

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

MEMORANDUM

June 10, 2016

To: Subcommittee on Communications and Technology Democratic Members and Staff

Fr: Committee on Energy and Commerce Democratic Staff

Re: Hearing on “FCC Overreach: Examining the Proposed Privacy Rules”

On Tuesday, June 14, 2016, at 10:15 a.m. in room 2123 of the Rayburn House Office Building, the Subcommittee on Communications and Technology will hold a hearing on “FCC Overreach: Examining the Proposed Privacy Rules.”

Earlier this year, the Federal Communications Commission (FCC) adopted a notice of proposed rulemaking that would apply the privacy requirements of the Communications Act to broadband internet access service providers (broadband providers).¹ In doing so, the FCC noted that broadband providers “are the most important and extensive conduits of consumer information and have access to very sensitive and very personal information that could threaten a person’s financial security, reveal embarrassing or even harmful details of medical history, or disclose to prying eyes the intimate details of interests, physical presence, or fears.”² Opponents of the Commission’s proposed rules have argued that the Federal Trade Commission (FTC) is better suited to enforce privacy protections. Currently, the FCC is still taking comments on its proposal with final reply comments due on June 27, 2016.

I. BACKGROUND

A recent survey conducted by the Pew Research Center found that 91 percent of adults agree or strongly agree that consumers have lost control of how personal information is collected

¹ *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking (Rel. Apr. 1, 2016) [hereinafter PRIVACY NPRM].

² *Id.* at ¶ 2.

and used by companies.³ But this is not a new trend or set of concerns: More than a decade ago, Consumer Reports found that 88 percent of consumers said that keeping personal information safe and secure online was very important.⁴

Similarly, in a study it conducted, the National Telecommunications and Information Administration (NTIA) found that “privacy and security concerns deterred many Americans from engaging in important economic and civic online activities.”⁵ NTIA’s survey observed that 84 percent of surveyed online households expressed at least one concern about online privacy or security, and 45 percent of those reported that these concerns stopped them from some online activities.⁶

II. THE FCC’S ROLE IN REGULATING PRIVACY

Before 2015, broadband privacy had been overseen by the FTC, which was limited to after-the-fact enforcement on a case-by-case basis. But in the early part of last year, the FCC reclassified broadband providers as common carriers when it issued its net neutrality rules.⁷ That reclassification had the additional effect of limiting the FTC’s authority to take action against broadband providers engaged in “unfair or deceptive acts or practices”—the standard used by the FTC to protect the privacy of consumers.⁸

The FCC stated its intention to craft privacy rules for broadband providers in early 2015, when it issued the most recent open internet order.⁹ The FCC formally issued a notice of proposed rulemaking earlier this year seeking to specify how broadband providers may share consumers’ data.¹⁰

Since the reclassification, some have raised concerns about the FCC’s place in protecting consumers’ privacy. Internet service providers argue that the FCC should do nothing more than *ex post* enforcement modeled on the FTC’s authority. They contend anything else will confuse

³ Lee Rainie, *The State of Privacy in America: What We Learned*, Pew Research Center (Jan. 20 1016) [hereinafter *The State of Privacy in America: What We Learned*].

⁴ See Princeton Survey Research Associates International, *Leap of Faith: Using the Internet Despite The Dangers Results of a National Survey of Internet Users for Consumer Reports WebWatch*, CONSUMER REPORTS (Oct. 26, 2005).

⁵ Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NTIA (May 13, 2016).

⁶ *Id.*

⁷ *Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601, 5743-44 at ¶ 331 (2015) [hereinafter *Protecting and Promoting the Open Internet Order*].

⁸ 15 U.S.C. § 45(a)(2).

⁹ See *Protecting and Promoting the Open Internet Order*, *supra* note 7 at ¶ 53-54.

¹⁰ See PRIVACY NPRM, *supra* note 1.

consumers because websites and social media companies will remain under the purview of the FTC, while broadband providers will be subject to the FCC's *ex ante* rules.

