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

and

Subcommittee on Digital Commerce and Consumer Protection

Hearing on

Algorithms: How Companies' Decisions About Data and Content Impact Consumers

Wednesday, November 29, 2017

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

Introduction and Summary

Chairman Blackburn, Chairman Latta, Ranking Member Doyle, Ranking Member Schakowsky, and Members of the Subcommittees:

Consumers share information about themselves with others every day. In some instances, consumers have no choice but to share highly private information, such as when sharing is necessary to access an essential service. In other instances, consumers do have a choice, and share private information voluntarily. Private entities collect this consumer information because it is valuable, either on its own (such as in the case of a data broker intending to resell the information), or to power algorithmic decision-making. Algorithmic decision-making may streamline some aspects of our lives, but sometimes has flaws that lead to negative or unfair consequences.

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.

To foster the increased control over private information that consumers want, Congress should consider establishing protections that are forward-looking, flexible, strongly enforced, and appropriate based on context. In particular, agencies that are to be tasked with protecting consumers' private information must be given more powerful regulatory tools and stronger enforcement authority. But as Congress considers establishing new privacy and data security protections for consumers' private information, it should not eliminate existing protections.

Because we are still in the months following the massive Equifax breach, I also offer these Subcommittees a few targeted recommendations to better protect information held by credit reporting agencies (CRAs) First, Congress should enhance the authority of federal agencies to oversee the data security practices of consumer reporting agencies, to promulgate rules governing the data security obligations of financial institutions, and to enforce those obligations with civil penalties. Congress should also consider giving consumers better tools for redress when their personal information is compromised in a future breach by streamlining the credit freeze process, establishing protective tools for victims of child identity theft and medical identity theft, and prohibiting mandatory arbitration clauses.

I thank you for inviting me to testify on these important topics, and for your attention to privacy and data security.

1. Consumers share highly private information about themselves with a variety of actors on- and offline, and have varying degrees of choice with respect to that sharing

Consumers share information about themselves with others every day. In some instances, consumers have no choice but to share highly private information, for example to access an essential service. In other instances, consumers do have a choice, and share private information voluntarily.

A. Consumers have no choice but to share highly private information with an Internet service provider

Virtually every single consumer shares information about everything they do online with an Internet service provider (ISP). Consumers share this information not because they want to, but because they must. In the words of major ISP Comcast, "Internet service has become essential for success."[1] Sharing information with an ISP is an unavoidable part of going online.

Making matters worse, many consumers cannot switch providers if they dislike the privacy practices of their ISP. In many areas, consumers have only one option when it comes to high-speed broadband. Even when there are two or three possible providers, switching costs—contract termination fees, installation fees, the time investment necessary to research and adopt an alternative—can make it very difficult for a subscriber of one provider to switch to another.

ISPs have tremendous visibility into nearly everything their clients do online, and can learn detailed information about consumers' private lives. An ISP can see what websites its subscribers visit and when they visit them, and can make inferences based on that information. For example, domain names can expose details about health (plannedparenthood.org), finances (acecashexpress.com, particularly if accessed before each payday), political views (joinnra.nra.org), and other sensitive attributes.[2]

---

[1] Comcast, Internet Essentials Flyer, http://www.gaithersburgmd.gov/~/media/city/documents/services/community/comcast_internet_essentials_flyer.pdf (last visited Apr. 6, 2017).

[2] The FCC's Role in Protecting Online Privacy (Jan. 21, 2016) at 5, *available at* https://www.newamerica.org/oti/policy-papers/the-fccs-role-in-protecting-online-privacy/.

In addition, even when consumers' online activities have been purged of personal identifiers, such as name or a subscriber identifier, browsing histories can still be linked back to specific individuals. As explained by anonymization experts Sharad Goel and Arvind Narayanan, who recently presented a paper on the challenges of anonymizing web histories, "'anonymous' web browsing records often contain an indelible mark of one's identity. We recruited nearly 400 users to send us their web browsing data stripped of any overt personal identifiers. In 70 percent of cases we could identify the individual from their web history alone."[3]

No other type of actor in the Internet ecosystem has access to as rich and reliable a stream of private information about individual users as ISPs. As noted privacy scholar Paul Ohm explained before the Senate Commerce Committee last year,

