of Covered Information Would Be Radically Overbroad

Many of the problems with the proposed data-security and breach rules arise from the same source: the NPRM's proposal (at ¶ 75) to define a data "breach" as unauthorized access to "all customer PI" as well as all CPNI. That threshold definitional choice would extend the proposed data-security and breach rules to virtually all the customer-specific information contained in broadband providers' systems and files.¹⁴⁹ That information would include, for example, the customer's name, address and telephone number, type-of-service information (such as the mere fact that a customer subscribes to broadband service), and the customer's IP address.¹⁵⁰

As an initial matter, extending the data security rules to cover this wide range of information would greatly exacerbate the costs imposed by the NPRM's "data security framework."¹⁵¹ The NPRM proposes rules that would require ISPs to perform regular risk management and assessment, conduct extensive employee training, and establish "robust customer authentication procedures"—in short, to "ensure the security, confidentiality, and integrity of all 'customer proprietary information' the [ISP] receives, maintains, uses, discloses or permits access to."¹⁵² Applying those requirements to all "customer proprietary information" as capaciously defined in the NPRM would force ISPs to devote considerable resources to

¹⁴⁹ See NPRM ¶¶ 57-62.

¹⁵⁰ See *id.* ¶¶ 41-42, 62. The Commission's existing CPNI rules for voice service require reporting to the Commission and law enforcement breaches involving a wide variety of CPNI. See generally 47 C.F.R. § 64.2011. While this rule has existed since 2007, the NPRM identifies no evidence that the breadth of these requirements has provided any public interest benefits, let alone benefits that exceed the costs of the reporting obligations. Yet the NPRM illogically proposes to *extend* these reporting obligations even further to cover additional categories of non-CPNI information that are not sensitive and present little risk of harm in the event of disclosure.

¹⁵¹ NPRM ¶ 175.

¹⁵² *Id.* ¶¶ 109-110 (Proposed Rule 65.7005(a)).

protecting various categories of nonsensitive data (such as mere names and addresses) rather than focusing their efforts to prevent breaches posing genuine threats to customers.

For example, AT&T (like other ISPs) serves many millions of customers and interacts with them continually in retail stores, by phone, and online. Customers' names and telephone numbers are likely to be more widely used in those customer contacts than any other information that would be defined as CPNI or PII, and are also frequently used to identify customer accounts in internal systems. Subjecting such information to the Commission's data security regime would thus require providers to "ensure" against the release of data that could not possibly harm anyone. Consumers routinely disclose their names and phone numbers, often in public where such information could be overheard by strangers. Likewise, consumers every day provide such information to businesses and third parties with the recognition that their nonsensitive data will not be protected from disclosure to the same degree or in the same manner as sensitive information. The Commission itself has never deemed such information to be "proprietary" despite regulating CPNI since the early 1980s.

Indeed, the Communications Act itself authorizes carriers to provide "any person" with the names and telephone numbers (along with addresses) of subscribers so they might *publish* such information.¹⁵³ Those directories typically list each subscriber's name, telephone number, and street address, except where a subscriber has affirmatively opted out by requesting to remain unlisted. Against that backdrop, it would be both arbitrary and inconsistent with Section 222(e)

¹⁵³ See 47 U.S.C. § 222(e).

for the Commission to treat customer names and basic contact information as “proprietary” and, on that basis, forbid ISPs to use or disclose that information.¹⁵⁴

The NPRM’s proposal (at ¶ 42) to treat “type of service” as proprietary customer information is equally arbitrary. The proposed rule would characterize as “proprietary” information as unremarkable as whether a customer has “fixed or mobile; cable or fiber; prepaid or term” broadband service. However, a customer’s status as a subscriber to these ubiquitously available services is not sensitive information. Millions of people disclose that they subscribe to mobile service every day when they make and receive mobile calls in public places or use a tablet to surf the web. And the NPRM is on no firmer ground when it proposes (at ¶¶ 45, 62) to treat a customer’s IP address as both CPNI and PII. ISPs must disclose each customer’s IP address to every website that he or she visits. That IP address is not “private” information under any definition, and the ISP cannot possibly be expected to constrain how all those millions of websites treat that information.

Quite apart from the irrational breadth of the proposed data security requirements, the Commission would also greatly exacerbate the costs imposed by its data breach framework if it swept all “customer proprietary information” within its scope. Extending the data security and breach rules to cover this wide range of information would cause the number of reportable “breaches” to skyrocket and would thus impose commensurately high costs on broadband providers.

In this regard, one of the questions posed in the NPRM inadvertently reveals the *reductio ad absurdum* of its virtually boundless definition of covered information (namely, “all customer

¹⁵⁴ For the same reasons, the Commission should not amend the voice rules to limit the use of this information, as the NPRM proposes (at ¶ 64).

PI”). The NPRM asks (at ¶ 42) whether other nonsensitive information, such as the nature of the customer’s device (*e.g.*, smartphone, tablet, computer, modem, router, videophone, or IP caption phone) must also be treated as CPNI because such information may indicate the type of service to which the customer subscribes. In other words, the NPRM acknowledges that, under the “logic” of its PII definition, the mere disclosure of a customer’s possession of a smartphone or a computer would become a reportable data breach. For example, if an AT&T employee exclaimed, “Mr. Jones, you forgot your iPhone!” to a customer leaving a crowded AT&T store, she would have committed a “data breach,” and AT&T would be required to “report” that breach to the Commission, even though Mr. Jones publicly uses his iPhone many times a day and has no “privacy” interest in concealing that use. The Commission presumably does not intend that absurd result, but it is the logical—and arbitrary and capricious—consequence of the NPRM’s proposed definition of the data subject to regulation under Section 222.

B. The Proposed Regulatory Requirements To “Ensure” Data Security Are Excessive and Irrational

The NPRM asserts (at ¶¶ 175, 217) that, like the FTC, the Commission wishes to adopt a “reasonableness” standard for data security that allows for “flexibility.” In reality, though, the proposed rules would grant no real flexibility at all. As just explained, under those rules, ISPs could *not*, as the NPRM suggests (at ¶ 220), make security decisions based on the sensitivity of the data they hold because the NPRM deems virtually *all* customer-specific information held by ISPs as “proprietary.” The NPRM’s discussion of “reasonable” data security also ignores many factors that are highly relevant to what security measures should be adopted, such as the nature of the threats that ISPs face and the costs of security measures. No determination of whether a ISP undertook “reasonable” security measures can be made without considering these factors.

Indeed, the actual rule proposed by the NPRM would effectively eliminate any semblance of a “reasonableness” standard. Proposed Rule 64.7005(a) would provide that an ISP “*must ensure* the security, confidentiality, and integrity of all customer [proprietary information]” that the provider holds. Literally construed, this would make ISPs *strictly liable* for data breaches, no matter how reasonable the data security measures they adopted. Any strict liability rule would create arbitrary and perverse over-deterrent effects, suppressing productive uses of data without any cost-benefit justification. The Commission should thus confirm that it has no intent to create such a strict liability standard.

The NPRM also proposes unrealistic and rigid requirements that would govern “risk management assessment” by ISPs—*i.e.*, “requiring BIAS providers to establish and perform regular risk management assessments.”¹⁵⁵ Remarkably, the NPRM proposes that companies must “promptly remedy *any*” security concerns that the assessments identify.¹⁵⁶ On its face, this would require ISPs to address any issue identified by a security assessment, regardless of whether it is material, regardless of cost, regardless of the sensitivity of the underlying data, and regardless of the risk of a breach. Relatedly, the requirement that ISPs “promptly” address any such issues fails to account for the seriousness of the deficiencies and what timeframe would be “reasonable” considering all relevant considerations, including the need to address more significant security concerns. In all of these respects, the proposed rules would ignore cost-benefit considerations and violate the APA’s ban on arbitrary and capricious decisionmaking.

Finally, the rigidity of the proposed rules would contradict the methodology widely adopted under the NIST cybersecurity framework, which explicitly calls for *companies* to

¹⁵⁵ NPRM ¶¶ 180-84.

¹⁵⁶ *Id.* ¶ 180.

conduct their own risk assessments and then develop individualized cybersecurity programs to address identified risks.¹⁵⁷ The NPRM’s proposal would effectively take that decisionmaking away from companies and insert the Commission instead as the final arbiter of how and where companies should be prioritizing resources to protect against cyber attacks, even though the FCC has no particular expertise in that area. As Chairman Wheeler has previously recognized, individual companies, not “prescriptive government mandates,” should take the lead in setting cybersecurity priorities.¹⁵⁸

C. The Proposed Regulatory Requirements Governing Data “Breaches” Are Excessive and Irrational

The NPRM also proposes a series of regulatory requirements in connection with data breaches that impose undue and unjustified burdens.

Data Breach Reporting. As noted above, the NPRM appropriately recognizes (at ¶¶ 237-38) the need for a materiality “trigger” for the reporting of data breaches to customers—consistent with the approach taken by many states and federal agencies. Such triggers appropriately provide that notification is required only when there is a real likelihood “of harm to the consumer.”¹⁵⁹ Yet, with regard to reporting obligation to the Commission and law

¹⁵⁷ NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, at 14 (Feb. 12, 2014), <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.

¹⁵⁸ Remarks of FCC Chairman Tom Wheeler, American Enterprise Inst., at 3 (June 12, 2014) (“[T]he FCC must build upon past Federal and private sector work in cybersecurity. Following President Obama’s Cyberspace Policy Review in early 2009, a robust national dialogue helped create a new consensus for cybersecurity. Our nation chose proactive private sector cyber *risk management*—and all the corporate responsibilities and accountability that go along with that—over a traditional regulatory approach of prescriptive government mandates.” (emphasis added)), https://apps.fcc.gov/edocs_public/attachmatch/DOC-327591A1.pdf.

¹⁵⁹ NPRM ¶ 237.

enforcement, the NPRM proposes that broadband providers be required to report “any” breach.¹⁶⁰ The costs of that categorical requirement would far outweigh the benefits.¹⁶¹

AT&T has consistently complied with existing reporting obligations, both federal and state. But because the NPRM would dramatically expand the information covered by the reporting scheme, the Commission should at a minimum include a “risk of harm” trigger for any reporting rules it adopts.¹⁶² Otherwise, broadband ISPs would have to report countless “breaches” that neither raise cognizable privacy concerns nor signify criminal activity. *See* Section III.A, *supra*. Indeed, such over-reporting would distract attention from genuine data security concerns and lead to notice fatigue.