Americans may already be confused when it comes to privacy, however, as approximately half of adults are not sure what information is being collected or how it is being used currently or might be used in the future.¹¹ The Pew Research Center recently observed that 68 percent of internet users find current laws insufficient to protect people's privacy online, and 64 percent believe the government should do more.¹² For its part, the staff at the FTC has commended "the FCC's focus on transparency, consumer choice, and data security" in its proposal.¹³ But the FTC staff has also noted that having a bifurcated privacy regime "is not optimal."¹⁴

III. THE FCC'S BROADBAND PRIVACY PROPOSAL

Recognizing the absence of consumer privacy protections caused by reclassification, the FCC sought to use its authority under section 222 of the Communications Act to fill the privacy void.¹⁵ Section 222 has traditionally protected Customer Proprietary Network Information, or CPNI. This includes call details, usage, and rate plans that must be obtained from a customer for them to receive telecommunications service.¹⁶ The FCC has recognized, however, that section 222 does not only pertain to and protect customers' network information,¹⁷ but that it also protects customers' personal information, such as addresses or telephone numbers.¹⁸

The proposed rules released earlier this year focus on transparency and giving consumers greater choice in how broadband providers share consumers' private information.¹⁹ Additionally, the proposed rules would include provisions to better secure data and provide notifications to consumers and law enforcement when breaches occur.²⁰

¹¹ See The State of Privacy in America: What We Learned, *supra* note 3.

¹² See *id.*

¹³ See Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106 (May 27, 2016) [hereinafter FTC Comments].

¹⁴ See *id.* at 8.

¹⁵ See 47 U.S.C. § 222; see also PRIVACY NPRM *supra* note 1 at ¶ 2.

¹⁶ See 47 U.S.C. § 222(c).

¹⁷ See PRIVACY NPRM *supra* note 1 at ¶ 56.

¹⁸ See 47 U.S.C. §222(a).

¹⁹ See PRIVACY NPRM *supra* note 1 at ¶ 17-18.

²⁰ See *id.*

A. Definition of Personally Identifiable Information

As a starting point in its proposed rules, the FCC would define personal identifiable information (PII). PII is a core principle of most privacy regimes, and the FCC proposes to define PII in this context as “any information that is linked or linkable to an individual.”²¹ The FCC intends for this definition to incorporate the “modern understanding of data privacy,” and to track FTC and National Institutes of Standards and Technology (NIST) guidelines.²² The FCC also proposes to recognize that a consumer’s name, postal address, and telephone number are PII and are protected by section 222.²³

The staff of the FTC’s Bureau of Consumer Protection filed comments with the FCC regarding the privacy proposals.²⁴ The FTC staff generally agrees with the FCC’s proposed definition of PII,²⁵ but offers some recommendations for consideration. Specifically, FTC staff recommends that the PII definition only include “reasonably” linkable information”²⁶

B. Transparency

The FCC’s proposed rules would require that broadband providers give “clear and conspicuous” notice of their privacy practices to their customers.²⁷ The proposal would require that broadband providers give consumers notice of the type of information a broadband provider collects, how that provider shares the data, and what rights consumers have with respect to that data, among other things.²⁸

C. Choice

The FCC proposes that broadband providers present consumers with three different levels of choice depending on the type of information collected and with whom the providers share that information. These three levels of choice include:

- (1) implied consent,
- (2) opt-out consent, and

²¹ See PRIVACY NPRM, *supra* note 1 at ¶ 60.

²² *Id.* at ¶ 60.

²³ *Id.* at ¶¶ 63-64.

²⁴ See Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106 (May 27, 2016).

²⁵ *Id.* at 9.

²⁶ *Id.*

²⁷ See *id.* at ¶ 82.

²⁸ See PRIVACY NPRM, *supra* note 1 at ¶ 82.