> No other entity on the Internet possesses the same ability to see. If you are a habitual user of the Google search engine, Google can watch you while you search, and it can follow you on the first step you take away from the search engine. After that, it loses sight of you, unless you happen to visit other websites or use apps or services that share information with Google. If you are a habitual Amazon shopper, Amazon can watch you browse and purchase products, but it loses sight of you as soon as you shop with a competitor. Habitual Facebook users are watched by the company when they visit Facebook or use websites, apps or services that share information with Facebook, but they are not visible to Facebook at any other times.[4]

The threat to consumer privacy posed by ISPs is not something that consumers can address on their own. As I explained in an op-ed earlier this

---

[3] Sharad Goel & Arvind Narayanan, *Why You Shouldn't Be Comforted by Internet Providers' Promises to Protect Your Privacy*, Future Tense (Apr. 4, 2017), http://www.slate.com/blogs/future_tense/2017/04/04/don_t_be_comforted_by_internet_providers_promises_to_protect_your_privacy.html (referring to Jessica Su, Ansh Shukla, Sharad Goel, & Arvind Narayanan, *Anonymizing Web Browsing Data with Social Networks*, *available at* https://5harad.com/papers/twivacy.pdf).

[4] Testimony of Paul Ohm Before the Senate Commerce Committee, July 12, 2016, at 3, http://paulohm.com/projects/testimony/PaulOhm20160712FCCPrivacyRulesSenate.pdf.

year, none of the potential privacy protecting tools that consumers could use to hide their online activities from their ISP are perfect.[5] Consumer-facing privacy options are weak, often difficult to locate, and even more difficult to understand. Tech-savvy consumers who can afford an additional monthly fee on top of what they already pay their ISP may consider signing up for a "virtual private network," or VPN service, but that can be technically difficult for some consumers, as well as slow down the Internet experience. Consumers also can install a browser extension that will take the consumer to the encrypted version of a website whenever one is available, but many websites do *not* have encryption available, and even when encryption is available, it does not hide all private information from the ISP.

The bottom line when it comes to ISPs is that consumers have no choice but to share their information in order to get online.

B. Consumers have no choice but to share highly private information with credit reporting agencies

As with Internet service providers, consumers have no choice but to share highly private information with CRAs like Equifax. The massive troves of valuable and potentially damaging information that CRAs maintain are provided by furnishers, not by consumers themselves.

This is part of why consumers are so outraged by the recent Equifax breach. The 165.5 million Americans whose private details were breached in the Equifax attack now face an increased risk of identity theft in perpetuity. Now that their names, Social Security numbers, and other difficult-to-change data closely tied to financial records have been breached, those details are out there forever—there is no putting the genie back in the bottle.

And there is no question that, entrusted with this private information through no affirmative choice by consumers, Equifax made serious mistakes. Equifax could and should have prevented a breach of this magnitude from occurring. Indeed, the scale of the breach alone—affecting some 45% of American consumers in an attack that took place over the course of months—indicates that Equifax's security program was riddled with problems. And it was. Equifax's unreasonable security failures include the failure to encrypt

---

[5] Laura Moy, *Think You Can Protect Your Privacy from Internet Providers Without FCC Rules? Good Luck.*, The Daily Dot (Mar. 28, 2017), https://www.dailydot.com/layer8/congress-kill-isp-privacy-protections/.

the large volume of data that ultimately was exfiltrated by attackers,[6] the months-long failure to patch the critical Apache Struts vulnerability that was exploited,[7] the apparent lack of appropriate management and redundancies to ensure the patch would be applied,[8] and the months-long failure to detect the breach even as attackers continued to access and steal sensitive consumer data.

Even though many consumers may have lost or diminished trust in Equifax—and perhaps other CRAs as well—following the Equifax breach, the decision to share private information with CRAs is out of consumers' hands.

C. Consumers often do have a choice whether or not to share private information

Although in some instances, such as where ISPs or CRAs are concerned, consumers have no choice but to share private information, consumers also are often asked or invited to share information about themselves in circumstances where such sharing would be completely voluntary. For example, consumers sometimes—but not always—are willing to participate in voluntary surveys in which they are asked to share information about their preferences or habits. Consumers also may share information with an online discussion forum so that they can participate in forum conversations, or with a shopping list application so that they can keep better track of groceries they need to purchase.