Timing of Data Breach Reporting. As the NPRM notes (at ¶ 239), there is no current Commission rule relating to the timing of customer notification in circumstances when an ISP determines that such notification is appropriate.¹⁶³ The Commission proposes to fill the gap with a bright-line requirement that, whenever ISPs concluded that customer notification is

¹⁶⁰ *Id.* ¶ 246.

¹⁶¹ In this regard, the NPRM would impose reporting obligations even greater than those imposed by the Commission’s existing, overbroad voice CPNI rules. The Commission’s existing rules do not require voice providers to report “any” data breach to the Commission and law enforcement officials, but only those where there has been an “intentional,” unauthorized access to proprietary data. *See infra* pp. 85-86. This requirement would at least obviate reporting of some breaches that do not pose a real risk of consumer harm—*i.e.*, where the data was not obtained by a purposeful wrongdoer. Again, the NPRM identifies no evidence that the “intentionality” requirement has undermined the ability of the FBI or the Commission to bring enforcement actions.

¹⁶² In addition to the numerous states that incorporate a risk of harm analysis, the federal government already uses this “risk of harm” standard when determining when to report unauthorized disclosures of the data it holds. *See, e.g.*, Office of Mgmt. and Budget Memo, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, at 13-14 (“To determine whether notification of a breach is required, the agency should first assess the likely risk of harm caused by the breach and then assess the level of risk. ... Agencies should bear in mind that notification when there is little or no risk of harm might create unnecessary concern and confusion.”), <https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>.

¹⁶³ The existing rules do properly require notification to law enforcement and the Commission before customer notification. 47 C.F.R. § 64.2011.

appropriate, they must send customers that notification within “10 days following discovery of the breach,” on the theory that this compressed timetable “will allow customers to take any measures they need to address the breach in as timely a manner as possible.”¹⁶⁴ No state imposes a similarly draconian requirement; instead, as the NPRM acknowledges, “many state data breach statutes impose an ‘expeditiously as practicable’ or ‘without unreasonable delay’ standard instead of a set timeframe for reporting.” *Id.* ¶ 241. That is for good reason: although investigations vary widely in their duration depending on the nature of each breach, it is often impossible to identify the extent and implications of many suspected data breaches within 10 days.

In particular, it often takes at least several weeks of diligent investigation to gather and confirm the information that, under the NPRM’s proposal, would have to be included in the breach notification to affected customers. Such information includes, for example, the estimated date of the breach and a description of the CPNI or PII that was (or is reasonably believed to have been) used, disclosed, or accessed as part of the breach.¹⁶⁵ To make these determinations, investigators often need to review system and video records, identify normal patterns of activity and any deviations from those patterns, interview personnel, and conduct other related tasks as well as consult with legal counsel. These activities often take far longer than the proposed 7-10 day timetable. If providers were required to report within such an unrealistic timeframe, they would often be unable to provide useful information or, in many cases, even identify the affected customers who need to be notified.

¹⁶⁴ *NPRM* ¶ 239.

¹⁶⁵ *See id.* ¶ 243.

Any information gathered at that early stage also may be incomplete and misleading. For example, where company or vendor personnel authorized to access customer information are suspected of engaging in improper account activity, the investigators must distinguish illegitimate from legitimate account activity. In such cases, conduct that initially may appear suspicious may be found to be legitimate business activity after further investigation. Such initial “false positives” are especially likely to occur where detection tools are used to identify potential data breaches based on deviations from normal activity patterns. In AT&T’s experience, the determination of whether apparently anomalous conduct reflects improper account access or merely a change in legitimate account activity requires analysis that would often take longer than 7-10 days.

Similarly, any requirement to submit customer notifications before completing an investigation would do more harm than good: customers would receive premature, incomplete, and often erroneous accounts of what has happened, and ISPs would face perverse incentives to cut corners in their investigations simply to meet arbitrary regulatory deadlines. Premature reports would also require frequent revision, thus wasting the time of the reporting entities as well as the Commission and any customer recipients. Incomplete or rushed investigations also could result in the mistaken identification of provider or vendor personnel as engaging in improper activity.

Certainly, no reporting obligation should be tied to an undefined “discovery” date, as the NPRM proposes (at ¶¶ 239, 242).¹⁶⁶ In particular, it would be unreasonable to treat, as the discovery of a data breach, the first identification of suspicious activity that is only later

¹⁶⁶ That requirement would far exceed what the Commission has required under its existing rules for voice CPNI. *See* 47 C.F.R. § 64.2011(b) (commencing the time to notify law enforcement of a breach based on “reasonable determination of the breach”).

determined to involve a data breach. In many cases, ISPs could not confirm whether a breach has occurred, and ascertain which customers are affected, within seven to ten days of first discovering suspicious activity that triggers the need for an investigation. The Commission should thus clarify that any reporting obligations are triggered only after a broadband provider has determined with substantial certainty that a breach has, in fact, occurred.

Reporting Based on Subjective Criteria. The NPRM asks (at ¶ 250) whether providers should be required to notify customers and law enforcement on discovery of conduct “that would reasonably lead to exposure of customer PI” and whether such notification should be in addition to or in place of a requirement to provide notification on discovery of a breach. That requirement would be unreasonable because ISPs would often be unable to anticipate all conduct that may require reporting under such subjective criteria and to report it if it occurred.

Providers have many thousands of employees who must continually access CPNI or PII to do their jobs of serving customers (particularly in light of the broad definitions of those terms proposed in the NPRM). Given the many circumstances that could lead to intentional or inadvertent “exposure” of CPNI or PII, providers could not feasibly establish procedures and train personnel to identify, on a timely basis, all conduct that may later be deemed to require reporting under such an ill-defined rule. The subjective nature of that rule, and the substantial enforcement penalties that could result from failures to report, would encourage providers to err on the side of filing reports for every circumstance that could conceivably result in some exposure of CPNI or PII. The likely result would be a massive volume of reports that would not provide useful information to customers or the Commission but would significantly increase providers’ compliance and reporting costs.

Account and Account Change Information. The NPRM proposes (at ¶ 203) to require broadband providers to notify customers of unsuccessful attempts to access “the customer’s account or account change information.” Such a rule apparently would require an ISP to notify customers of every unsuccessful log-in attempt that generated an error message. But most of the time, such incidents are completely innocuous and result from customers mistyping their user names or passwords. For example, AT&T estimates that unsuccessful log-in attempts to “My AT&T” online customer account information generate on average more than 500,000 error messages *each day*. The proposed rule would thus require providers to barrage their customers with millions of meaningless “notifications” that would achieve nothing beyond consumer confusion and annoyance.

Inadvertent Data Breaches. The NPRM proposes (at ¶ 75) not to include an “intent” element in the definition of “data breach” under its existing CPNI rules in order to “ensure data breach notification in the case of inadvertent breaches that have potentially negative consequences for customers.” AT&T has no objection to such a change, *provided that* the Commission adopts a “substantial risk of harm” standard for determining whether there has been a data breach requiring customer notification. Such notification should only be required where there is a reasonable likelihood that the breach of data security has or is likely to lead to identify theft, fraud or deception—*i.e.*, a substantial risk of harm. To the extent the Commission is proposing to eliminate the “intent” requirement to align its rules with state data-breach requirements, most state laws require a company to provide customer notification only where a breach is reasonably likely to result in significant customer harm.¹⁶⁷

¹⁶⁷ See, e.g., Alaska Stat. § 45.48.010(c); Ark. Code Ann. § 4-110-105(d); Conn. Gen. Stat. § 36a-701b(b)(1); 6 Del. Code Ann. § 12B-102(a); Haw. Rev. Stat. §§ 487N-1, 487N-2; Idaho Code § 28-51-105(2); Kan. Stat. § 50-7a02(a); La. Rev. Stat. Ann. tit. 51, § 3074(G); 10 Me. Rev. Stat. Ann.

Under the Commission’s existing rules, the “intentionality” requirement serves as an imperfect proxy for materiality. Where a party has “intentionally” sought to gain unlawful access to protected information, there is a strong basis for concern that such access may cause consumer harm. In contrast, if the Commission eliminated the intentionality requirement without also adopting a materiality standard, it would require reporting and notification of many inadvertent breaches that do *not* have “potentially negative consequences for customers.” For example, it would require notification of such everyday occurrences as a customer service representative accidentally inputting the wrong customer name or telephone number when seeking to access a customer account in an AT&T system and thereby accessing the wrong customer account. That approach would serve no purpose and would both confuse customers and impose substantial costs on carriers.

In addition, if the Commission eliminates the “intentionality” requirement, it should also exempt the good-faith acquisition of covered data by an employee or agent of the company, or a reasonably comparable “innocent” inadvertent recipient of data, where such information is not used improperly or further disclosed. By definition, there is no risk of consumer harm in such circumstances.

Third-Party Data Breach Notification. The NPRM requests comment (at ¶ 255) on whether broadband providers should “contractually require” the third parties with which they share CPNI or PII to file data breach notifications, either in place of or in addition to the notifications filed by ISPs. Where ISPs share CPNI or PII with agents, it is unnecessary to

§ 1348(1)(B); Md. Code Ann., Comm. Law § 14-3504(c); Mich. Comp. Laws § 445.72(1); Miss. Code Ann. § 75-24-29(3); Mo. Rev. Stat. § 407.1500.1-4(2)(5); Mont. Code Ann. § 30-14-1704(4)(a); Neb. Rev. Stat. § 87-803(1); N.H. Rev. Stat. §§ 359-C:19(V), 359-C:20(I)(a); Ohio Rev. Code Ann. § 1349.19(A)(1)(a); Or. Rev. Stat. § 646A.604(7); S.C. Code Ann. § 39-1-90(A); Utah Code Ann. § 13-44-202(1); Vt. Stat. Ann. tit. 9, § 2435(d)(1); Va. Code Ann. § 18.2-186.6(A); W. Va. Code. § 46A-2A-102(a); Wyo. Stat. Ann. § 40-12-502(a).

require those third parties to file data breach notifications because the risk of vicarious liability already creates strong incentives for the ISP to ensure compliance with FCC rules.¹⁶⁸ For example, AT&T's standard contract with its agents requires them to safeguard customer information and to cooperate fully in the investigation of any suspected improper access, use, or disclosure of this information. Given that background, it would make no sense to require an agent to file a duplicative data-breach report in addition to the one the ISP will already file, particularly given the limited resources that many agents could be expected to devote to the process.

