GEORGETOWN LAW
Center on Privacy & Technology

Statement of Laura Moy, Deputy Director
Center on Privacy & Technology at Georgetown Law

Before the

U.S. House of Representatives

Committee on Energy and Commerce

Subcommittee on Communications and Technology

Hearing on

Protecting Customer Proprietary Network Information in the Internet Age

Wednesday, July 11, 2018

For more information, contact Laura Moy at laura.moy@georgetown.edu.

Introduction and Summary

Chairman Blackburn, Ranking Member Schakowsky, and Members of the Subcommittee:

Consumers feel that they have lost control of their private information, and consistently are asking for greater control. 91% of adults agree or strongly agree that consumers have lost control of how personal information is collected and used by companies, and 68% believe current laws are not good enough in protecting people's privacy online.

Today's hearing is framed around customer proprietary network information, or CPNI. Generally speaking, CPNI is information collected by telecommunications providers about subscribers' use of the service. Information like who we call, and who calls us; how often we call them; how long we talk to them; and where we're calling from.

It is appropriate for a hearing about privacy to be framed around CPNI because the law that protects CPNI is one of the strongest federal consumer privacy laws we have.[1] It requires that phone carriers get their customers' consent before using CPNI for purposes other than to provide the phone service. In other words, phone carriers simply deliver the service we pay for without always trying to make an extra buck off of the details of our private lives. That means that a phone carrier cannot use the fact that a customer has been calling banks and credit card companies to market him payday loans, or that a customer has been calling an elderly relative and doctors' offices more frequently to market her home health services. Nor can it sell that information to outsiders—not without getting the customer's permission.

The CPNI privacy law also allows an expert agency to craft specific rules implementing the statute—rules that can be modified and updated in accordance with changing technology and business practices. For example, FCC rules protecting CPNI require phone carriers to protect customers' call details with a customer-created PIN, to maintain records of all sales and marketing campaigns that use their customers' CPNI, and to notify customers of security breaches.

The CPNI privacy law also gives the FCC robust enforcement authority in the form of fines. Using this authority, just in the last few years the FCC:

---

[1] 47 U.S.C. § 222.

- Slapped Verizon with fines when the company misused its customers' private information for internal marketing;
- Fined smaller providers YourTel and TerraCom for storing customers' sensitive information on unprotected Internet servers that anyone could access; and
- Fined AT&T $25 million when call center employees who were working with people trafficking in stolen cell phones accessed customer records without authorization.

The CPNI privacy law should serve as a model for future privacy laws this Congress may consider, because of its substantive strength, the regulatory flexibility it offers through rulemaking, and its enforcement strength.

Instead, however, the benefits to consumer privacy presented by the CPNI privacy law have faced major setbacks. Last year Congress—including a number of members of this subcommittee—voted against the extension of these strong CPNI privacy rules to broadband providers. Like the phone, broadband is now an essential service. And like phone carriers, broadband providers enjoy privileged insight into their subscribers' private communications. This year, as it eliminated net neutrality rules, the FCC removed broadband providers altogether from the reach of the CPNI privacy law—which, as I said, might be the strongest consumer privacy law we have on the books.

That brings us to today, and here, as we consider what our path forward should be. Consumers clearly want *more* privacy protection, not *less*—this is why the recent elimination of existing privacy protections was so unpopular among the American public.[2] As Congress considers how to give Americans the privacy protections they deserve, it should keep a few things in mind:

- Rulemaking authority is needed to protect consumer privacy prospectively and foster regulatory flexibility.
- Consumer protections are only as good as their enforcement, so any new protections Congress creates on privacy or data security must

[2] *See* Matthew Yglesias, *Republicans' Rollback of Broadband Privacy Is Hideously Unpopular*, Vox (Apr. 4, 2017), https://www.vox.com/policy-and-politics/2017/4/4/15167544/broadband-privacy-poll.

be accompanied by strong enforcement, including civil penalty authority.

- Congress should avoid the temptation to address complex challenges with a one-size-fits-all approach.
- Congress should not eliminate existing protections for consumers' information.

I appreciate your commitment to this issue.

