

**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 THE INTERNET ASSOCIATION

Mark W. Brennan
Partner
Hogan Lovells US LLP
555 13th Street, NW
Washington, DC 20004
(202) 637-6409

Counsel for The Internet Association

May 27, 2016

Abigail Slater
General Counsel
The Internet Association
1333 H Street NW
West Tower, Floor 12
Washington, DC 20005
(202) 770-0023

TABLE OF CONTENTS

	<u>Page</u>
I. Introduction and Summary.....	1
II. About the Internet Association.....	2
III. Congress Expressly Limited the Application of Section 222 to Title II Telecommunications Services.....	3
IV. The FTC’s Comprehensive, Time-Tested Data Privacy and Security Enforcement Framework Already Protects Consumers of Internet Edge Services and Other Non-Title II Offerings.....	4
A. The FTC is widely recognized as a thought leader on data privacy and security issues.....	4
B. The FTC’s existing enforcement standards establish meaningful consumer data privacy and security protections for edge services and non-Title II offerings. ..	6
C. As the FCC has recognized, the FTC has zealously enforced Section 5 of the FTC Act when companies fail to meet data privacy and security expectations. 7	
D. Existing state laws also provide additional consumer protections.....	8
V. The FCC Should Consider Providing Additional Flexibility and Support for Small Businesses.....	10
VI. Conclusion.....	10

**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 THE INTERNET ASSOCIATION

I. Introduction and Summary.

The Internet Association, through counsel, respectfully submits these comments in response to the Federal Communications Commission’s (“Commission” or “FCC”) April 1, 2016 Notice of Proposed Rulemaking (“*NPRM*”) in the above-captioned proceeding.¹ In the *NPRM*, the Commission seeks comment on, *inter alia*, a series of proposals to apply Section 222 of the Communications Act (the “Act”) to broadband Internet access service (“BIAS”), which it reclassified in 2015 as a “telecommunications service” subject to Title II of the Act.²

As discussed below, the *NPRM* properly excludes “edge services” from the proposed Section 222 requirements. To do otherwise would run contrary to the plain language of the Communications Act. Moreover, new requirements on edge services are unnecessary, including for example because of the Federal Trade Commission’s (“FTC’s”) robust oversight of non-Title II services on privacy, security, and other consumer protection issues, along with additional oversight by state regulators.

¹ *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, FCC 16-39 (rel. Apr. 1, 2016) (“*NPRM*”).

² *Id.* ¶¶ 2, 13; *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5820-24 ¶¶ 462-67 (“*2015 Open Internet Order*”).

The Internet Association supports the Commission’s consumer privacy goals of promoting transparency, choice, and security. Our members provide a host of consumer-facing, Internet-based “edge services” – for example, search, video and audio streaming and downloading, and social networking, to name a few. As the Commission recognized in the *NPRM*, these services are not BIAS or telecommunications services and do not fall within the ambit of Section 222, which Congress has expressly limited to the providers of Title II telecommunications services. Instead, edge services, as well as other non-Title II offerings, are subject to robust federal and state data privacy and security laws and regulations that are actively enforced by the FTC and state attorneys general. Finally, the Commission should also examine the impact its proposals could have on small businesses and consider providing additional flexibility to such entities.

II. About the Internet Association.

The Internet Association represents the interests of America’s leading Internet companies and their global community of users.³ It is dedicated to advancing public policy solutions that strengthen and protect Internet freedom, foster innovation and economic growth, and empower users. The Internet Association is also committed to protecting users’ online privacy by providing cutting-edge tools that empower users to make choices about how they view content online.

³ The Internet Association’s members include Airbnb, Amazon, Coinbase, Doordash, Dropbox, eBay, Etsy, Expedia, Facebook, FanDuel, Google, Groupon, Handy, IAC, Intuit, LinkedIn, Lyft, Monster, Netflix, Pandora, PayPal, Pinterest, Practice Fusion, Rackspace, reddit, Salesforce.com, Snapchat, Spotify, SurveyMonkey, Ten-X, TransferWise, TripAdvisor, Turo, Twitter, Uber Technologies Inc., Yahoo!, Yelp, Zenefits, and Zynga.

III. Congress Expressly Limited the Application of Section 222 to Title II Telecommunications Services.

In the *NPRM*, the Commission proposes to apply its existing statutory authority “solely to the existing class of services that Congress included within the scope of Title II, namely the delivery of telecommunications services.”⁴ Recognizing this important distinction, the Commission’s proposals in the *NPRM* properly exclude edge services from any new requirements. Consistent with the limits imposed by Congress, the Commission has repeatedly declined to extend new Title II obligations to edge services and should do so again in this proceeding.