* * *

In sum, by imposing data-security obligations that would extend far beyond existing state law requirements, the proposed rules would impose staggering costs on ISPs, dramatically increase the number of harmless incidents treated as reportable “breaches,” and submerge consumers in unprecedented volumes of pointless breach notifications. The rules would thus achieve little beyond desensitizing consumers to breach notifications and increasing the costs—and thus ultimately the price—of broadband service. Consumers would be unlikely to view any of this as a positive development.

IV. THE PROPOSED RULES WOULD BE UNLAWFUL

The proposed rules would be unlawful as well as unwise. First, they would violate the Administrative Procedure Act (“APA”) as arbitrary and capricious, in part because they ignore cost-benefit considerations. *See* Section IV.A, *infra*. Second, they would violate the First Amendment because they would unduly burden speech without adequate—indeed, any—

¹⁶⁸ 2002 CPNI Order ¶ 47. Under some state laws, the service provider or data licensee could be required to provide notice to the data owner or licensor. *See, e.g.*, 815 Ill. Comp. Stat. Ann. § 530/10; Ky. Rev. Stat. § 365.732; Okla. Stat. Ann. tit. 24, § 163; Vt. Stat. Ann. tit. 9, § 2435.

justification. *See* Section IV.B, *infra*. Third, the Commission lacks statutory authority to adopt many of these rules in the first place. *See* Section IV.C, *infra*. Finally, aspects of the proposed rules would violate several other statutory schemes, including the Cable and Satellite Acts (Section IV.D, *infra*), the Federal Arbitration Act (Section IV.E, *infra*), the Paperwork Reduction Act (Section IV.F, *infra*), and various national-security statutes (Section IV.G, *infra*).

A. The Proposed Rules Would Be Arbitrary and Capricious

Under the APA, an agency “must examine the relevant data and articulate a satisfactory explanation for its action, including a rational connection between the facts found and the choice made.”¹⁶⁹ For all of the reasons discussed above, the proposed rules flunk that basic requirement: they are irrational and unsupported by evidence. For example, insofar as the rules would subject ISPs to restrictions more onerous than those applicable to other participants in the Internet ecosystem, they are unmoored from any defensible analysis of market conditions; they purport to solve a “problem” that does not exist; they treat similarly situated parties differently without any plausible justification;¹⁷⁰ and they are profoundly over-prescriptive. We will not repeat the arguments made in previous sections of these comments; instead, we incorporate those arguments by reference here.

Nonetheless, because many of the rules would fail APA scrutiny for lack of a cost-benefit justification, it bears emphasizing that the Commission has no discretion to forgo a cost-benefit

¹⁶⁹ *Motor Vehicle Mfrs. Ass’n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) (internal quotation omitted).

¹⁷⁰ *See Burlington N. & Santa Fe Ry. v. Surface Transp. Bd.*, 403 F.3d 771, 777 (D.C. Cir. 2005) (“Where an agency applies different standards to similarly situated entities and fails to support this disparate treatment with a reasoned explanation and substantial evidence in the record, its action is arbitrary and capricious.”); *Transactive Corp. v. United States*, 91 F.3d 232, 237 (D.C. Cir. 1996) (“A long line of precedent has established that an agency action is arbitrary when the agency offered insufficient reasons for treating similar situations differently.”); *Airmark Corp. v. FAA*, 758 F.2d 685, 692 (D.C. Cir. 1985) (vacating agency orders regarding exemptions from noise regulations because the agency’s treatment of different entities was “grossly inconsistent and patently arbitrary”).

analysis. As the Supreme Court recently explained in *Michigan v. EPA*,¹⁷¹ cost-benefit comparisons are essential to reasoned decisionmaking: “Agencies have long treated cost as a centrally relevant factor when deciding whether to regulate. Consideration of cost reflects the understanding that reasonable regulation ordinarily requires paying attention to the advantages *and* the disadvantages of agency decisions.”¹⁷² There is also no “privacy” exception to the requirement for a cost-benefit analysis, as explained by Cass Sunstein, President Obama’s former OMB Administrator for the Office of Information and Regulatory Affairs. In his words, while “dignity, privacy, and other values” are plainly important to society and proper objects of reasonable regulation, they must not be played as “trump cards that would allow the agencies to escape the analytic discipline of cost-benefit analysis.”¹⁷³

Here, the Commission would violate its APA obligation to “consider an important aspect”¹⁷⁴ of privacy regulation if it does not adequately consider both the costs of regulation *and* the putative benefits, in the form of a solution to a demonstrated problem.¹⁷⁵ An agency may not impose heavy-handed regulatory “solutions” to a problem whose existence it has never substantiated.¹⁷⁶ As the Supreme Court recently explained, moreover, “not all [information-

¹⁷¹ 135 S. Ct. 2699 (2015) (emphasis in original); *see also id.* at 2707 (“[n]o regulation is ‘appropriate’ if it does significantly more harm than good”).

¹⁷² *Id.*

¹⁷³ Council on Foreign Relations, *Regulation, Behavior, and Paternalism* (June 11, 2013), <http://www.cfr.org/economics/regulation-behavior-paternalism/p35500> (transcript of discussion). Although it may be difficult to quantify the benefits of regulation designed to protect intangible values such as privacy, a regulatory agency must try to estimate them anyway and compare them against the costs; “[i]f best is unattainable second best will have to do.” *Ill. Commerce Comm’n v. FERC*, 756 F.3d 556, 565 (7th Cir. 2014).

¹⁷⁴ *State Farm*, 463 U.S. at 43.

¹⁷⁵ *Michigan*, 135 S. Ct. at 2711.

¹⁷⁶ *See, e.g., Nat’l Fuel Gas Supply Corp. v. FERC*, 468 F.3d 831, 843 (D.C. Cir. 2006); (“Professing that an order ameliorates a real industry problem but then citing no evidence demonstrating that there is in

related practices that trigger consumer objections] cause harm or present any material risk of harm.”¹⁷⁷ But the NPRM here offers no examples of consumer harm attributable to ISP data practices or even any rigorous theory of how such practices may cause such harm, let alone show how the proposed rules are needed to rectify such harm.

Nor is this one of the handful of contexts in which Congress precluded the use of a cost-benefit analysis by enacting rigid statutory imperatives.¹⁷⁸ To the extent that Section 222 applies to ISPs in the first place, *see* Section IV.C, *infra*, Congress gave the Commission considerable room to implement that provision in a manner that minimizes costs while preserving consumer benefits and thus approximates the FTC’s approach. For example, Congress specified that “approval of the customer” must take the form of opt-in consent (“express prior authorization”) in only two contexts: access to “call location information” for cellular and VoIP telephone calls and certain uses of “automatic crash notification information.”¹⁷⁹ The Commission otherwise has no statutory obligation to require opt-in consent and may permit the less intrusive opt-out

fact an industry problem is not reasoned decisionmaking.”); *Fox TV Stations, Inc. v. FCC*, 280 F.3d 1027, 1051 (D.C. Cir. 2002) (“A single incident . . . —and one that seems to have been dealt with adequately under [existing] rules—is just not enough to suggest an otherwise significant problem”); *Associated Gas Distribs. v. FERC*, 824 F.2d 981, 1019 (D.C. Cir. 1987) (agency lacks any basis for fashioning “an industry-wide solution for a problem that exists only in isolated pockets,” and “the disproportion of remedy to ailment” is therefore arbitrary and capricious).

¹⁷⁷ *Spokeo, Inc. v. Robins*, No. 13-1339, slip op. 11 (U.S. May 16, 2016) (holding that to have Article III standing, privacy plaintiff must demonstrate “injury-in-fact” that is “concrete and particularized” and “actual or imminent, not conjectural or hypothetical”).

¹⁷⁸ *Cf. Public Citizen v. Young*, 831 F.2d 1108 (D.C. Cir. 1987) (holding that the Delaney Clause of the Food, Drug and Cosmetic Act categorically prohibits color dyes posing any risk of cancer to humans or animals, with no de minimis exception for dyes posing only trivial risks to humans).

¹⁷⁹ 47 U.S.C. § 222(f).

approach wherever Section 222 requires “approval of the customer” (as indeed the Commission has done in a variety of contexts).¹⁸⁰

B. The Proposed Rules Would Violate the First Amendment

As discussed, the proposed rules would fail ordinary APA review even if they raised no First Amendment concerns. But the rules proposed in the NPRM, including the broad proposed opt-in requirements, do raise such concerns because they would impede the flow of truthful commercial information and would therefore trigger even more exacting judicial review than typical APA claims do.¹⁸¹ The Commission would thus face severe litigation risks if, in implementing the open-ended terms of Section 222, it saddles ISPs with more onerous speech restrictions than apply to other participants in the Internet ecosystem. The Commission would bear the burden of justifying those incremental restrictions, and it could not meet “[t]his burden ... by mere speculation or conjecture; rather, a governmental body seeking to sustain a restriction on speech must demonstrate that the harms it recites are real and that its restriction will in fact alleviate them to a material degree.”¹⁸² Similarly, the “canon of constitutional avoidance”—which requires resolving any statutory ambiguities to avoid constitutional

¹⁸⁰ See Section I, *supra*. In any event, the Commission can and should use its Section 10 authority to forbear from any statutory requirement that it concludes would obstruct its ability to adopt a flexible privacy regime in harmony with the FTC’s longstanding approach. For the reasons discussed throughout these comments, the statutory criteria are met because privacy-related regulatory burdens more restrictive than those long enforced under the FTC’s regime “are not necessary to ensure that” ISP privacy practices “are just and reasonable and are not unjustly or unreasonably discriminatory,” because such burdens are “not necessary for the protection of consumers,” and because forbearance from such burdens is “consistent with the public interest.” 47 U.S.C. § 160(a)(1)-(3).