---

[6] *Oversight of the Equifax Data Breach: Answers for Consumers: Hearing Before the H. Comm. on Energy and Commerce Subcomm. on Digital Commerce and Consumer Protection*, 115th Cong. (Oct. 3, 2017) (statement of Richard F. Smith, Former Chairman and CEO, Equifax, Inc.), preliminary transcript at 81, *available at* http://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Transcript-20171003.pdf ("To be very specific this data was not encrypted at rest.")[hereinafter *Oct. 3 Hearing*]

[7] *See* Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sept. 14, 2017), https://www.wired.com/story/equifax-breach-no-excuse/.

[8] *Oct. 3 Hearing* (statement of Richard F. Smith, Former Chairman and CEO, Equifax, Inc.), preliminary transcript at 35, ("The human error was the individual who is responsible for communicating in the organization to apply the patch did not."); *see* Russell Brandom, *Former Equifax CEO Blames Breach on a Single Person Who Failed to Deploy Patch*, The Verge (Oct. 3, 2017), https://www.theverge.com/2017/10/3/16410806/equifax-ceo-blame-breach-patch-congress-testimony.

2. Information collected from and about consumers is used to power algorithmic decision-making that can be problematic

Information about consumers is not collected in a vacuum; private entities collect consumer information because it is valuable, either on its own (such as in the case of a data broker intending to resell the information), or to power automated decision-making. Indeed, many things that once were decided by humans are now often decided—or at least influenced—by predictive formulas designed by data scientists, and those formulas may be responsible for decisions that have important effects on consumers' lives. Algorithms may be used to determine which job applicants are invited to come in for an interview,[9] where police officers should patrol,[10] or how long a person convicted of a crime should spend in jail.[11] Algorithms also select much of what we read and see online. They may determine which products are presented to us in advertisements, which movies are recommended to us, which friends' photos we see, and which news articles we read.

Algorithmic decision-making may streamline some aspects of our lives, but algorithms can sometimes have flaws that lead to negative or unfair consequences. For example, hiring algorithms have been accused of unfairly discriminating against people with mental illness.[12] Sentencing algorithms—intended to make sentencing fairer by diminishing the role of potentially biased human judges—may actually discriminate against Black people.[13] Search algorithms may be more likely to surface advertisements for arrest

---

[9] Lauren Weber & Elizabeth Dwoskin, *Are Workplace Personality Tests Fair? Growing Use of Tests Sparks Scrutiny Amid Questions of Effectiveness and Workplace Discrimination*, W.S.J. (Sept. 29, 2014), https://www.wsj.com/articles/are-workplace-personality-tests-fair-1412044257.

[10] Laurel Eckhouse, Big Data May Be Reinforcing Racial Bias in the Criminal Justice System, Wash. Post (Feb. 10, 2017), https://www.washingtonpost.com/opinions/big-data-may-be-reinforcing-racial-bias-in-the-criminal-justice-system/2017/02/10/d63de518-ee3a-11e6-9973-c5efb7ccfb0d_story.html.

[11] Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner, *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[12] Weber & Dwoskin, *supra* note 9.

[13] Angwin, et al., *supra* note 11.

records—regardless of whether such records exist—when presented with characteristically Black names.[14]

The use of consumer data to power algorithmic decision-making deserves particularly close scrutiny when the decisions to be made will affect opportunities for education, healthcare, financial products, or employment. For example, policymakers may reasonably not be concerned with flawed algorithms that display ads for wine to the wrong crowd, but there is greater cause for concern when a study shows—as one has—that male job seekers are much more likely than equivalent female jobs seekers to be shown ads for high-paying executive ads.[15]

It may also be problematic when consumer data is used to power the targeted distribution of content that may distort consumers' perception of issues of importance, such as political issues. This is especially the case when consumers are not aware that algorithms are at work personalizing which content they will see and in what order.[16] Consider, for example, a hypothetical posed by digital analytics consultant Angela Grammatas:

> [I]magine that "Jane Internet" loves cats, and visits cats.com daily. One day, she's considering how to vote on a local proposition, and she does some research by visiting two political news sites at opposite ends of the spectrum. She reads a relevant article on each site, getting a balanced view of the issue. Let's imagine that the "Yes on Prop A" campaign has access to

---

[14] Latanya Sweeney, *Discrimination in Online Ad Delivery*, Communications of the Association of Computing Machinery (Jan. 2013).