1. Online privacy is important

Consumers care about and have well-founded concerns about online privacy. In response to one 2015 survey, 80% of respondents were "concerned" or "very concerned" when asked about their online privacy.[3] For years, consumers have been expressing concern and even anger about the way their personal information is collected and used without their control, consent, or even knowledge.[4] Consumers feel powerless to regain control over their privacy—in the modern era, Internet access is necessary for employment, education, access to housing, and full participation in economic and civic life.

Consumer privacy concerns can chill both adoption and free and open use of the internet. For example, according to an FCC survey in 2010, 57% of Internet non-adopters reported feeling that online activities made it too easy for theft of personal information.[5] The FCC concluded in the *National*

---

[3] Freedman Consulting, *Poll Finds Strong Support for Expanding Online Privacy Protections and Internet Access* (Nov. 23, 2015), *available at* https://www.freedmanconsulting.com/documents/PrivacyandAccessResearchFindings_151123.pdf.

[4] Lee Rainie & Maeve Duggan, Pew Research Center, *Privacy and Information Sharing* 2 (Jan. 14, 2016), http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf ("In online focus groups and in open-ended responses to a nationally representative online survey, many people expressed concerns about the safety and security of their personal data in light of numerous high-profile data breaches. They also regularly expressed anger about the barrage of unsolicited emails, phone calls, customized ads or other contacts that inevitably arises when they elect to share some information about themselves.").

[5] This number was reported in contrast to 39% of adopters who felt the same way. John Horrigan, *Broadband Adoption and Use in America* 17 (FCC Nat'l Broadband Plan, Working Paper No. 1, 2010),

Broadband Plan that concerns about online privacy and security "may limit [consumers'] adoption or use of broadband."[6] More recently, NTIA reported that 45% of households limited their online activities because of privacy and security concerns.[7] And in 2016, focus groups examining adoption challenges in Portland, Oregon universally raised privacy concerns.[8]

It is particularly important to protect online privacy because the Internet is where we practice First Amendment speech in the modern era. The health of our democracy relies on the Internet functioning as a trustworthy platform for free and unfettered association and speech. But as privacy diminishes, so does speech. For example, studies have shown that people self-censor opinions they believe may be unpopular when informed that they are under surveillance.[9]

2. Protections for consumers' private information should be forward-looking and flexible

To foster the increased control over private information that consumers want, Congress should consider establishing protections that are forward-looking and flexible. Agencies that are to be tasked with protecting consumers' private information should be given rulemaking authority, just as the CPNI statute grants rulemaking authority to the FCC. After-the-fact enforcement can be helpful, but an enforcement-only regime does not always

---

https://transition.fcc.gov/DiversityFAC/032410/consumer-survey-horrigan.pdf.

[6] FCC, *Connecting America: The National Broadband Plan* 17 (2010), https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf.

[7] Rafi Goldberg, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities, NTIA (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[8] Angela Siefer, Signs On Letter Encouraging FCC Protect Privacy Of Broadband Consumers, NDIA (Jan. 26, 2016), http://www.digitalinclusionalliance.org/blog/2016/1/26/ndia-signs-on-letter-encouraging-fcc-protect-privacy-of-broadband-consumers.

[9] *See* Elizabeth Stoycheff, Mass Surveillance Chills Online Speech Even When People Have "Nothing to Hide," Slate (May 3, 2016), http://www.slate.com/blogs/future_tense/2016/05/03/mass_surveillance_chills_online_speech_even_when_people_have_nothing_to.html.

create clarity, and because it comes only after a problem has occurred, it does not necessarily protect consumers from the problem in the first place.

