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
Financial Services Committee

Hearing on

Continuation of Hearing Entitled
"Examining the Equifax Data Breach"

Wednesday, October 25, 2017

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

Introduction and Summary

Chairman Hensarling, Ranking Member Waters, and Members of the Committee:

Thank you for working to study and address data security and data breaches, and for the opportunity to testify on this important issue. I am the Deputy Director of the Center on Privacy & Technology at Georgetown University Law Center,[1] a think tank focused on privacy and surveillance law and policy. Today I represent my individual views on the Equifax data breach, data security, and breach notification, and not the views of my employer.

Consumers deserve better than this. They have no choice but to share highly private information with financial institutions in order to participate in the modern economy, and simply must trust that those institutions will do their absolutely best to safeguard that information. Equifax failed Americans, and nearly half of us—myself included—are going to be paying for that failure with a heightened risk of identity theft for the rest of our lives.

That is why hearings like this one, to interrogate the state of data security in our country today and to discuss ways that we might improve upon the status quo, are so important. As we try to move forward from the Equifax breach, I offer this Committee a few recommendations:

- 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
- Streamline the credit freeze process
- Establish protective tools for victims of child identity theft and medical identity theft

[1] I am very grateful for the assistance of four law student research assistants who assisted in the preparation of this testimony: Caroline Zitin, Eric Olson, Pia Benosa, and Zach Noble.

- Prohibit mandatory arbitration clauses designed to keep victims of data security or privacy violations out of court
- Avoid advancing legislation that weakens or eliminates consumer protections that currently exist at the state level
- Ensure that any federal legislation designed to enhance data security and/or breach notification standards includes regulatory flexibility to adapt to shifting threats
- Ensure that any federal legislation designed to enhance data security and/or breach notification standards includes enforcement authority for state attorneys general

I thank you for this opportunity and I look forward to answering your questions.

1. Equifax Made Mistakes

There is no question that 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 the large volume of data that ultimately was exfiltrated by attackers,[2] the months-long failure to patch the critical Apache Struts vulnerability that was

[2] *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*]

exploited,[3] the apparent lack of appropriate management and redundancies to ensure the patch would be applied,[4] and the months-long failure to detect the breach even as attackers continued to access and steal sensitive consumer data. These failures are well documented elsewhere,[5] so I will not elaborate on them.

Making matters worse, Equifax bungled post-breach activities as well.[6] First, Equifax did not directly notify affected consumers.[7] Instead, Equifax required consumers to visit a website to check whether they had been affected by the breach, but constructed that website on an unfamiliar domain (i.e. not Equifax.com) newly registered for that express purpose, which created confusion and introduced phishing vulnerabilities.[8] Second, Equifax's

---

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

[4] *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.

[5] *See, e.g.*, Complaint, Commonwealth of Massachusetts v. Equifax, Inc. (Sept. 19, 2017), *available at* http://www.mass.gov/ago/docs/press/2017/equifax-complaint.pdf.

[6] *See* Brian Krebs, *Equifax Breach Response Turns Dumpster Fire*, Krebs on Security (Sept. 8, 2017), https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/.

[7] *Examining the Equifax Data Breach: Hearing Before the H. Comm. on Financial Services*, 115th Cong. (Oct. 5, 2017) (dialogue between Rep. Brad Sherman and Richard F. Smith, Former Chairman and CEO, Equifax, Inc.), transcript not yet available (Rep. Sherman: "Is it the intention of Equifax to send a notice to those whose . . . data were compromised? Or is it up to them to go to your difficult-to-use, overburdened website to find out?" Smith: "We followed what we thought was due process. We sent out press releases, set up . . . a website, a phone number." Sherman: "How about noticing? Are you going to give notice to the 143 million people? Are you going to send them a letter?" Smith: "No, sir.").

[8] Dani Deahl & Ashley Carman, *For Weeks, Equifax Customer Service Has Been Directing Victims to a Fake Phishing Site*, The Verge (Sept. 20, 2017), https://www.theverge.com/2017/9/20/16339612/equifax-tweet-wrong-website-

call center and website were overwhelmed by visits from concerned consumers, many of whom found themselves completely unable to get through.[9] On top of all that, some Equifax executives are facing allegations of insider trading related to the breach.[10]

Consumers are justifiably outraged. 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 bac in the bottle.

Equifax's failures are all the more infuriating because consumers are not given a choice about whether or not their information will be shared with consumer reporting agencies (CRAs) like Equifax. The massive troves of valuable and potentially damaging information that CRAs maintain are provided by furnishers, not by consumers themselves.