[15] Tom Simonite, *Probing the Dark Side of Google's Ad-Targeting System*, MIT Technology Review (July 6, 2015), https://www.technologyreview.com/s/539021/probing-the-dark-side-of-googles-ad-targeting-system/.

[16] One study of 40 Facebook users found that a majority of participants—62.5%—did not know that content on Facebook was filtered. According to the study's authors, "In [the unaware users'] opinion, missing a public story was due to their own actions, rather than those of Facebook. Importantly, these participants felt that they missed friends' stories because they were scrolling too quickly or visiting Facebook too infrequently." Motahhare Eslami, Aimee Rickman, Kristen Vaccaro, Amirhossein Aleyasen, Andy Vuong, Karrie Karahalios, Kevin Hamilton, & Christian Sandvig, *"I Always Assumed that I Wasn't Really that Close to [Her]": Reasoning About Invisible Algorithms in the News Feed*, *in* CHI '15: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems at 153, 156 (New York 2015).

retargeting capabilities that utilize that large, blended dataset. Soon, Jane starts to see "Vote Yes on Prop A" advertisements on many unrelated websites, with the message that Prop A will be great for local wildlife.

Jane has no way of knowing this, but that pro-wildlife message has been chosen specifically for her, because of her past visits to cats.com. The ads are everywhere online (for Jane), so Jane believes that this message is a primary "Yes on A" talking point, and she's encouraged to vote in agreement. The "No on A" campaign never has any opportunity to discuss or debate the point. They may not even know that the cats-related topic has been raised, because they've never even been exposed to it—that message is reserved for retargeting campaigns directed at people like Jane. Jane's attempt to be a well-informed voter has been usurped by retargeting. And, perhaps most importantly, Jane doesn't even know this has happened.[17]

Even when the use of consumer data to power algorithmic decision-making can be directly harmful, such as when it affects livelihood-related opportunities or distorts consumers' perception of issues of importance, it may still be considered privacy violative when it exceeds consumers' expectations about how the data would be used.

3. Protections for consumers' private information should be forward-looking, flexible, strongly enforced, and carefully tailored based on context

Consumers want more control over their private information, and consistently are asking for it. According to a 2016 report from the Pew Research Center, "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

[17] Angela Grammatas, *Guest Post: Make Your Browsing Noiszy*, Mathbabe (Mar. 31, 2017), https://mathbabe.org/2017/03/31/guest-post-make-your-browsing-noiszy/.

privacy online.[18] Consumers need clear forward-looking protections that are flexible, strongly enforced, and appropriate based on context.

A. Protections for consumers' private information should be forward-looking, flexible, and strongly enforced

The FTC brings the bulk of federal privacy enforcement actions, but it lacks the tools it needs to be as effective as it could be. The agency only has after-the-fact enforcement authority, but no ability to define rules of the road before consumer data is used in ways that consumers consider inappropriate. And apart from the few contexts in which it has specific privacy authority, the FTC generally can only take enforcement action against entities that use consumer information in ways that violate their own consumer-facing commitments. When the FTC does take 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.[19] To improve privacy and data security for consumers, the FTC—or another agency or agencies—must be given more powerful regulatory tools and stronger enforcement authority.

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.

Regulations should also be flexible, allowing agencies to adjust them as technology changes, as the FTC did just a few years ago with the COPPA Rule.[20] Consumers are constantly encountering new types of privacy and data

---

[18] Lee Rainie, Pew Research Center, *The State of Privacy in Post-Snowden America* (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

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

[20] 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/

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.[21] We can't always forecast the next big threat years in advance, but unfortunately, we know that there will be one.

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. Indeed, the FTC has repeatedly asked for the civil penalty authority it needs to enforce data security.[22] Regulations are effective to deter violations only if entities fear the punishment that would surely follow.

B. Protections for consumers' private information should be tailored based on the avoidability of the information sharing,

---

press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over.

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

[22] *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.

the sensitivity of the information, and the expectations of consumers

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.