In particular, the FTC should be given rulemaking authority over data security, data brokers, and consumer privacy. The FTC brings the bulk of federal privacy enforcement actions, but it only has after-the-fact enforcement authority, with no ability to define rules of the road before consumer data is used in ways that consumers consider inappropriate. And with few exceptions, when it comes to privacy and data security the FTC can only take enforcement action against entities that use consumer information in ways that violate their own consumer-facing commitments. Indeed, commissioners of the agency have themselves asked Congress for rulemaking authority.[10]

Rulemaking authority helps to future-proof consumer protections, enabling agencies to adjust regulations as technology changes, as the FTC did just a few years ago with the COPPA Rule.[11] Consumers are constantly encountering new types of privacy and data security threats as the information landscape evolves. Where flexibility exists, policymakers use it to respond to changing threats. For example, states adjust data security and breach notification protections as changing circumstances require, such as by extending protection to additional categories of information, including medical information and biometric data.[12] We can't always forecast the next

---

[10] Maureen K. Ohlhausen, FTC Commissioner, Remarks Before the Congressional Bipartisan Privacy Caucus (Feb. 3, 2014), *available at* https://www.ftc.gov/system/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen/140203datasecurityohlhausen.pdf ("Legislation in both areas – data security and breach notification – should give the FTC the ability to seek civil penalties to help deter unlawful conduct, rulemaking authority under the Administrative Procedure Act, and jurisdiction over non-profits.");

[11] Federal Trade Commission, *FTC Strengthens Kids' Privacy, Gives Parents Greater Control over Their Information by Amending Children's Online Privacy Protection Rule* (Dec. 19, 2012), https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over.

[12] William Elser, *Recent Updates to State Data Breach Notification Laws in New Mexico, Tennessee, Virginia*, Lexology (May 1, 2017), https://www.lexology.com/library/detail.aspx?g=b02a15ac-a3c3-460d-bc5e-1d29778c4e59 ("New Mexico's new law defines 'personal identifiable information' consistently with most other states, and joins a growing number of states that have broadened the definition to include 'biometric data,' which is

big threat years in advance, but unfortunately, we know that there will be one.

The law should grant an expert agency or agencies the authority to develop prospective privacy and data security rules, in consultation with the public, so that data collectors and users can know in advance what standards apply to consumers' information.

3. Protections for consumers' private information should be strongly enforced

Congress also should ensure that whatever agency or agencies are to be in charge of enforcing privacy and data security standards have substantial civil penalty enforcement authority, just as the CPNI statute grants the FCC. Regulations are effective to deter violations only if entities fear the punishment that would surely follow.

Agencies recognize the importance of—and ask for—strong enforcement tools. Indeed, the FTC has repeatedly asked for the civil penalty authority it needs to enforce data security.[13] At present when the FTC takes action to enforce, it is generally unable to pursue penalties that would serve as an effective punishment for violators, and an effective deterrent for others.[14] To improve privacy and data security for consumers, the FTC—or

---

defined to include 'fingerprints, voice print, iris or retina patterns, facial characteristics or hand geometry.'").

[13] *See, e.g.*, Testimony of Jessica Rich, Federal Trade Commission, before the House Oversight and Government Reform Committee Subcommittees on Information Technology and Health, Benefits, and Administrative Rules regarding Opportunites and Challenges in Advancing Health Information Technology (Mar. 22, 2016) at 7, *available at* https://oversight.house.gov/wp-content/uploads/2016/03/2016-03-22-Rich-Testimony-FTC.pdf; Maureen Ohlhausen, Commissioner, Fed. Trade Comm'n, Remarks Before the Congressional Bipartisan Privacy Caucus (Feb. 3, 2014), transcript *available at* https://www.ftc.gov/system/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen/140203datasecurityohlhausen.pdf.

[14] There are exceptions to this rule. As the FTC explains, "If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain privacy statutes and rules, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Telemarketing Sales

another agency or agencies—must be given more powerful regulatory tools and stronger enforcement authority.

Agencies also need resources to do their jobs well. Unlike the FCC, the FTC has no Office of Engineering & Technology. An agency expected to enforce the privacy and security obligations of companies that do business in a digital world should be vested with the necessary expertise and resources to do that job well.

To provide an additional backstop for consumers the event that agencies lack the capacity or motivation to effectively enforce, Congress should also consider granting state attorneys general or even individual consumers themselves the right to bring civil actions against companies for violating privacy regulations. This type of authority exists, for example, under the Children's Online Privacy Protection Act.[15]

4. Protections for consumers' private information should take into account the context in which information is shared

There is no one-size-fits-all approach for privacy. Rather, privacy laws and regulations should be context-specific, carefully tailored based on the avoidability of the information sharing, the sensitivity of the information shared, and the expectations of consumers.