¹⁸¹ See, e.g., *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011).

¹⁸² *Edwards v. District of Columbia*, 755 F.3d 996, 1003 (D.C. Cir. 2014) (quoting *Edenfield v. Fane*, 507 U.S. 761, 770-71 (1993)) (internal ellipsis omitted); see also *Greater New Orleans Broadcasting v. United States*, 527 U.S. 173, 183 (1999) (“the Government bears the burden of identifying a substantial interest and justifying the challenged restriction”).

concerns—“trumps *Chevron* deference, ... and [courts] will not submit to an agency’s interpretation of a statute if it ‘presents serious constitutional difficulties.’”¹⁸³

It is particularly well-settled that the Commission faces rigorous judicial scrutiny if it chooses opt-in rather than opt-out consent requirements for marketing by telecommunications carriers. As a threshold matter, the proposed opt-in requirements are subject to strict scrutiny because they would discriminate against certain speakers (ISPs) and against certain subject matter (truthful messages concerning “non-communications-related” services).¹⁸⁵ But the precise level of scrutiny is immaterial because the proposed rules would violate even the somewhat less exacting *Central Hudson* standard.¹⁸⁶ Under that standard, the Commission may impose an opt-in rather than opt-out requirement only if, at a minimum, (1) it has a “substantial interest” it seeks to vindicate, (2) the opt-in requirement “directly advances” that interest, and

¹⁸³ *Nat’l Mining Ass’n v. Kempthorne*, 512 F.3d 702, 711 (D.C. Cir. 2008) (quoting *Chamber of Commerce v. FEC*, 69 F.3d 600, 605 (D.C. Cir. 1995)); see also *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575-76 (1988) (refusing to defer to NLRB interpretation of statute because it raised serious First Amendment issues); *Public Citizen v. Dep’t of Justice*, 491 U.S. 440, 466 (1989) (“[i]t has long been an axiom of statutory interpretation that where an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress”) (internal quotation marks omitted).

¹⁸⁴ See 2002 CPNI Order ¶ 29 (“[A]ny new [CPNI rules] ... must meet the standard articulated by the Supreme Court in *Central Hudson*”); Report and Order, *Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, 22 FCC Rcd 6927, ¶ 44 (2007) (“2007 EPIC CPNI Order”) (acknowledging a “burden of showing” that its CPNI rules “pass[] the *Central Hudson* test”).

¹⁸⁵ See *Sorrell*, 131 S. Ct. at 2663, 2667 (invalidating a law that imposed “content- and speaker-based restrictions on the sale, disclosure, and use of prescriber-identifying information,” noting that “[i]n the ordinary case it is all but dispositive to conclude that a law is content-based,” yet declining to specify the precise standard of review because “the outcome is the same whether a special commercial speech inquiry or a stricter form of judicial scrutiny is applied”); *Retail Digital Network, LLC v. Appelsmith*, 810 F.3d 638, 648 (9th Cir. 2016) (“*Sorrell* modified the *Central Hudson* test for laws burdening commercial speech” where the law “is content- or speaker-based”), *reh’g pet. filed*, No. 13-56069 (9th Cir. Mar. 21, 2016).

¹⁸⁶ *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm’n*, 447 U.S. 557, 564-66 (1980).

(3) the requirement is “not more extensive than is necessary to serve that interest.”¹⁸⁷ The Tenth Circuit invalidated the Commission’s initial attempt to impose opt-in requirements in this context because, it held, the Commission had “fail[ed] to meet its burden” of justification under both the second and third prongs of the *Central Hudson* analysis.¹⁸⁸ That holding comports with a long line of Supreme Court precedent addressing the constitutionally problematic “deterrent effect[s]” that the government imposes on information flows when it conditions speech on a recipient’s prior affirmative consent to be spoken to.¹⁸⁹

The broad opt-in requirements proposed in the NPRM would likewise fail the *Central Hudson* test. Indeed, they would fail all three prongs.

First, although the Commission may have a “substantial” government interest in “protecting people from the disclosure” of personal information, *U.S. West*, 182 F.3d at 1236 (assuming point *arguendo*), that interest has nothing to do with the proposed opt-in rules, which do not focus on “disclosure” to begin with. They focus instead on how an ISP may *use* information already lawfully in its possession—and, in particular, whether the ISP may use that

¹⁸⁷ *Central Hudson*, 447 U.S. at 564-66. To qualify for *Central Hudson* protection, commercial speech must be lawful and non-misleading. The commercial messages at issue here indisputably qualify as such. *See, e.g., U.S. West*, 182 F.2d at 1234 (“no one disputes that the commercial speech based on CPNI is truthful and nonmisleading”); *2002 CPNI Order* ¶ 27 n.80 (“the commercial speech impacted by the Commission’s CPNI rules is neither misleading nor does it involve illegal activities”).

¹⁸⁸ *U.S. West*, 182 F.3d at 1237-39.

¹⁸⁹ *Lamont v. Postmaster General*, 381 U.S. 301, 307 (1965) (striking down federal law requiring addressees of “communist political propaganda” from foreign countries affirmatively to request delivery of such mail); *see United States v. Playboy Enter. Group, Inc.*, 529 U.S. 803, 816, 824 (2000) (invalidating statutory restrictions on access to sexually explicit channels, enacted to protect children of non-subscribers, on the ground that a “less restrictive alternative [wa]s available” in that parents could individually block (opt out of) such programming); *Denver Area Educ. Telecomm’ns Consortium, Inc. v. FCC*, 518 U.S. 727, 753-54 (1996) (striking down federal law requiring cable system operators to block certain sex-related material and then require subscribers affirmatively to request “unblocking” if they wish to view the material, because these requirements “have obvious restrictive effects,” “will further restrict viewing by subscribers,” and impose “added costs and burdens” on cable system operators).

information to increase the relevance of advertisements and other commercial messages sent to its customers. In some cases, the ISP may send advertisements for its own services; for example, AT&T might wish to use its database of existing ISP subscribers and their email addresses to market an AT&T-branded home-security system. In other cases, the ISP may pass through third-party advertisements to specific customers who would be most interested in them, based on customer information that *the ISP* already has in its possession but that it does not share with *the third-party advertisers* themselves. In each of these scenarios, the information itself remains confined to the ISP. Requiring opt-in consent would thus have no effect on access to the information, but would merely burden the ability of ISPs and third parties to increase the relevance of the commercial messages they send to ISP customers. The Commission has neither articulated nor justified any valid governmental interest in imposing that burden and thereby degrading the relevance of the commercial speech that ISPs and third parties can direct to particular customers.¹⁹⁰

The opt-in rules would similarly fail *Central Hudson*'s second prong, which requires that commercial speech restrictions "directly advance" the proffered state interest (here, protecting consumer privacy). Even if there were a genuine "privacy" problem that opt-in rules might theoretically solve, the NPRM's proposed rules would do nothing to solve it because, as discussed, they are radically underinclusive. Specifically, they would apply only to ISPs and not to the myriad other companies that, with or without the rules, will go on tracking, using, and selling all of the same online consumer information. Such underinclusiveness is fatal to commercial speech restrictions, both because it "raises serious doubts about whether the

¹⁹⁰ Significantly, the question here is not the *volume* of commercial messages that consumers see, which enactment of the proposed rules would not reduce. The question instead is *how relevant* those messages will be to particular consumers.

government is in fact pursuing the interest it invokes”¹⁹¹ and because, in any event, it shows that the restrictions would be “ineffective” in furthering the government’s stated purposes.¹⁹² These constitutional concerns are particularly acute where, as here, the government proposes to “single[] out” specific market participants for “disfavored treatment” with respect to constitutionally protected speech and “has given no persuasive reason why.”¹⁹³

Again, the Commission cannot fix these constitutional defects simply by asserting that ISPs present greater privacy concerns than other online companies. There is no empirical basis for such an argument because, as discussed, ISPs have access to *less* sensitive and *less* comprehensive consumer information than do more established data-use players such as Google, and consumers find it easier to switch among ISPs than to abandon webmail or social media accounts. *See* Tech. Background, *supra*; Section I, *supra*. The Commission would fare no better if it tried to justify targeting this arbitrarily defined subset of companies for special speech burdens on the ground that its statutory authority extends only to those companies and not to all the other companies that are similarly situated from a consumer privacy perspective. No matter what the reason, the government cannot burden commercial speech ostensibly to pursue cited policy objectives if the speech restrictions, because of their underinclusiveness, would not

¹⁹¹ *Brown v. Entm’t Merchants Ass’n*, 564 U.S. 784, 802 (2011) (citing cases); *accord Rubin v. Coors Brewing Co.*, 514 U.S. 476, 489 (1995) (“exemptions and inconsistencies bring into question the purpose of” a speech restriction).

¹⁹² *Central Hudson*, 447 U.S. at 564 (a regulation “may not be sustained if it provides only ineffective or remote support for the government’s purpose”); *accord Greater New Orleans Broadcasting*, 527 U.S. at 190 (regulatory regime could not advance asserted governmental interests when the regime was “pierced by exemptions and inconsistencies”).

¹⁹³ *Brown*, 564 U.S. at 802 (striking down under the First Amendment a California law that singled out “violent” content in the wares of video game purveyors as “compared to booksellers, cartoonists, and movie producers”); *see also Sorrell*, 131 S. Ct. at 2663; *Greater New Orleans Broadcasting*, 527 U.S. at 193-94 (“in commercial speech cases, decisions that select among speakers conveying virtually identical messages are in serious tension with the principles under girding the First Amendment”).

substantially promote those objectives in the first place.¹⁹⁴ More generally, the First Amendment prohibits the government writ large from applying unreasonably underinclusive speech regulations against some speakers but not others, and the government cannot justify such underinclusiveness simply by invoking the jurisdictional limitations that it imposed on the various instrumentalities it created.¹⁹⁵

The NPRM’s expansive opt-in requirements would likewise fail the third prong of the *Central Hudson* test, under which commercial speech restrictions must be “narrowly tailored” to serve the stated government interest and “may extend only as far as the interest it serves.”¹⁹⁶ Under that prong, there must be a “fit” between the government’s means and its desired end—“a fit that is not necessarily perfect, but reasonable; that represents not necessarily the single best disposition but one whose scope is in proportion to the interest served.”¹⁹⁷

Here, while an opt-in requirement might be a reasonable restriction on sharing sensitive personal information with third parties, the opt-in requirement proposed here would draw none of the basic distinctions that apply everywhere else in the Internet ecosystem, such as distinctions based on whether customer information is sensitive¹⁹⁸ and whether it is shared with third

¹⁹⁴ See, e.g., *Edenfield v. Fane*, 507 U.S. 761, 770-71 (1993) (government must demonstrate that speech restriction “will in fact alleviate [alleged harms] to a material degree”).