Whether a consumer has the ability to avoid sharing personal information with a private entity—such as in the case of a shopping list application, or no choice—such as in the case of an ISP or CRA, is relevant in considering what level of privacy protection is appropriate for a particular context. When information sharing is unavoidable or less avoidable by consumers, it is important that the information be protected. 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,[23] by consumers in a financial context,[24] by customers in a telecommunications context,[25] and by patients in a medical context.[26]

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

---

[23] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.
[24] Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338, (1999).
[25] 47 U.S.C. § 222.
[26] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 (1996).

> 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.[27]

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 Internet connectivity—information sharing may be considered unavoidable because the consumer cannot reasonably decline the service altogether.

Policymakers should also consider how the avoidability of any particular choice presented to a consumer may be affected or distorted by other factors that make it unavoidable as a practical matter, such as whether the choice is technically difficult for most consumers to understand or exercise, whether network effects diminish consumers' perception of the choice as optional, whether well-documented cognitive biases inhibit consumers' ability to rationally evaluate potential risks associated with the

[27] FTC, *FTC Policy Statement on Unfairness* (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

choice,[28] or whether the entity collecting consumer information is using coercive or deceptive tactics to get consumers to exercise a particular choice.[29]

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.[30] Other laws recognize the heightened sensitivity of health information[31] and financial information.[32] 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."[33]

---

[28] *See* Alessandro Acquisti, *Privacy in Electronic Commerce and the Economics of Immediate Gratification*, *in* EC '04 Proceedings of the 5th ACM Conference on Electronic Commerce (New York 2004), at 21, 27 ("We have shown that a model of rational privacy behavior is unrealistic, while models based on psychological distortions offer a more accurate depiction of the decision process. We have shown why individuals who genuinely would like to protect their privacy may not do so because of psychological distortions well documented in the behavioral economics literature. We have highlighted that these distortions may affect not only naïve individuals but also sophisticated ones. Surprisingly, we have also found that these inconsistencies may occur when individuals perceive the risks from not protecting their privacy as significant.").

[29] *See* Lauren E. Willis, *When Nudges Fail: Slippery Defaults*, 80 U. Chi. L. Rev. 1155 (2012); Lauren E. Willis, *Why Not Privacy by Default?*, 29 Berkeley Tech. L.J. (2014).

[30] 15 U.S.C. §§ 6501–6506.

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

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

[33] *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

Last year the FTC found that television viewing history can be considered sensitive information,[34] and the Federal Communications Commission (FCC) found that web browsing history can be considered sensitive.[35] Indeed, patent applications filed by Google indicate that it is possible to estimate user demographics and location information based on browsing histories.[36]

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

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

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 earlier this year to eliminate strong privacy regulations that had recently been passed by the FCC, consumers—on both sides of the aisle—were outraged.[37]

University) *available at* http://www.judiciary.senate.gov/meetings/continued-oversight-of-the-foreign-intelligence-surveillance-act.

[34] 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.

[35] 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.

[36] *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).

[37] *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.

Some lawmakers argued that repeal of the FCC's rules was needed to foster development of a consistent approach to privacy across the Internet.[38] 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."[39]

Congress also should not eliminate existing 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. 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.[40] 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

---

[38] *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.

[39] 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/documents/public_statements/1210663/mcsweeny_-_new_americas_open_technology_institute_4-17-17.pdf.

[40] *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 Qeustions 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.

reported in 2013, 97% of which involved fewer than 10,000 affected individuals.[41] Each data breach affected, on average, 74 individuals.[42]

4. Specific recommendations for regulation of CRAs

Congress should advance federal legislation to subject CRAs to closer regulatory oversight and stronger enforcement, and to enhance consumers' control of their own personal information.

A. Congress should consider subjecting the security practices of consumer reporting agencies to closer regulatory oversight and stronger enforcement

First and foremost, Congress should consider vesting a federal agency or agencies with the authority to more closely regulate and enforce the data security practices of CRAs. Both the FTC and the Consumer Financial Protection Bureau announced they were looking into the Equifax breach shortly after it occurred. But to help prevent similar breaches from occurring in the future, Congress should explore bolstering these agencies' authority to promulgate rules governing the data security practices of CRAs, to conduct ongoing review of CRAs' data security practices, to enforce rules, and to seek civil penalties for violations.