When information sharing is unavoidable or less avoidable by consumers, it is important that heightened privacy protections apply. This explains in part why there are a variety of laws that protect consumer information in specific contexts in which sharing is unavoidable—such as the information shared by students in an educational context,[16] by consumers in a financial context,[17] by customers in a telecommunications context,[18] and by patients in a medical context.[19]

Rule." FTC, *Privacy & Security Update 2016*, https://www.ftc.gov/reports/privacy-data-security-update-2016.

[15] For example, the Children's Online Privacy Protection Act enables state attorneys general to bring actions on behalf of residents of their states against operators of online sites or services that they believe have violated children's privacy regulations. 15 U.S.C. §6504.

[16] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.

[17] Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338, (1999).

[18] 47 U.S.C. § 222.

[19] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 (1996).

This is also consistent with the FTC's evaluation of potentially problematic data-related practices under its Section 5 authority to prohibit unfair practices. When considering whether a practice is unfair, the FTC asks not only whether the practice is harmful, but also whether the practice is one that consumers can avoid. In its policy statement on unfairness, the FTC explained,

> Normally we expect the marketplace to be self-correcting, and we rely on consumer choice—the ability of individual consumers to make their own private purchasing decisions without regulatory intervention—to govern the market. We anticipate that consumers will survey the available alternatives, choose those that are most desirable, and avoid those that are inadequate or unsatisfactory. However, it has long been recognized that certain types of sales techniques may prevent consumers from effectively making their own decisions, and that corrective action may then become necessary. Most of the Commission's unfairness matters are brought under these circumstances. They are brought, not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking.[20]

In recognition of the heightened privacy protections that should attach to information consumers cannot avoid sharing, Congress should consider strengthening the FTC's unfairness authority.

Whether or not information sharing is avoidable by a consumer is often tied to the question of whether or not a service or transaction is essential. When a service is essential—such as with phone service—information sharing may be considered unavoidable because the consumer cannot reasonably decline the service altogether. This, too, helps explain why heightened privacy protections apply in the educational,[21] financial,[22]

---

[20] FTC, *FTC Policy Statement on Unfairness* (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.
[21] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.
[22] Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338, (1999).

telecommunications,[23] and medical contexts—all of these contexts involve essential services.[24]

In determining what level of protection should be afforded to information shared in a particular context, policymakers should also examine how sensitive the shared information is. For example, the Children's Online Privacy Protection Act recognizes that information about children deserves heightened protection.[25] Other laws recognize the heightened sensitivity of health information[26] and financial information.[27] In the past, the question of sensitivity has often been the most important in considering how well the law should protect consumers' information. Data analysis techniques have advanced over time, however, and it is becoming clear that classically sensitive information can often be deduced from categories of information not traditionally thought of as sensitive. For example, as computer scientist Ed Felten explained in testimony before the Senate Judiciary Committee regarding telephone metadata, "Calling patterns can reveal when we are awake and asleep; our religion . . . our work habits and our social attitudes; the number of friends we have; and even our civil and political affiliations."[28] In 2016 the FTC found that television viewing history can be considered sensitive information,[29] and the Federal Communications Commission (FCC) found that web browsing history can be considered sensitive.[30] Indeed, patent

---

[23] 47 U.S.C. § 222.
[24] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 (1996).
[25] 15 U.S.C. §§ 6501–6506.
[26] *E.g.* Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 (1996).
[27] *E.g.* Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338, (1999).
[28] *Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing before the S. Comm. on the Judiciary,* 113th Cong. 8-10 (2013) (statement of Edward Felten, Professor of Computer Science and Public Affairs, Princeton University) *available at* http://www.judiciary.senate.gov/meetings/continued-oversight-of-the-foreign-intelligence-surveillance-act.
[29] Complaint at ¶ 32, *FTC v. Vizio*, Case No. 2:17-cv-00758, D.N.J. (filed Feb. 6, 2017), *available at* https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf.
[30] Federal Communications Commission, *Fact Sheet: The FCC Adopts Order to Give Broadband Consumers Increased Choice over Their Personal Information*, https://apps.fcc.gov/edocs_public/attachmatch/DOC-341938A1.pdf.

applications filed by Google indicate that it is possible to estimate user demographics and location information based on browsing histories.[31]

Protection for consumers' information should also be tailored based on consumers' expectations for how the information will be used.