As the Commission recognized, Section 222 is a “sector-specific statute that includes detailed requirements that Congress requires be applied to the provision of telecommunications services, *but not* the provision of other services by broadband providers nor to information providers at the edge of the network.”⁵ In its *2010 Open Internet Order*, the Commission appropriately chose not to extend net neutrality requirements to edge services, recognizing that in contrast to “edge provider activities, such as the provision of content or applications over the Internet,” the Communications Act “particularly directs [the Commission] to prevent harms related to the utilization of networks and spectrum to provide communication by wire and radio.”⁶

Consistent with its jurisdiction under the Communications Act, the Commission has appropriately continued to refrain from imposing new obligations on edge services. In the *2015*

⁴ *NPRM* ¶ 13; *see also* 47 U.S.C. § 153(51) (stating that Title II’s common-carrier requirements apply to telecommunications carriers “only to the extent that [they are] engaged in providing telecommunications services”).

⁵ *NPRM* ¶ 13 (emphasis added).

⁶ *Preserving the Open Internet, Broadband Industry Practices*, Report and Order, 25 FCC Rcd 17905, 17934 ¶ 50 (rel. Dec. 23, 2010) (“*2010 Open Internet Order*”).

Open Internet Order in which the Commission reclassified BIAS under Title II and prompted this proceeding, the Commission again rejected calls to impose regulations on edge services. Recently, in its Order denying a petition filed by Consumer Watchdog requesting that the Commission require edge providers to honor ‘Do Not Track’ requests, the Commission stressed that it has been “unequivocal in declaring that it has no intent to regulate edge providers.”⁷

There is no reason to switch course. Moreover, as discussed below, adopting additional data privacy and security requirements on edge services is unnecessary and would upend the current regulatory framework for such services without providing meaningful additional benefits for consumers.

IV. The FTC’s Comprehensive, Time-Tested Data Privacy and Security Enforcement Framework Already Protects Consumers of Internet Edge Services and Other Non-Title II Offerings.

The FTC’s existing data privacy and security enforcement framework provides strong consumer protections, and there is no need for the FCC to impose regulations that duplicate, displace, or “supplement” that framework. The FTC is widely recognized as a leading voice for data privacy and security matters, and its numerous enforcement actions and guidance documents – coupled with similar enforcement frameworks at the state level – have established well-settled, comprehensive, and effective data privacy and security expectations.

A. The FTC is widely recognized as a thought leader on data privacy and security issues.

As the FCC recognized in the *NPRM*, the FTC is “critically important in this sphere.”⁸ For example, in both domestic and international legal and policy circles, parties turn to the FTC for privacy and security leadership. The FTC has been described as the “nation’s privacy

⁷ *Consumer Watchdog Petition for Rulemaking to Require Edge Providers to Honor ‘Do Not Track’ Requests*, Order, 30 FCC Rcd 12424, 12424 ¶ 1 (rel. Nov. 6, 2015).

⁸ *NPRM* ¶ 8.

arbiter”⁹ and the “chief regulatory agency charged with protecting privacy and data security.”¹⁰ This position as a national thought leader and strong enforcement authority has helped define privacy standards for consumers and commercial entities alike. Privacy scholars, for instance, have noted that “FTC privacy jurisprudence is the broadest and most influential regulating force on information privacy in the United States....”¹¹

In drafting its proposed data privacy and security legislation, the White House recognized the FTC’s privacy leadership and chose to vest authority with the FTC to enforce the requirements. It also expressed its support for “simplifying and clarifying the legal landscape and making the FTC responsible for enforcing the Consumer Privacy Bill of Rights against communications providers.”¹²

The FTC’s leadership role in the U.S. is also recognized in privacy forums around the world. For example, the FTC helped negotiate the U.S.-EU Safe Harbor Framework and its successor, the Privacy Shield, which seeks to provide a mechanism to transfer data on EU persons to the U.S.¹³ The FTC also led federal efforts to create the Asia-Pacific Economic

⁹ Katy Bachman, *FTC Chair Edith Ramirez Fights for Data Security and Privacy Rights*, ADWEEK (May 27, 2014), <http://www.adweek.com/news/television/ftc-chair-edith-ramirez-fights-data-security-and-privacy-rights-157930>.

¹⁰ Press Release, Georgetown University Law Center, Georgetown Law Launches New Center on Privacy and Technology, (Jul. 21, 2014), <http://www.law.georgetown.edu/news/press-releases/georgetown-law-launches-center-on-privacy-and-technology.cfm>.