(3) opt-in consent.²⁹

1. Implied Consent

For some uses of customer data, the FCC proposes that consumer consent be implied, meaning that no formal consumer authorization is needed.³⁰ For example, the FCC proposes that consent be implied when a broadband provider uses information to market additional broadband offerings to a consumer.³¹ Additionally the FCC proposes that affirmative consent not be necessary when a broadband provider is sharing information when reasonably necessary to respond to a cybersecurity threat or to inform a family of a loved ones location during an emergency.³²

2. Opt-Out Versus Opt-In

In other instances, the FCC proposes requiring that broadband providers give consumers notice of sharing and allow those consumers to opt-out of having their data shared.³³ The FCC proposes that this framework apply when a broadband provider shares information with an affiliate “communications-related service” provider to market its product.³⁴ For all other uses, however, the FCC proposes to require that broadband providers give notice and require that customers affirmatively opt-in for providers to share consumers’ data.³⁵

For the opt-in proposal, the FTC staff has called for even stronger protections, supporting an opt-in mechanism when a broadband provider shares content of consumer communications with a first party, affiliate, or third party.³⁶ More generally, the FTC staff also recommends the level of choice to be tied to the sensitivity of data, and not only with whom the data is shared and for what purpose.³⁷

In addition, some legal scholars argue that the FCC’s broadband privacy rules could violate the First Amendment.³⁸ These scholars argue the FCC’s transparency and choice

²⁹ PRIVACY NPRM, *supra* note 1 at ¶ 109-33.

³⁰ *See id.* at ¶ 112-13.

³¹ *See id.*

³² *See id.* at ¶ 116-17.

³³ *See id.* at ¶ 122.

³⁴ *See id.*

³⁵ *See id.* at ¶ 127.

³⁶ *See* FTC Staff Comments, *supra* at note at 20.

³⁷ *See id.* at 22-23.

³⁸ *See* Comments of CTIA, NCTA, and USTelecom, *Protecting the Privacy of Customers of Broadband and Other Telecommunications, Services*, WC Docket No. 16-106 (May 27, 2016).

framework amounts to an impermissible restriction on commercial speech.³⁹ The D.C. Circuit in a recent case, however, found that nearly identical requirements when applied to traditional telephone service did not violate the First Amendment.⁴⁰

Securing Consumers Information

In addition to the transparency and choice requirements, the FCC also proposes that broadband providers be liable for ensuring the security of consumers' data. Data security is undoubtedly important to Americans with only 56 percent actually trusting businesses with their personal information online.⁴¹ At a minimum, the FCC proposes to require providers to:

- (1) adopt risk management practices,
- (2) institute personnel training practices,
- (3) adopt customer authentication requirements,
- (4) identify a senior manager responsible for data security, and
- (5) assume accountability for the use and protection of customer PII when shared with third parties.⁴²

With the aim of encouraging providers to protect the confidentiality of customer's information, and to give consumers and law enforcement notice, the FCC also proposes requiring broadband providers notify consumers and law enforcement when data breaches occur.⁴³ The FTC staff, in its comments, generally support the FCC's approach to data security, but argues that the standard for security be lowered so that only *reasonable* security, confidentiality, and integrity of customer proprietary information be required.⁴⁴

IV. WITNESSES

The following witness have been invited to testify:

Doug Brake
Telecommunications Policy Analyst
Information Technology and Innovation Foundation

³⁹ *See id.* at 9.

⁴⁰ *See NCTA v. FCC*, 555 F3d 996 (D.C. Cir. 2009).

⁴¹ TRUSTe/National Cyber Security Alliance, *U.S. Consumer Privacy Index 2016* (Jan. 28, 2016).

⁴² *See id.* at ¶ 174.

⁴³ *See id.* at 233.

⁴⁴ *See* FTC Comments, *supra* note 11 at 27-28.

Jon Leibowitz

Co-Chair

21st Century Privacy Coalition

Paul Ohm

Professor, Center on Privacy and Technology

Georgetown University Law Center