And the consumers who suffer the worst are those who lack the time, resources, or technical sophistication to research and secure credit freezes or credit monitoring services. Even individuals with relatively sophisticated understanding of credit and the CRAs have expressed frustration with these

---

phishing-identity-monitoring ("Full-stack developer Nick Sweeting set up the misspelled phishing site in order to expose vulnerabilities that existed in Equifax's response page. 'I made the site because Equifax made a huge mistake by using a domain that doesn't have any trust attached to it [as opposed to hosting it on equifax.com],' Sweeting tells *The Verge*. 'It makes it ridiculously easy for scammers to come in and build clones — they can buy up dozens of domains, and typo-squat to get people to type in their info.'").

[9] Michelle Singletary, *Equifax Says It's Overwhelmed. Its Customers Say They Are Getting the Runaround*, Wash. Post (Sept. 19, 2017), https://www.washingtonpost.com/news/get-there/wp/2017/09/19/equifax-says-its-overwhelmed-its-customers-say-they-are-getting-the-runaround/.

[10] Tom Schoenberg, Anders Melin, & Matt Robinson, *Equifax Stock Sales Are the Focus of U.S. Criminal Probe*, Bloomberg (Sept. 18, 2017), https://www.bloomberg.com/news/articles/2017-09-18/equifax-stock-sales-said-to-be-focus-of-u-s-criminal-probe.

tools, which may therefore be unavailable as a practical matter to many under-resourced consumers.

2. Federal Legislation Should Set a Strong Consumer Protection Standard to Address Problems Highlighted by the Equifax Breach

Consumers need more control over their personal data, and companies need stronger incentives to improve data security. 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. Members of this committee and others have expressly called for the Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB) to examine the Equifax breach and take enforcement action in response to poor security practices. Both agencies appear to be looking into the Equifax breach. 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,[11] which governs the data security obligations of financial

[11] 16 C.F.R. §314

institutions, including CRAs.[12] Companies covered by the rule not only must align their own data security practices with the requirements of the rule, but also must ensure that their affiliates and service providers safeguard customer information in their care.[13] 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."[14]

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.[15] 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."[16]

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

---

[12] 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).
[13] *Id.*
[14] N. Eric Weiss, *The Equifax Data Breach: An Overview and Issues for Congress*, CRS Insight (Sept. 29, 2017) at 2.
[15] *Id.*
[16] 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.

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?"[17] The FTC has not completed the update. Most recently, in June, the FTC published a notice indicating that the Safeguards Rule is "currently under review," and that the agency does not expect to complete the review in 2017.[18]

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.[19] 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.[20]

---

[17] 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.

[18] 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.

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

[20] Maureen Ohlhausen, Commissioner, Fed. Trade Comm'n, Remarks Before the Congressional Bipartisan Privacy Caucus (Feb. 3, 2014), transcript

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.

B. Congress Should Consider Expanding Consumer Tools for Redress in the Event of a 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,"[21] and the IRS encourages consumers to consider requesting a freeze "if you were part of a large-scale data breach."[22] But the FTC cautions consumers considering a credit freeze to "[c]onsider the cost and hassle factor," because a credit freeze

---

available at https://www.ftc.gov/system/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen/140203datasecurityohlhausen.pdf.

[21] 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.

[22] 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).

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.[23] 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 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.[24] Congress should make clear that mandatory arbitration is never permissible where the privacy and data security obligations of financial institutions are concerned.

---

[23] 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).

[24]

3. Congress Should Not Issue Federal Data Security or Breach Notification Legislation that Eliminates Existing Consumer Protections

As I have argued before this committee in the past, many states are currently doing a very good job passing and adjusting data security and breach notification laws to respond to developing threats, monitoring threats to residents, guiding small businesses, and selectively bringing enforcement actions against violators. Therefore, 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 broad preemption, 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,

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.[25]

A. Federal Legislation Should Address Physical and Emotional Harms that Consumers Could Suffer as a Result of Misuses of Their Personal Information

This Committee's attention to the issue of data security and breach notification is driven first and foremost by the threat of identity theft and related financial harms. Thus some legislation that this Committee has considered in the past would allow covered entities to avoid notifying customers of a breach if they determine that there is no risk of financial harm. Such "harm triggers" in breach notification bills are problematic, because it is often very difficult to trace a specific harm to a particular breach, and because after a breach has occurred, spending time and resources on the completion of a risk analysis can delay notification. Moreover, a breached entity may not have the necessary information—or the appropriate incentive—to effectively judge the risk of harm created by the breach.