At this point, the FTC has rulemaking and enforcement authority over CRAs' data security practices, but no supervisory authority. In accordance with the Gramm-Leach-Bliley Act (GLBA), in 2002 the FTC promulgated the Safeguards Rule,[43] which governs the data security obligations of financial institutions, including CRAs.[44] Companies covered by the rule not only must align their own data security practices with the requirements of the rule, but

---

[41] 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.

[42] *Id.*

[43] 16 C.F.R. §314.

[44] Fed. Trade Comm'n, *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying (last visited Oct. 23, 2017).

also must ensure that their affiliates and service providers safeguard customer information in their care.[45] But as the Congressional Research Service explains, the FTC "has little up-front supervisory or enforcement authority, making it difficult to prevent an incident from occurring and instead often relying on enforcement after the fact."[46]

The CFPB, on the other hand, has exercised supervisory authority over CRAs since 2012, but lacks the authority to promulgate rules implementing or to enforce the data security provisions of GLBA.[47] Title X of the Dodd-Frank Act granted the CFPB rulemaking authority for much of GLBA, but according to the CFPB itself, Dodd-Frank "excluded financial institutions' information security safeguards under GLBA Section 501(b) from the CFPB's rulemaking, examination, and enforcement authority."[48]

In addition, Congress should consider urging the FTC and/or CFPB to complete a notice and comment rulemaking process to update the Safeguards Rule. The existing Safeguards Rule was promulgated in 2002. In 2016 the FTC began the process of updating that rule, and solicited public comment on a number of both questions, including about the substantive standards set forth in the rule, such as, "Should the Rule be modified to include more specific and prescriptive requirements for information security plans?" and "Should the Rule be modified to reference or incorporate any other information security standards or frameworks, such as the National Institute of Standards and Technology's Cybersecurity Framework or the Payment Card Industry Data Security Standards?"[49] The FTC has not completed the update. Most recently, in June, the FTC published a notice indicating that

---

[45] *Id.*

[46] N. Eric Weiss, *The Equifax Data Breach: An Overview and Issues for Congress*, CRS Insight (Sept. 29, 2017) at 2.

[47] *Id.*

[48] Consumer Fin. Protection Bureau, *Privacy of Consumer Financial Information – Gramm-Leach-Bliley Act (GLBA) Examination Procedures* at 1 (Oct. 2016), https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/102016_cfpb_GLBAExamManualUpdate.pdf.

[49] FTC Standards for Safeguarding Customer Information, Request for Public Comment, 81 Fed. Reg. 173 (Sept. 7, 2016), https://www.ftc.gov/system/files/documents/federal_register_notices/2016/09/frn_standards_for_safeguarding_customer_informtion.pdf.

the Safeguards Rule is "currently under review," and that the agency does not expect to complete the review in 2017.[50]

Congress should also consider giving one or both agencies the authority to seek civil penalties for violations of the Safeguards Rule. The FTC has itself called for civil penalty authority in the past to buttress its data security authority. As now–Acting Chairman of the FTC (then a Commissioner) Maureen Ohlhausen argued in remarks she delivered before Congressional Bipartisan Privacy Caucus in 2014,

> 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. Under current laws, the FTC only has the authority to seek civil penalties for data security violations with regard to children's online information under COPPA or credit report information under the FCRA.[51] To help ensure effective deterrence, we urge Congress to allow the FTC to seek civil penalties for data security and breach notice violations in appropriate circumstances.[52]

To improve the FTC's and CFPB's ability to protect Americans from poor data security practices of financial institutions that house extremely sensitive information, Congress should consider vesting one or both agencies with full-throated supervisory, rulemaking, and enforcement authority, and consider urging the update of the Safeguards Rule.

---

[50] FTC Regulatory Review Schedule, 82 Fed. Reg. 123 (June 28, 2017), https://www.ftc.gov/system/files/documents/federal_register_notices/2017/06/reg_review_schedule_published_frn.pdf.

[51] The FTC can also seek civil penalties for violations of administrative orders. 15 U.S.C. § 45(*l*) (footnote in original).

[52] 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.

B. Congress should consider expanding consumer tools for redress in the event of a CRA breach

In addition to taking steps to bolster regulatory and enforcement authority to help prevent similar breaches from taking place in the future, Congress should consider giving consumers better tools for redress when their personal information is compromised in a future breach. Specifically, Congress should consider streamlining the credit freeze process, establishing protective tools for victims of child identity theft and medical identity theft, and prohibiting mandatory arbitration clauses.