¹⁹⁵ See *Rubin*, 514 U.S. at 488 (federal law prohibiting beer labels from displaying alcohol content did not advance purported government interest in preventing brewers from engaging in “strength wars” to promote their products because the majority of state laws allowed the disclosure of alcohol content in beer advertising).

¹⁹⁶ 447 U.S. at 564-65 (internal quotation omitted).

¹⁹⁷ *Bd. of Trustees of the State Univ. of N.Y. v. Fox*, 492 U.S. 469, 480 (1989) (internal quotation omitted).

¹⁹⁸ See *2012 FTC Privacy Report* at 47 (discussing need for special safeguards for “sensitive data” such as “data about children, financial and health information, Social Security numbers, and certain [very precise] geolocation data”).

parties.¹⁹⁹ Instead, the proposed requirement would ham-handedly apply to any use by an ISP of any customer information to market anything (whether an ISP's own service or a third party's) that does not fall within the arbitrarily defined category of "communications-related services." Depending on how the Commission defines that term, the proposed opt-in requirement might apply whenever an ISP uses its customers' nonsensitive information (such as their names and email addresses) to offer them, for example, its own branded home-alarm system or mobile applications.

If the government has any interest at all in "protecting" consumers from such unobjectionable uses of nonsensitive information, an opt-out mechanism is readily available to serve that exceptionally attenuated interest. If any consumers actually do object to such uses, they are likely so unusually attentive to "privacy" issues that they can be expected to seek that mechanism out and avail themselves of it.²⁰⁰ And under *Central Hudson's* third prong, the availability of that less restrictive alternative bars the government from suppressing truthful commercial speech through a one-size-fits-all opt-in requirement.²⁰¹ The proposed rules would also fail the narrow-tailoring test for the independent reason that they would restrict commercial speech on the basis of information that is not genuinely private in any meaning of the word, such as subscriber names or device types.

¹⁹⁹ See *id.* at 44 (noting that generally there is no need for any consumer consent mechanism "if the first party does not share information with third parties or track consumers across third-party websites").

²⁰⁰ See Wright White Paper at 16-17.

²⁰¹ 2002 CPNI Order ¶ 30 (*U.S. West* and *Central Hudson* require the FCC to "take into account the burden on carriers' commercial speech rights" and "consider whether opt-out provides sufficient protection of consumer privacy"); *id.* ¶ 31 (adopting "an opt-out rule" as "a less restrictive alternative ... which is less burdensome on commercial speech" than "the more stringent opt-in rule").

The Commission could find no support for its proposed rules in the D.C. Circuit’s 2009 decision in *NCTA v. FCC*,²⁰² which upheld certain telephony-oriented opt-in rules that the Commission had imposed in 2002 and modified in 2007. First, the rules upheld there “required opt-in consent only with respect to a carrier’s *sharing* of customer information with *third-party marketers*.”²⁰³ Indeed, the court found that information-sharing feature essential to distinguishing the Tenth Circuit’s *U.S. West* decision. As it explained, “[t]he evidence showed that customers were less willing to have their information shared with third parties as opposed to affiliated entities,” and the Commission “reasonably concluded that customer information would be at a greater risk of disclosure once out of the control of the carriers and in the hands of entities not subject to § 222.”²⁰⁴ In contrast, the opt-in requirements proposed here would apply whenever an ISP seeks merely to *use* consumer information to market “non-communications-related services,” even in the vast majority of cases in which the ISP would not share the data with third parties. In addition, the rules upheld in *NCTA* faced no underbreadth challenge and no claim that they irrationally discriminated against telecommunications carriers vis-a-vis other providers that systematically collected and used the same consumer information. As discussed, those are key constitutional defects in the proposed rules.

In addition, the challengers in *NCTA* both (1) “conced[ed] the constitutionality of § 222” and (2) abandoned any claim under the first prong of *Central Hudson* that the government had a relevant “substantial interest” to invoke,²⁰⁵ whereas we make neither concession here. Insofar as the Commission purports to apply Section 222 to impose a broad opt-in requirement, or claims

²⁰² 555 F.3d 996 (D.C. Cir. 2009).

²⁰³ *Id.* at 1002 (emphasis added).

²⁰⁴ *Id.*

²⁰⁵ *Id.* at 1000-1001.

that Section 222 forces it to impose requirements that fail the *Central Hudson* test, we challenge Section 222 as so applied. We likewise challenge the proposed rules under *Central Hudson*'s first prong (as well as its second and third) because as discussed, the Commission has identified no substantial interest to be served by keeping ISPs from using their existing (unshared) databases to increase the relevance of the commercial messages their customers see.

Quite apart from the proposed opt-in requirement, other aspects of the proposed rules would likewise violate the First Amendment.²⁰⁶ For example, the NPRM asks (at ¶¶ 157-159) whether the Commission should narrowly construe the statutory exemption authorizing telecommunications carriers to “use, disclose, or permit access to aggregate customer information”²⁰⁷ or, by the same token, should expansively construe what it means for CPNI to be “individually identifiable” and thus subject to the restrictions of Section 222(c)(1). Those proposals would violate the plain language of that provision and are without merit for the reasons discussed in Section II, above. They would also violate the First Amendment principles that the Supreme Court adopted in *Sorrell* when it invalidated similar restrictions on the disclosure of information used in marketing. For example, if the Commission sought to restrict or burden the dissemination of aggregate information, it would trigger (and fail) at least *Central Hudson* scrutiny insofar as the dissemination of that information is viewed as commercial speech and would trigger (and *a fortiori* fail) strict scrutiny insofar as it is viewed as noncommercial speech.

Finally, any speech-restrictive interpretation of Section 222 (or any other provision)—including any interpretation of the word “proprietary” to extend beyond trade secrets—would

²⁰⁶ If the Commission banned companies from offering discounts to win opt-in consent from consumers to use their information, *see* Section I.B.4, *supra*, it would violate the First Amendment for all the reasons discussed in this section. Indeed, the invalidity of such a prohibition would follow *a fortiori* from the invalidity of an opt-in requirement.

²⁰⁷ 47 U.S.C. § 222(c)(3).

yield to the principle of constitutional avoidance, which (as discussed) requires construing statutory provisions to avoid raising First Amendment concerns.

C. The Commission Lacks Statutory Authority to Address Key Subject Areas in Which the NPRM Proposes Rules

The preceding two sections demonstrated that, even if the Commission has statutory authority to regulate ISP data practices, the Commission could not reasonably or constitutionally exercise that authority to subject ISPs to restrictions more burdensome than those that apply to other participants in the Internet ecosystem. This section, by contrast, argues that the Commission generally lacks statutory authority to regulate ISP data practices in the first place.²⁰⁸

1. *The Statutory Category of “CPNI” Excludes Any Information Category That Is Widely Accessible to Non-ISP Companies Operating Online*

Most of the customer information that the Commission seeks to regulate in this proceeding—specifically, any type of information that is broadly collected and used by non-ISP entities—does not qualify for protection under any provision of Section 222 because it is not “proprietary” in any relevant sense of the word.

Congress enacted Section 222 in 1996 for two purposes: to keep local telephone monopolies from leveraging their unique access to other carriers’ “proprietary information” to gain an anticompetitive advantage in adjacent markets (such as interexchange services), *see* 47 U.S.C. § 222(b), and to protect consumers’ interest in the privacy of “individually identifiable customer proprietary network information,” *see id.* § 222(c). In either context, information must

²⁰⁸ For purposes of this discussion, AT&T assumes *arguendo* that broadband Internet access service is properly classified as a Title II telecommunications service, but it preserves its argument that this classification is erroneous.

be “proprietary” to trigger statutory protection. And to be proprietary, information cannot be freely available to the public; it must be kept confidential.²⁰⁹

That is an apt characterization for traditional telephone records. For a typical PSTN call, the only parties privy to the call (other than the calling and called parties) are the local exchange carriers on either end and, for some calls, an interexchange carrier in the middle. Congress passed Section 222(c) in 1996 to keep such carriers from disclosing call details (such as who called whom, when, and for how long) to anyone else without customer consent. Congress generally had no need for concern about disclosure by any third party *not* covered by the CPNI rules because (absent wiretapping) there was typically no such third party; there was simply a closed universe of carriers subject to Section 222(c).²¹⁰

In contrast, when a typical ISP end user today uses a search engine and visits a webpage, any number of unregulated third parties track his movements, including his browser (e.g., Google Chrome), the search engine (e.g., Google), the webpage (e.g., Amazon), the content delivery network serving the webpage (e.g., Akamai), and any number of data brokers (e.g., Acxiom) that sell the end user’s online information to others. These various third parties often have far more comprehensive information about the end user than his ISP does, and the ISP “sees” only a limited subset of what they see. *See* Tech. Background, *supra*. Moreover, these third parties are not subject to the Commission’s CPNI rules, and no one argues that they should be. In short, there is thus nothing confidential, and thus nothing “proprietary,” about information

²⁰⁹ *See, e.g., Black’s Law Dictionary* 1414 (10th ed. 2014) (defining “proprietary information” as “[i]nformation in which the owner has a protective interest. *See* TRADE SECRET.”); *Inc. Encyclopedia, Proprietary Information* (“Courts will not treat information readily available in public sources as proprietary.”), <http://www.inc.com/encyclopedia/proprietary-information.html> (visited Apr. 25, 2016).

²¹⁰ Congress separately addressed wiretapping in Title III of the Omnibus Crime Control and Safe Streets Act of 1968. *See* 18 U.S.C. §§ 2510-22. No legislation imposes comparably effective restrictions on widespread commercial access to information about Internet communications.

accessible not only to ISPs, but more broadly to other entities throughout the Internet ecosystem. And because such information is not proprietary, it does not qualify as CPNI, and it falls outside the ambit of Section 222.