¹¹ See Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014).

¹² The White House, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 39 (Feb. 2012), <https://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

¹³ U.S. DEP’T OF COMMERCE, EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES (2016), https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf.

Cooperation Cross Border Privacy Enforcement arrangement, among other international efforts, on behalf of the U.S.¹⁴

B. The FTC’s existing enforcement standards establish meaningful consumer data privacy and security protections for edge services and non-Title II offerings.

The FTC has authority under Section 5 of the FTC Act to take action against businesses that engage in “unfair” or “deceptive” acts or practices,¹⁵ and it has used this authority to shape the U.S. data privacy and security landscape for consumers and industry. As part of these efforts, the FTC has sought to address a comprehensive range of privacy and security issues. To date, the FTC has brought almost 60 data security cases, more than 50 general privacy actions, and almost 30 cases for violations of the Gramm-Leach-Bliley Act.¹⁶ As examples, the FTC has sued businesses that allegedly spammed consumers, installed spyware on computers, failed to secure consumers’ personal information, deceptively tracked consumers online, violated children’s privacy, unlawfully collected information on consumers’ mobile devices, and failed to secure Internet-connected devices used to store personal information.¹⁷

“Deception” and “unfairness” are the legal standards that the FTC applies for enforcement actions under Section 5, but the principles underlying the FTC’s data privacy and security enforcement are rooted in a set of commonly utilized privacy standards: the Fair

¹⁴ ASIA-PACIFIC ECONOMIC COOPERATION, APEC COOPERATION ARRANGEMENT FOR CROSS-BORDER PRIVACY ENFORCEMENT (“CPEA”) (2009), <http://www.apec.org/~media/Files/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf>.

¹⁵ 15 U.S.C. § 45(a)(2).

¹⁶ Letter from FTC Chairwoman Edith Ramirez to Věra Jourová, Commissioner for Justice, Consumers, and Gender Equality at the European Commission Attachment A (Feb. 23, 2016) (“*Věra Jourová Letter*”). In some instances, the FTC’s privacy and data security cases involve alleged violations of multiple statutes.

¹⁷ *Id.*

Information Security Practice Principles (“FIPPs”)¹⁸—the same principles on which the FCC bases some of its proposals in its *NPRM*.¹⁹ With these consumer protections already in place for edge services and other non-Title II offerings, there is simply no need for the FCC to reinvent the privacy and security wheel for such services.

C. As the FCC has recognized, the FTC has zealously enforced Section 5 of the FTC Act when companies fail to meet data privacy and security expectations.

As the FCC notes in the *NPRM*, “[t]aken together the FTC’s online privacy cases focus on the importance of transparency; honoring consumers’ expectations about the use of their personal information and the choices they have made about sharing that information; and the obligation of companies that collect personal information to adopt reasonable data security practices.”²⁰ Collectively, the FTC’s enforcement actions have shown that the FTC is an active, zealous privacy enforcer willing to bring actions against non-exempt entities whenever it believes appropriate standards have not been met. This continued leadership on privacy and security underscores why there is no need for additional data privacy or security regulation by the FCC over edge services or other non-Title II offerings.

The FTC also has substantial administrative and judicial enforcement powers to protect consumers. The FTC’s administrative enforcement authority allows the agency to “prosecute any inquiry necessary to its duties in any part of the United States,” and to “gather and compile

¹⁸ ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 14-15 (2013), <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf> (Part Two – Basic Principles of National Application); *see also* Executive Office of the President, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 17-18 (2014), http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (describing “global consensus around the FIPPs”).

¹⁹ *NPRM* ¶ 5.

²⁰ *Id.* ¶ 8.

information concerning, and to investigate from time to time the organization . . . engaged in or whose business affects commerce.”²¹

Administrative enforcement actions generally result in consent orders to undergo independent, third-party audits of a company’s data privacy or security programs every year or every other year for a period of 20 years,²² a process that is viewed as “exhaustive and demanding.”²³ The audits generally involve specific reviews of agreed-upon safeguards, explanations of how the safeguards are appropriate, and explanations of how the safeguards are implemented.²⁴ In addition, FTC consent orders often prescribe certain steps that the subject company must take in the future (*e.g.*, providing enhanced notice or obtaining specific and informed consent for data practices).²⁵ Violations of the FTC’s administrative orders can lead to civil penalties of up to \$16,000 per violation, or \$16,000 per day for a continuing violation, which, in the case of practices affecting many consumers, can amount to millions of dollars.²⁶

D. Existing state laws also provide additional consumer protections.

In addition to federal protections, nearly every state has enacted its own consumer protection statute that creates additional data privacy and security protections.²⁷ These statutes

²¹ 15 U.S.C. § 46(a); *see A Brief Overview of the Federal Trade Commission’s Investigative and Law Enforcement Authority*, FED. TRADE COMM’N (July 2008), <http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority>.