5. Congress should not eliminate existing protections for consumers' information

Perhaps this should go without saying, but as Congress considers establishing new privacy and data security protections for consumers' private information, it should not eliminate existing protections. Americans are asking for *more* protections for their private information, not less. This explains why when this body voted last year to eliminate strong privacy regulations that had recently been passed by the FCC, consumers—on both sides of the aisle—were outraged.[32] Some lawmakers argued that repeal of the FCC's rules was needed to foster development of a consistent approach to privacy across the Internet.[33] But as FTC Commissioner Terrell McSweeny noted, "If consistency were truly the goal, then we would likely increase protections for privacy, rather than unraveling them. That is the policy conversation we ought to be having—instead we are fighting a rear-guard action defending basic protections."[34]

---

[31] *See* U.S. Patent Application No. 13/652,198, Publication No. 20130138506 (published May 30, 2013)(Google Inc., applicant)("demographics data may include a user's age, gender, race, ethnicity, employment status, education level, income, mobility, familial status (e.g., married, single and never married, single and divorced, etc.), household size, hobbies, interests, location, religion, political leanings, or any other characteristic describing a user or a user's beliefs or interests."); U.S. Patent Application No. 14/316,569, Publication No. 20140310268 (published Oct. 16, 2014)(Google Inc., applicant).

[32] *See* Matthew Yglesias, *Republicans' Rollback of Broadband Privacy Is Hideously Unpopular*, Vox (Apr. 4, 2017), https://www.vox.com/policy-and-politics/2017/4/4/15167544/broadband-privacy-poll.

[33] *See* Alex Byers, *House Votes to Revoke Broadband Privacy Rules*, Politico (Mar. 28, 2017), https://www.politico.com/story/2017/03/house-votes-to-revoke-broadband-privacy-rules-236607.

[34] Terrell McSweeny, Commissioner, Fed. Trade Comm'n, Remarks on *"The Future of Broadband Privacy and the Open Internet: Who Will Protect Consumers?"* (Apr. 17, 2014), at 4, https://www.ftc.gov/system/files/

Congress also should not eliminate existing and future consumer protections at the state level. State laws play an important role in filling gaps that exist in federal legislation, and state attorneys general play an important role in enforcing privacy and data security standards.[35] For example, in data security and breach notification, some state laws protect categories of information that are not protected by other states, and would not be protected by a number of proposals for federal data security and breach notification legislation.[36] State attorneys general play a critical role in policing data security and guiding breach notification to match the needs of their own residents, and are essential in conducting ongoing monitoring after a breach has occurred to help protect residents from any aftermath, especially where small data breaches are concerned. According to the Massachusetts State Attorney General's Office, Massachusetts alone saw 2,314 data breaches reported in 2013, 97% of which involved fewer than 10,000 affected individuals.[37] Each data breach affected, on average, 74 individuals.[38]

6. Conclusion

I am grateful for the Subcommittee's attention to these important issues, and for the opportunity to present this testimony.

---

documents/public_statements/1210663/mcsweeny_-_new_americas_open_technology_institute_4-17-17.pdf.

[35] *See generally* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747 (2016).

[36] *See* Testimony of Laura Moy before the House Energy & Commerce Committee Subcommittee on Commerce, Manufacturing, and Trade regarding the Data Security and Breach Notification Act of 2015 (Mar. 11, 2015) at 3–5, *available at* https://democrats-energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony-Moy-CMT-Data-Breach-Legislation-2015-03-18.pdf; *see also* Responses to Additional Questions for the Record of Laura Moy before the House Energy & Commerce Committee Subcommittee on Commerce, Manufacturing, and Trade, http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-Wstate-MoyL-20150318.pdf.

[37] Testimony of Sara Cable before the House Energy & Commerce Committee Subcommittee on Commerce, Manufacturing, and Trade regarding the Data Security and Breach Notification Act of 2015, *available at* http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-Wstate-CableS-20150318.pdf.

[38] *Id.*