Finally, even though “customer proprietary network information” is a defined statutory term, the plain meaning of “proprietary” must still be considered in construing the scope of that term. When Congress provides a statutory definition of a phrase, the plain meanings of the phrase’s constituent words still have “the import of showing us what Congress had in mind” when using that phrase.²¹¹ And here the statutory definition itself comports with the meaning of its constituent words and supports the conclusion that non-confidential information cannot be “CPNI.” Section 222(h)(1) defines “consumer proprietary network information” as certain information that is “made available” to a telecommunications carrier “solely by virtue of the carrier-customer relationship.”²¹² But, in many instances, an ISP need not rely on its own relationship with its customers to collect information about their online activities because it could obtain the same information independently (at a price) from data brokers or other unregulated third parties.²¹³ Even standing alone, therefore, the statutory definition tends to confirm the same conclusion suggested by Congress’s use of the term “proprietary”: information is not “customer *proprietary* network information” under Section 222 if it is not genuinely confidential because it widely available outside of the carrier-customer relationship.

These considerations illustrate a glaring anomaly at the heart of the proposed rules. The Commission’s proposed rules would thus bar an ISP from making use of customer information

²¹¹ See *Solid Waste Agency v. U.S. Army Corps of Engineers*, 531 U.S. 159, 173 (2001).

²¹² 47 U.S.C. § 222(h)(1).

²¹³ For example, an ISP can obtain information about its customers’ browsing history and location from third-party data brokers, which collect such data from those customers’ visits to particular websites or from applications that collect such data. See Tech. Background, *supra*.

unless it pays to obtain the same information from one of the many unregulated companies that already have the same information—and whom the proposed rules would thus shield from competition by ISPs. Any reading of Section 222 that would produce this bizarre outcome is untenable, both because statutes must be construed to avoid absurd results and because, as discussed above, they must also be construed to avoid raising constitutional concerns about the free flow of truthful commercial information.²¹⁴

2. *Section 222 Authorizes the Commission to Regulate Only CPNI, Not Some Broader Category of “Personal Information”*

Contrary to the NPRM’s suggestion,²¹⁵ Section 222(a) grants the Commission no legal authority to “protect customer information that is not CPNI” and thus would not authorize the Commission to regulate the collection and use of such information even if (despite the immediately preceding discussion) the information otherwise qualified as “proprietary.” Section 222 thus encompasses only the information categories listed in Section 222(h)—“the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service”—and not other categories of customer information collected by ISPs, such as names, email addresses, and mailing addresses. And even if Section 222(a) did authorize the Commission to address such non-CPNI customer information, it could not support the proposed rules to the extent that they address only the *uses* of that information rather than the protection of its confidentiality.

a. Section 222(a), titled “In general,” provides that “[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other

²¹⁴ See, e.g., *Public Citizen*, 491 U.S. at 466; *DeBartolo Corp.*, 485 U.S. at 575-76.

²¹⁵ *NPRM* ¶ 300; see also *id.* ¶ 299 (“the set of customer information protected by Section 222(a) is broader than CPNI”); *id.* ¶ 298 (Section 222(a) imposes a “duty to secure the confidentiality of customer information beyond CPNI”).

telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunication carrier.” Sections 222(b) and (c) then set forth telecommunications carriers’ obligations with respect to “[c]onfidentiality of carrier information,” and “[c]onfidentiality of customer proprietary network information,” respectively. Within this statutory structure, subsection (a) merely confirms Congress’s intent to hold all telecommunications carriers to the requirements specified in subsections (b) and (c) and thus extends those requirements to carriers other than AT&T, the BOCs, and GTE—the subjects of the pre-1996 CPNI regulations under the *Computer Inquiries*.²¹⁶ In short, Section 222(a) identifies *who* has duties under Section 222, while Sections (b) and (c) specify *what* those duties are.

The Commission itself has embraced that interpretation until very recently.²¹⁷ As it explained, “the Commission ... established CPNI requirements [before 1996] applicable to the enhanced services operations of AT&T, the BOCs, and GTE,” designed both “to protect independent enhanced services providers and [customer premises equipment] suppliers from discrimination” and “to protect legitimate customer expectations of confidentiality.”²¹⁸ After Congress enacted Section 222, the Commission observed that subsection (a) of that provision was enacted to “recognize the duty of *all* carriers to protect customer information.”²¹⁹ And the

²¹⁶ See generally *1998 CPNI Order* ¶ 7 (describing pre-1996 CPNI rules).

²¹⁷ Not until 2014 did the Commission first suggest that Section 222(a) reaches information other than CPNI. See Notice of Apparent Liability, *TerraCom, Inc. and YourTel America, Inc.*, 29 FCC Rcd 13325 (2014) (“*TerraCom NAL*”). That interpretation is implausible, and should be rejected, for the reasons discussed in the text.

²¹⁸ *1998 CPNI Order* ¶ 7; see also *NPRM* ¶ 298.

²¹⁹ *1998 CPNI Order* ¶ 3 & n.10 (emphasis in original).

Commission has repeatedly described “CPNI” as the entire subject matter addressed by Section 222, including Section 222(a).²²⁰

The NPRM acknowledges (at ¶ 298) that earlier Commission decisions “could be read to imply that CPNI is the only type of customer information protected” by Section 222, and offers the explanation that “those decisions simply did not need to address the broader protections offered by Section 222(a).” But courts are rightly skeptical about any agency’s claim that it overlooked a key aspect of a statutory scheme for decades and has only recently discovered previously unknown authority lurking within its language.²²¹ The more plausible explanation is that the agency overlooked that authority because it does not exist. That conclusion is particularly compelling here because the NPRM’s interpretation of Section 222(a) would create several glaring statutory anomalies that Congress could not have intended.

First, Section 222(d), titled “Exceptions,” provides that Section 222 does not prohibit telecommunications carriers from using or disclosing “customer proprietary network information” for the purposes of billing, protecting their networks and customers from fraud and abuse, and providing call location information in certain emergency situations. These exceptions

²²⁰ See 2007 *EPIC CPNI Order* ¶ 6 (“Every telecommunications carrier has a general duty pursuant to Section 222(a) to protect the confidentiality of CPNI.”); 1998 *CPNI Order* ¶ 208 (describing “the duty in section 222(a) upon all telecommunications carriers to protect the confidentiality of customers’ CPNI”); 1998 *CPNI Order* ¶ 2 (“Section 222 sets forth three categories of customer information to which different privacy protections and carrier obligations apply – individually identifiable CPNI, aggregate customer information, and subscriber list information.”); see also *U.S. West*, 182 F.2d at 1228 n.1 (“The statute recognizes three types of customer information: (1) CPNI; (2) aggregate customer information; and (3) subscriber list information.”); 2002 *CPNI Order* ¶ 6 (“[S]ection 222 establishes three categories of customer information to which different privacy protections and carrier obligations apply: (1) individually identifiable CPNI, (2) aggregate customer information, and (3) subscriber list information.”).

²²¹ *American Library Ass’n v. FCC*, 406 F.3d 689, 691, 704, 708 (D.C. Cir. 2005) (rejecting Commission assertion of “sweeping authority” to regulate that it had “never before asserted”); accord *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 159 (2000) (rejecting FDA’s position that the Food, Drug, and Cosmetic Act gave it jurisdiction to regulate tobacco products because, “[c]ontrary to its representations to Congress since 1914, the FDA has now asserted jurisdiction to regulate an industry constituting a significant portion of the American economy”).

all serve critical purposes, but they apply only to carriers' use and disclosure of CPNI. Thus, if 222(a) applied to non-CPNI "proprietary information," as the NPRM contends, it would be subject to no exceptions permitting the use of such information for billing, fraud prevention, and emergency services. Under that approach, carriers could use and share CPNI to prevent network harm and assist emergency responders, but they could not use or share non-CPNI "proprietary information" for these same purposes. In an apparent effort to avoid this anomaly, the NPRM proposes (at ¶ 120) "to expand the exceptions in Section 222(d) in the broadband context to permit broadband providers to use all customer PI for these delineated purposes." But the Commission lacks statutory authority to "expand" those exceptions beyond CPNI when Congress explicitly limited them to CPNI. In all events, Congress certainly would not have written Section 222(d) as it did had it intended for Section 222 to cover non-CPNI customer information.

Sections 222(e) and 222(g) further illustrate the absurd consequences of construing Section 222(a) as the NPRM proposes. Section 222(e), titled "Subscriber list information," provides that, "[n]otwithstanding subsections (b), (c), and (d)" of Section 222, telecommunications carriers that provide telephone exchange service must provide subscriber list information²²² on a reasonable and nondiscriminatory basis to those who publish directories.²²³ Likewise, Section 222(g), titled "Subscriber listed and unlisted information for emergency services," states that, "[n]otwithstanding subsections (b), (c), and (d)," telecommunications carriers must provide subscriber list information on a reasonable and nondiscriminatory basis to providers of emergency services and emergency support services. But if Section 222(a) protects

²²² See 47 U.S.C. § 222(h)(3) (defining "subscriber list information" to include names, addresses, and telephone numbers of subscribers).

²²³ 47 U.S.C. § 222(e).

customer personal information beyond CPNI, Congress would logically have included that subsection—along with subsections (b), (c), and (d)—in the list of subsections that Sections 222(e) and 222(g) trump. Indeed, it would have been essential for Congress to have included Section 222(a) in order to avoid a conflict between that section (which, under the Commission’s interpretation, requires carriers to protect the confidentiality of proprietary customer information) and Sections 222(e) and 222(g) (which require carriers who provide telephone exchange service to disclose such information on a non-discriminatory basis). Congress’s failure to do so confirms that the NPRM’s interpretation of Section 222(a) is implausible.