²² Solove & Hartzog, *supra* note 11, at 606.

²³ *Id.*

²⁴ *Id.*

²⁵ *Id.* at 635.

²⁶ *Věra Jourová Letter*.

²⁷ *See* Jonathan Sheldon & Carolyn L. Carter, *Unfair and Deceptive Acts and Practices* 967-89 (6th ed. 2004) (noting that all states, the District of Columbia, Puerto Rico, Guam and the Virgin Islands have one or more consumer protection statutes).

prohibit fraudulent, unfair, or deceptive practices,²⁸ and state attorneys general have been called “crucial agents of regulatory change” for their role in enforcing these laws to protect consumer privacy.”²⁹

Additionally, some states have passed a wide range of specific privacy laws that often serve as the basis for *de facto* national standards. For example, California and Delaware require providers of online services that collect personally identifiable information to make their privacy policies conspicuously available.³⁰ California and Delaware also prohibit providers of online services from using or disclosing a minor’s personal information for purposes of marketing or advertising certain products where the online services are directed to minors or the providers have knowledge that the services are used by minors.³¹ Because it would be unduly burdensome for most technology companies to design products and services for particular state markets, such companies often choose to adopt state-specific requirements as a national standard.³²

Businesses also are subject to a host of state data security laws that require parties to notify consumers in the event of the unauthorized disclosure of their personal information.³³

²⁸ See Michael M. Greenfield, *Consumer Law: A Guide for Those Who Represent Sellers, Lenders, and Consumers* 158-62 (1995).

²⁹ Danielle Keats Citron, *Privacy Enforcement Pioneers: The Role of State Attorneys General in the Development of Privacy Law*, Notre Dame Law Review, Forthcoming, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733297.

³⁰ CAL. BUS. & PROF. CODE § 22575(a); DEL. CODE ANN. tit. 6 § 1205C(a).

³¹ CAL. BUS. & PROF. CODE § 22580(c); DEL. CODE ANN. tit. 6 § 1204C.

³² Katy Bachman, *California Paves the Way for Privacy Taking the Reins on Behalf of the Nation*, ADWEEK (Oct. 21, 2013), <http://www.adweek.com/news/technology/california-paves-way-privacy-153260>.

³³ See Security Breach Notification Laws, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 4, 2016), <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

And some states require businesses to implement and maintain reasonable security programs designed to safeguard consumers' personal information.³⁴

V. The FCC Should Consider Providing Additional Flexibility and Support for Small Businesses.

Throughout the *NPRM*, the Commission seeks comment on the impact its proposals could have on small businesses.³⁵ As the FTC recognized in its 2012 Privacy Report, in certain situations the burden that additional requirements impose on small businesses can sometimes outweigh the risk of harm the requirements are attempting to prevent.³⁶ Consistent with the FTC's analysis, the Commission should explore the potential burdens that its new requirements could impose on small businesses, along with flexible compliance mechanisms, including for example its proposed recordkeeping and breach notification requirements.

VI. Conclusion.

For the forgoing reasons, the Internet Association urges the Commission to continue to refrain from imposing any new privacy- and security-related requirements on providers of edge services and other non-Title II offerings. The requirements set forth in Section 222 of the Communications Act are expressly limited to Title II telecommunications services and do not extend to edge services. Moreover, new requirements are unnecessary for the edge, including for example because providers of edge services and other non-Title II offerings are already subject

³⁴ See, e.g., ARK. CODE ANN. § 4-110-104(b); CAL. CIV. CODE § 1798.81.5; MD. CODE ANN., COM. LAW § 14-3503(a).

³⁵ See, e.g., *NPRM* ¶¶ 30, 35, 40, 59, 77, 80, 89, 92, 95, 101, 131, 151, 164.

³⁶ FEDERAL TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 15 (Mar. 2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

to the FTC's robust and comprehensive data privacy and security framework, as well as other federal and state laws.

Respectfully submitted,

/s/ Mark W. Brennan

Abigail Slater
General Counsel
The Internet Association
1333 H Street NW
West Tower, Floor 12
Washington, DC 20005
(202) 770-0023

Mark W. Brennan
Partner
Hogan Lovells US LLP
555 13th Street, NW
Washington, DC 20004
(202) 637-6409

Counsel for The Internet Association

May 27, 2016