In addition, trigger standards narrowly focused on financial harm ignore the many non-financial harms that can result from a data breach. For example, an individual could suffer harm to dignity if he stored embarrassing photos in the cloud and those photos were compromised. If an individual's personal email were compromised and private emails made public, she could suffer harm to her reputation. And in some circumstances, breach could even lead to physical harm. For example, the fact that a domestic violence victim had called a support hotline or attorney, if it fell into the wrong hands, could endanger her life.

---

[25] These points are closely related to concerns I have previously presented before this Committee. *See* Testimony of Laura Moy before the House of Representatives Financial Services Committee Hearing on Protecting Consumers: Financial Data Security in the Age of Computer Hackers, *available at* https://financialservices.house.gov/UploadedFiles/HHRG-114-BA00-WState-LMoy-20150514.pdf.

Many state laws recognize these various types of non-financial harms. Accordingly, many states and the District of Columbia either require breach notification regardless of a risk assessment, or, if they do include some kind of harm trigger, take into account other types of harms beyond the strictly financial. There is no harm trigger at all in a handful of states, including, notably, California[26] and Texas.[27] In a majority of states, although the duty to notify is conditioned on a trigger, the trigger is not explicitly limited to risk of financial harm, and arguably encompasses non-financial harms as well. States in this category include Alaska,[28] Delaware,[29] Maryland,[30] North Carolina,[31] and Pennsylvania.[32]

A bill with a narrow financial harm trigger that preempts state laws that contemplate other types of harm would thus constitute a step backwards for many consumers. To address this problem, any legislation the Committee considers should either limit preemption so as to leave room for states to require notification even in circumstances where the harm is not clear or is

---

[26] Cal. Civ. Code § 1798.29.
[27] Tex. Bus. & Com. Code § 521.053.
[28] Alaska Stat. § 45.48.010 (notification not required if "the covered person determines that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach").
[29] Del. Code tit. 6, § 12B-102 (notification not required if, "after an appropriate investigation, the person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached").
[30] Md. Code Ann. Com. Law § 14-3504 (notification required if "the business determines that misuse of the individual's personal information has occurred or is reasonably likely to occur as a result of a breach of the security of a system").
[31] N.C. Gen. Stat. § 75-61 (definition of "security breach" limited to situations in which "illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer"); *see* N.C. Gen. Stat § 75-65.
[32] 73 Pa. Stat. Ann. § 2302 (definition of "breach of the security of the system" limited to situations in which unauthorized access "causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth").

not financial in nature, or include a trigger provision as inclusive as the most inclusive state-level triggers.

B. Federal Legislation Should Not Eliminate Data Security and Breach Notification Protections for Types of Data Currently Protected Under State Law

Many privacy and consumer advocates are concerned about recent legislative proposals on data security and breach notification that define the protected class of personal information too narrowly. A definition narrower than that of state data security and breach notification laws, in combination with broad preemption, would weaken existing protections in a number of states.

For example, under California law, entities must implement and maintain reasonable security procedures and practices to protect—and notify consumers of unauthorized access to—"[a] username or email address in combination with a password or security question and answer that would permit access to an online account."[33] Not only does coverage for online account login credentials help protect accounts holding private, but arguably non-financial, information such as personal emails and photographs, but it often protects a range of other online accounts, because many consumers recycle the same password across multiple accounts. To illustrate, consider when, in 2015, Uber accounts were hacked into, resulting in fraudulent charges to customers for rides they never took. Reporter Joseph Cox wrote about how those accounts may have been broken into using login credentials for unrelated accounts that were disclosed in other breaches:

> First, a hacker will get hold of any of the myriad data dumps of email and password combinations that are circulated in the digital underground. This list of login details will then be loaded into a computer program along with the Uber website

[33] Cal. Civ. Code §§ 1798.29; 1798.81.5.

configuration file. From here, the program will cycle through all of the login credentials and try them on the Uber website, in the hope that they have also been used to set up an Uber account.

"It's basically checking a database dump/account list against a certain website and displaying results," [a hacker who calls himself] Aaron told Motherboard over encrypted chat.