The legislative history also confirms that Section 222 extends no further than CPNI. As explained in the Conference Report, “the new section 222 strives to balance both competitive and consumer privacy interests *with respect to CPNI*.”²²⁴ Significantly, prior versions of Section 222 did cover a much broader category of information. For example, the House version included a “catch-all” category in the CPNI definition (in addition to the information currently covered in Section 222(h)(1)) that would have encompassed “such other information concerning the customer as is available to the local exchange carrier by virtue of the customer’s use of the carrier’s telephone exchange service or telephone toll services, and specified as within the definition of such term by such rules as the Commission shall prescribe consistent with the public interest.”²²⁵ But that approach, which would have given the Commission broader power to regulate the use and disclosure of customer information, was ultimately rejected in favor of the more circumscribed CPNI definition found in Section 222(h)(1).

²²⁴ H.R. Rep. No. 104-458, at 205 (1996) (Conf. Rep.) (emphasis added).

²²⁵ H.R. Rep. No. 104-204, Pt. I, 104th Cong., 1st Sess., at 23 (1995).

b. In any event, even if Section 222(a) did apply to non-CPNI customer information, it could not support the majority of the rules the Commission seeks to impose on the use of such information. By its terms, Section 222(a) addresses only the duty of telecommunications carriers “to protect the confidentiality” of the information within its scope. But many of the proposed rules have nothing to do with confidentiality concerns and instead address only the *uses* of information within an ISP’s possession. Thus, even if Section 222(a) required ISPs to protect the confidentiality of non-CPNI customer information, it still would not authorize the Commission to regulate how an ISP obtains its customers’ consent (i.e., opt-in or out-out) to use that information in tailoring particular messages to those customers without sharing customer-specific information with third parties. Nor could the Commission invoke Section 222(a) to prohibit ISPs from obtaining information about its customers from third parties and combining it for marketing purposes with information it has already collected about those customers (while taking due precautions to keep individually identifiable information confidential).

3. *Other Miscellaneous Provisions of the Communications Act Do Not Authorize the Commission to Adopt the Regime Proposed in the NPRM*

The Commission asserts (at ¶ 294) that its proposed rules would be “primarily grounded in Section 222,” but asks whether it could alternatively find authority for them in an assortment of other statutory provisions, including Sections 201, 202, and 705 of the Communications Act and Section 706 of the Telecommunications Act of 1996. The answer is no.

Section 201(b). Section 201(b) provides that “[a]ll charges, practices, classifications, and regulations for and in connection with such communication service, shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is

declared to be unlawful.”²²⁶ That provision is inapplicable here because, under established principles of statutory construction, more general statutory provisions are unavailable as sources of regulatory authority where Congress has adopted a comprehensive and much more specific provision to address the subject matter at issue.²²⁷ Here, Section 222 reflects Congress’s considered decisions about which consumer privacy protections are necessary and which are not. The Commission cannot simply ignore those decisions by invoking Section 201(b) to create privacy-related rules that, in Section 222, Congress could have authorized the Commission to adopt but chose not to.

In any event, in construing Section 201(b)’s ban on unjust and unreasonable prices and practices “in connection with” communications services, courts must find “a limiting principle consistent with the structure of the statute and its other provisions.”²²⁸ Here, placing privacy practices within the ambit of Section 201 would defy any reasonable limiting principle because such practices are not an inherent or necessary aspect of providing communications services. Indeed, when Congress sought to regulate them in the telecommunications context—more than 60 years after it passed the 1934 Act—it saw the need to supplement the Act’s general provisions with a new provision (Section 222). In Commissioner O’Rielly’s words, “[i]f data protection falls within the ambit of 201(b),” one “can only imagine what else might be a practice ‘in connection with’ a communications service.”²²⁹

²²⁶ 47 U.S.C. § 201(b).

²²⁷ See, e.g., *Bloate v. United States*, 130 S. Ct. 1345, 1354 (2010) (“There is no question that . . . ‘[g]eneral language of a statutory provision, although broad enough to include it, will not be held to apply to a matter specifically dealt with in another part of the same enactment.’”) (quoting *D. Ginsberg & Sons, Inc. v. Popkin*, 285 U.S. 204, 208 (1932)).

²²⁸ *Maracich v. Spears*, 133 S. Ct. 2191, 2200 (2013) (interpreting phrase “in connection with” in the Driver’s Privacy Protection Act of 1994).

²²⁹ See *TerraCom NAL*, 29 FCC Rcd at 13353 (dissenting statement of Commissioner O’Rielly).

Section 202. It is unclear why the NPRM seeks comment on the relevance of Section 202, which prohibits “unjust or unreasonable discrimination” by carriers in their prices, practices, and services.²³⁰ The NPRM makes no attempt to justify any of the proposed rules on the ground that they would combat “unreasonable discrimination.” Instead, the Commission relies upon broad policy rationales about consumer privacy that have nothing to do with discrimination concerns.

Section 705. Section 705(a) provides that, subject to criminal penalties and civil liability, “no person receiving, assisting in receiving, transmitting, or assisting in transmitting” shall “divulge or publish the existence, contents, substance, purport, effect, or meaning” of interstate communications.²³¹ But this narrow prohibition on divulging the content of customer communications cannot provide legal authority for the vast majority of proposed rules in the NPRM, which addresses the “content of consumer communications” only in a single paragraph (§ 67). Moreover, because Section 705 is accompanied by criminal penalties, any effort by the Commission to construe this provision broadly would collide not only with the First Amendment, *see* Section IV.B, *supra*, but also with due process and the rule of lenity, under which “ambiguous criminal laws [must] be interpreted in favor of ... defendants.”²³²

Section 706. It is at best ironic that the Commission has sought comment on whether Section 706 authorizes it to adopt the proposed rules because, in fact, the rules would affirmatively violate that provision. Section 706 directs the Commission to “encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all

²³⁰ 47 U.S.C. § 202(b).

²³¹ *Id.* § 605(a).

²³² *United States v. Santos*, 553 U.S. 507, 514 (2008).

Americans” and “to accelerate deployment of such capability by removing barriers to infrastructure investment.”²³³ But the proposed rules would have exactly the opposite effect. As discussed, they would both increase the costs of broadband service while diminishing the supplemental, non-subscription-based revenues that ISPs could earn through targeted first- and third-party advertising. In both respects, the proposed rules would exert upward pressure on retail broadband prices, depress broadband adoption, and erect rather than remove “barriers to infrastructure investment.” *See* Section I.B, *supra*. And they would thus stifle, rather than “align with,” the “virtuous cycle” of innovation that the Commission has interpreted Section 706 to promote.²³⁴

The proposed rules would also contradict the purposes of Section 706 in a second respect. While privacy is important to Internet users, regulatory simplicity is important too. The Commission would needlessly confuse consumers and thus deter broadband acceptance if, because of the proposed rules, consumers must navigate confusingly disparate privacy rules applicable to different players in the Internet ecosystem. And the Commission would compound that confusion if, as it proposes, it adopts marketing restrictions that have little to do with keeping users’ information private and instead merely restrict how ISPs may *use* that information without sharing it. *See* Section I, *supra*.

Finally, the Commission would unsettle the entire Internet ecosystem if it invoked Section 706 as a basis for adopting the proposed rules because any authority the Commission derives from that provision is not restricted to common carriers. As an initial matter, there is no evidence, and the NPRM cites none, that privacy concerns deter consumers from using

²³³ 47 U.S.C. § 1302(a) & (b).

²³⁴ *Cf. NPRM* ¶ 309.

broadband services, and thus Section 706 could not possibly support any exercise of privacy authority.²³⁵ But even if privacy concerns *did* chill broadband adoption, they would do so not only—or even primarily—because of any ISP data uses; they would more likely do so because of the much more free-wheeling collection, use, and sometimes outright sale of consumer data by many others in the ecosystem, from Google and Amazon to Acxiom. *See* Technical Background, *supra*; Section I, *supra*. The Commission could not reasonably invoke Section 706 as a basis for regulating ISPs without regulating those non-ISP providers as well.

Sections 303(b), 303(r), and 316. In passing, the NPRM suggests that several provisions in Title III of the Communications Act—47 U.S.C. §§ 303(b), 303(r), and 316—“would appear to support” the proposed rules as applied to “licensed entities providing mobile BIAS.”²³⁶ But those provisions are irrelevant because they authorize the Commission only to regulate how licensees use their assigned radio spectrum, not how they design their privacy policies.²³⁷ For the same reason, there is no merit to the Commission’s apparent reliance on *CellCo Partnership*

²³⁵ *See* Lenard & Wallsten at 19-23. Moreover, Section 706 and the rest of federal telecommunications law must be interpreted in light of Congress’s express desire “to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation.” 47 U.S.C. § 230(b)(2).

²³⁶ *See* NPRM ¶ 310 (citing Sections 303(b), 303(r), and 316). Section 303(b) authorizes the FCC to “[p]rescribe the nature of the service to be rendered by each class” of wireless licensee. Section 303(r) authorizes the FCC to “[m]ake such rules and regulations and prescribe such restrictions and conditions, not inconsistent with law, as may be necessary to carry out the provisions of this chapter.” Section 316 authorizes the FCC to modify wireless licenses in order to “promote the public interest, convenience, and necessity.”

²³⁷ Specifically, Section 303(b) authorizes the Commission to “[p]rescribe the nature of the service to be rendered by each class of licensed stations and each station within any class,” and Section 316 authorizes it thereafter to “modif[y]” a “station license or construction permit.” And Section 303(r) generically authorizes the Commission to “[m]ake such rules and regulations and prescribe such restrictions and conditions ... as may be necessary to carry out the provisions” of Title III. That “necessary and proper” clause does not itself enlarge the scope of the Commission’s substantive authority. *See Motion Picture Ass’n of Am., Inc. v. FCC*, 309 F.3d 796, 806 (D.C. Cir. 2002) (“The FCC must act pursuant to *delegated authority* before any ‘public interest’ inquiry is made under § 303(r).”) (emphasis in original).

v. FCC,²³⁸ in which the D.C. Circuit upheld the Commission’s data-roaming rules. The court found that the Commission had permissibly “moor[ed] its action to a distinct grant of authority” in Section 303(b) only because the challenged regulations “lay[] down [rules] about ‘the nature of service to be rendered’” by mobile licensees.²³⁹ Here, in contrast, the proposed rules do *not* address “the nature of service to be rendered” over licensed spectrum.