The credit freeze process is overdue for an overhaul—although credit freezes offer useful protection, they can be tedious, inconvenient, and costly. The credit freeze is, according to U.S. PIRG, "your best protection against someone opening new credit accounts in your name,"[53] and the IRS encourages consumers to consider requesting a freeze "if you were part of a large-scale data breach."[54] But the FTC cautions consumers considering a credit freeze to "[c]onsider the cost and hassle factor," because a credit freeze can delay access to credit, is only truly effective if secured across all three major CRAs, and may come at a cost of $5 to $10 for each CRA every time a consumer wishes to freeze or thaw their credit.[55] Congress should consider requiring CRAs to make it faster, easier, and free for consumers to freeze or thaw their credit, and to work together to ensure that a credit freeze or thaw request made with one CRA is applied to other bureaus as well. A protective tool like the credit freeze should be simplified so that consumers can easily access it, and should not be made available only to those consumers who can afford to pay for it either in time or in dollars.

Congress should also consider expanding the suite of tools that the law requires be made available to help consumers who become victims of identity

---

[53] Mike Litt & Edmund Mierzwinski, U.S. PIRG, *Why You Should Get Credit Freezes Before Your Information Is Stolen: Tips to Protect Yourself Against Identity Theft & Financial Fraud* at 1 (Oct. 2015), *available at* https://uspirg.org/sites/pirg/files/reports/USPIRGFREEZE_0.pdf.

[54] Internal Revenue Service, *Tips for Using Credit Bureaus to Help Protect Your Financial Accounts*, https://www.irs.gov/newsroom/tips-for-using-credit-bureaus-to-help-protect-your-financial-accounts (last visited Oct. 23, 2017).

[55] Lisa Weintraub Schifferle, Fed. Trade Comm'n, *Fraud Alert or Credit Freeze – Which Is Right for You?* (Sept. 14, 2017), https://www.consumer.ftc.gov/blog/2017/09/fraud-alert-or-credit-freeze-which-right-you (last visited Oct. 23, 2017).

theft. For consumers of financial identity theft, there are modest protections in place, including enhanced free credit monitoring and fraud alert options. But for other forms of identity theft, such as child identity theft and medical identity theft, no such tools exist. Congress should consider providing these victims with the tools they'll need to protect their identity—and if stolen, restore it.

In addition, Congress should consider prohibiting the use of mandatory arbitration clauses designed to keep consumers who have been the victim of data security or privacy violations out of court. Equifax invited tremendous criticism for its inclusion of a forced arbitration clause in the terms made available to individuals subject to its breach, and has since stated that it never intended to include the arbitration clause.[56] Congress should make clear that mandatory arbitration is never permissible where the privacy and data security obligations of financial institutions are concerned.

5. Congress should not issue federal data security or breach notification legislation that eliminates existing consumer protections

If Congress considers passing federal legislation on data security and breach notification, consumers would best be served by a bill that does not preempt state laws. If Congress nevertheless considers legislation that does preempt state data security and breach notification provisions, I urge you to explore legislation that is narrow, and that merely sets a floor for disparate state laws—not a ceiling.

In the event, however, that Congress nevertheless seriously considers broadly preemptive data security and breach notification legislation, the new federal standard should strengthen, or at the very least preserve, important protections that consumers currently enjoy at the state level. In particular, federal legislation:

1) should not ignore the serious physical, emotional, and other non-financial harms that consumers could suffer as a result of misuses of their personal information,

[56] *Oct. 3 Hearing* (prepared testimony of Richard F. Smith, Former Chairman and CEO, Equifax, Inc.), at 5, http://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf.

2) should not eliminate data security and breach notification protections for types of data that are currently protected under state law,

3) should provide a means to expand the range of information protected by the law as technology develops,

4) should include enforcement authority for state attorneys general, and

5) should be crafted in such a way as to avoid preempting privacy and general consumer protection laws.

I have previously presented these arguments before this Committee,[57] so I will not elaborate on them here.

6. Conclusion

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

[57] 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), *available at* https://democrats-energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony-Moy-CMT-Data-Breach-Legislation-2015-03-18.pdf.