Sections 338(i) and 631. Without explanation, the NPRM obliquely suggests that Sections 338(i) and 631 of the Communications Act²⁴⁰ might independently support the proposed rules. They do not. Section 631 provides certain privacy protections to cable subscribers and imposes corresponding obligations on cable MVPDs, while Section 338(i) provides similar privacy protections to satellite subscribers and imposes corresponding obligations on satellite MVPDs. Neither provision speaks to the Commission’s authority to impose privacy rules for ISPs qua ISPs.

D. The Commission Lacks Authority to Extend Its Rules to Cable Operators and Satellite Providers

The NPRM separately asks (e.g., at ¶ 108) whether it can and should extend the rules proposed for ISPs to cable and satellite MVPDs as well. It cannot and should not. The Commission would lack statutory authority to apply the proposed marketing restrictions to non-Title II cable operators and satellite providers even if it could apply them to ISPs. An entirely different statutory regime, set forth under the Cable and Satellite Acts, governs the collection and disclosure of cable and satellite television subscribers’ personally identifiable information. Those Acts define the four corners of the Commission’s authority over these non-Title II

²³⁸ 700 F.3d 534 (D.C. Cir. 2012); *see NPRM* ¶ 310 n. 488.

²³⁹ 700 F.3d at 542.

²⁴⁰ 47 U.S.C. §§ 338(i), 551.

providers, and neither of those statutes authorizes the proposed requirements to the extent they would impose greater burdens.²⁴¹ In any event, extension of the proposed rules to cable and satellite providers would violate the APA and the First Amendment (1) for the same reasons that application of those rules to ISPs would violate the APA and First Amendment and (2) for the additional reason that there is no record basis in this proceeding for applying any new rules to non-Title II MVPD services.

E. The Proposed Ban on Arbitration Clauses Is Unlawful

As the Supreme Court has explained, the Federal Arbitration Act (“FAA”) “was designed to promote arbitration” and “embod[ies] a national policy favoring arbitration.”²⁴² Congress enacted the FAA precisely because it wished to encourage contractual parties “to realize the benefits of private dispute resolution: lower costs, greater efficiency and speed, and the ability to choose expert adjudicators to resolve specialized disputes.”²⁴³

In the teeth of that national policy, the NPRM proposes (at ¶ 274) to “prohibit BIAS providers from compelling arbitration in their contracts with customers.” That prohibition would flatly violate the FAA.²⁴⁴ Section 2 of the FAA provides that arbitration clauses are “valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract.”²⁴⁵ As the Supreme Court has explained, Section 2 embodies a

²⁴¹ See generally 47 U.S.C. § 551(c)(1) (requiring cable operators to “take such actions as are necessary to prevent unauthorized access” to “personally identifiable information”); 47 U.S.C. § 338(i)(4)(A) (similar provision for satellite carriers).

²⁴² *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 345-46 (2011) (brackets omitted).

²⁴³ *Id.* at 348 (quoting *Stolt-Nielsen S.A. v. AnimalFeeds Int’l Corp.*, 559 U.S. 662, 685 (2010)).

²⁴⁴ 9 U.S.C. § 1 *et seq.*; see *id.* § 2 (FAA governs arbitration clauses in any “contract evidencing a transaction involving commerce”).

²⁴⁵ 9 U.S.C. § 2.

strong congressional policy in favor of private arbitration,²⁴⁶ and reflects the “fundamental principle that arbitration is a matter of contract.”²⁴⁷ Accordingly, “courts must place arbitration agreements on an equal footing with other contracts, and enforce them according to their terms.”²⁴⁸ Of particular relevance here, the FAA compels enforcement of arbitration clauses in disputes alleging violations of federal statutes, absent a clear congressional statement to the contrary in some other statutory scheme.²⁴⁹ The Communications Act contains no such statement and delegates no authority to the Commission to ignore the pro-arbitration policy of the FAA by categorically prohibiting arbitration clauses in contracts for broadband services.

F. The Proposed Rules Raise Substantial Issues Under the Paperwork Reduction Act

The NPRM acknowledges (at ¶ 315) that it “contains proposed new information collection requirements” that are subject to the requirements of the Paperwork Reduction Act.²⁵⁰ AT&T will provide a full response to the Commission (and the Office of Management and Budget) once the Commission has issued final rules and sought public comment in the Federal Register.²⁵¹ AT&T merely notes for now that the NPRM proposes a host of new information-collection obligations that would impose substantial burdens on ISPs of every type and size and

²⁴⁶ *Moses H. Cone Memorial Hosp. v. Mercury Constr. Corp.*, 460 U.S. 1, 24 (1983) (FAA declares a “liberal federal policy favoring arbitration agreements”).

²⁴⁷ *Concepcion*, 563 U.S. at 339 (2011) (internal quotation omitted).

²⁴⁸ *Id.* (citation omitted); *see also DIRECTV, Inc. v. Imburgia*, 136 S. Ct. 463, 468 (2015).

²⁴⁹ *E.g., American Express Co. v. Italian Colors Restaurant*, 133 S. Ct. 2304, 2309 (2013) (pursuant to the FAA, “courts must ‘rigorously enforce’ arbitration agreements according to their terms,” and this “holds true for claims that allege a violation of a federal statute, unless the FAA’s mandate has been ‘overridden by a contrary congressional command’”) (quoting *Shearson/American Express Inc. v. McMahon*, 482 U.S. 220, 226 (1987)).

²⁵⁰ 44 U.S.C. §§ 3501 *et seq.*

²⁵¹ *See* 44 U.S.C. § 3506(c)(2)(A) (requiring each agency to “provide 60-day notice in the Federal Register, and otherwise consult with members of the public . . . concerning each proposed collection of information, to solicit comment” before the agency submits the proposed collection to OMB).

that the NPRM falls far short of justifying the necessity for and practical utility of the proposed collections.²⁵²

G. The Commission Should Make Clear That Any Rules It Adopts Have No Effect on the Ability of ISPs to Respond to Legitimate Requests By Law Enforcement or National Security Authorities

The Commission should ensure that, whatever else it does in this proceeding, it does not interfere with procedures governing the government’s ability to access information from telecommunications carriers, including through the use of validly authorized wiretaps. Congress has specifically limited the scope of the Commission’s authority under Section 705 of the Communications Act, and it intended for the Wiretap Act, 18 U.S.C. §§ 2510 *et seq.*, to establish the exclusive procedures by which federal and state law enforcement may require recipient entities to intercept and disclose communications contents.²⁵³ Similarly, federal law specifically authorizes carriers to accommodate authorized requests for information from the United States government, “notwithstanding any other law,” and the Commission should respect that congressional decision.²⁵⁴

²⁵² *See id.* § 3508 (OMB shall not approve any proposed information collection unless it determines that the collection is “necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility”).

²⁵³ Congress amended Section 705 to add the phrase “except as authorized by chapter 119, Title 18” at the same time that it adopted the Wiretap Act, 18 U.S.C. §§ 2510 *et seq.* Contemporaneous with the Wiretap Act’s passage, Congress explained that “[t]he new provision [18 U.S.C. §§ 2510-2520] is intended as a substitute [for Section 705]. The regulation of the interception of wire or oral communications in the future is to be governed by proposed new chapter 119 of title 18, United States Code.” S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2196. *See also* 18 U.S.C. § 2516(2) (establishing procedures for State law enforcement to seek wiretap orders “in conformity with section 2518 of this chapter and ... applicable State statute[s].”)

²⁵⁴ 18 U.S.C. § 2511(2)(a)(ii) (authorizing carriers to “provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance.”); *see also* Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801 *et seq.*, as amended by the FISA Amendments Act of 2008, 50 U.S.C. §§ 1881a *et seq.* Disclosure of such requests, or information provided in response to such requests, including to the customer, may be specifically prohibited by law. *See, e.g.*, 50 U.S.C. § 1805(c)(2), 50 U.S.C. §1842(d)(2)(B), 50 U.S.C. § 1861(d), 18

Finally, the Commission should avoid intruding into areas where Congress has established clear and distinct frameworks authorizing private information disclosures (including “customer PI”) to address recognized policy goals. One prominent and recently-enacted example is the Cybersecurity Act of 2015,²⁵⁵ through which Congress sought to “encourage public and private sector entities to share cyber threat information *without legal barriers and the threat of unfounded litigation.*”²⁵⁶ Under Congress’s clear statutory choice, the Commission has no role to play in overseeing the information-sharing initiatives authorized under this or other statutory schemes.²⁵⁷

U.S.C. § 2511(2)(a)(ii), 18 U.S.C. § 2709(c), 15 U.S.C. § 1681u(d)(1), 15 U.S.C. § 1681v(c)(1), 12 U.S.C. § 3414(a)(3)(A), 50 U.S.C. 436(b)(1), 18 U.S.C. § 1802(a)(4), 50 U.S.C. § 1881a(h)(1). Of course, “before [AT&T] responds to any legal demand, we determine that we have received the correct type of demand based on the applicable law and the type of information being sought.” AT&T, *Transparency Report* at 6 (2016), http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_Transparency%20Report_Jan%202016.pdf.

²⁵⁵ See Cybersecurity Act of 2015, Pub. L. No. 114-113, Division N, §§ 101 *et seq.* (“CISA”).

²⁵⁶ See Joint Explanatory Statement to Accompany the Cybersecurity Act of 2015 (emphasis added).

²⁵⁷ Cf. *NPRM* ¶ 117. Congress has established clear statutory definitions for “cybersecurity threat” and has not invited the FCC to opine on this matter. See CISA § 102(5). Instead, these issues are properly administered by the Department of Justice and national security authorities. See generally Dep’t of Justice, *Sharing Cyberthreat Information Under 18 USC § 2702(a)(3)* (May 9, 2014), <http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/03/26/guidance-for-ecpa-issue-5-9-2014.pdf>.

CONCLUSION

The Commission should reject the NPRM's proposals to the extent, and for the reasons, discussed above.

Respectfully submitted,

James J.R. Talbot
Gary L. Phillips
David L. Lawson
AT&T SERVICES INC.
1120 20th Street, N.W.
Washington, D.C. 20036
(202) 457-3048

/s/ Jonathan E. Nuechterlein

Jonathan E. Nuechterlein
Alan Charles Raul
C. Frederick Beckner III
Clayton G. Northouse
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
(202) 736-8000

May 27, 2016