Aaron then demonstrated this process, and had accessed an Uber account within minutes. He tested 50 email and password combinations sourced from a leak of a gaming website, and two worked successfully on Uber. Aaron claimed one of these was a rider's account, and he then sent several censored screenshots of the user's trip history and some of their credit card details.[34]

A number of state laws also require private entities to protect information about physical and mental health, medical history, and insurance, including laws in California,[35] Florida,[36] and Texas.[37] This is important because attackers use information about health and medical care to facilitate medical identity theft, a rapidly growing threat.[38] Not only does medical identity theft often result in enormous charges to a patient for medical care she never received, but it can also pollute her medical record with false information about her health status, which could lead to additional

---

[34] Joseph Cox, *How Hackers Can Crack People's Uber Accounts to Sell on the Dark Web*, Medium (May 4, 2015), http://motherboard.vice.com/read/how-hackers-cracked-peoples-uber-accounts-to-sell-on-the-dark-web.
[35] Cal. Civ. Code § 1798.81.5.
[36] Fla. Stat. § 501.171.
[37] Tex. Bus. & Com. Code § 521.002.
[38] Ponemon Institute, *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data* (2016), *available at* https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf; Michelle Andrews, *The Rise of Medical Identity Theft*, Consumer Reports (Aug. 25, 2016), https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/.

complications or even physical harm down the road.[39] Health and medical information can also be used to inform spear phishing attacks, in which an attacker posing as a medical or insurance provider sends a fake bill or email to a patient asking for billing information related to recent treatment, thus tricking the patient into providing sensitive financial information.

North Dakota's breach notification law protects electronic signature, date of birth, and mother's maiden name, all pieces of information that could be used to verify identity for the purpose of fraudulently creating or logging into an online or financial account.[40]

Some states are also now requiring entities to take steps to protect biometric data.[41] This important step recognizes that a biometric identifier such as a fingerprint or iris scan cannot be changed by the individual to whom it belongs. Some states that now require protection of biometric data include Connecticut[42] and New Mexico.[43]

Health and medical information, login credentials for online accounts, and electronic signatures are just a few important categories of private information that would not be covered by a number of federal legislative proposals that have been under consideration in past years. At the same time, many of those same proposals would have preempted all of the above-referenced state laws that *do* protect that information, substantially

---

[39] *See* Joshua Cohen, *Medical Identity Theft—The Crime that Can Kill You*, MLMIC Dateline (Spring 2015), *available at* https://www.mlmic.com/wp-content/uploads/2014/04/Dateline-SE_Spring15.pdf ("A patient receiving medical care fraudulently can lead to the real patient receiving the wrong blood type, prescription, or even being misdiagnosed at a later time.").

[40] N.D. Cent. Code § 51-30.

[41] 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.'").

[42] Conn. Gen. Stat. § 38a-999b.

[43] NMSA §§ 57-12C-2; 57-12C-4.

weakening the protections that consumers currently enjoy. I urge this Committee not to approve such a bill.

C. Federal Legislation Should Provide Flexibility to Adjust to New and Changing Threats

Relatedly, a number of legislative proposals that have been advanced in the past would not provide the necessary flexibility to account for changing technology and information practices. Consumers are constantly encountering new types of threats as the information landscape evolves and creative attackers come up with new ways to exploit breached data. States are responding to developing threats affecting their residents by adjusting data security and breach notification protections as changing circumstances require, including by adding new categories of protected information such as medical information and biometric data.

We can't always forecast the next big threat years in advance, but unfortunately, we know that there will be one. For example, there are now multiple services that allow customers to upload photographs of physical car keys and house keys to the cloud, then order copies of those keys through an app, over the Web, or at key-cutting kiosks located at brick-and-mortar stores.[44] Will malicious attackers begin targeting photographs of keys to victims' homes? It might be too early to tell, but if they do, companies that collect and maintain that information ought to notify their customers, and the law ought to be able to be quickly adjusted to make sure that they do, without Congress having to pass another bill first.

The flexibility we need could be built into federal legislation in one of two ways. First, Congress could limit preemption in a manner that allows states to continue to establish standards for categories of information that

---

[44] Andy Greenberg, *The App I Used to Break into My Neighbor's Home*, WIRED (Jul. 25, 2014), http://www.wired.com/2014/07/keyme-let-me-break-in/; Sean Gallagher, *Now You Can Put Your Keys in the Cloud—Your* House *Keys*, Ars Technica (Mar. 20, 2015), http://arstechnica.com/information-technology/2015/03/now-you-can-put-your-keys-in-the-cloud-your-house-keys/.

fall outside the scope of federal protection as, for example, states have recently done with medical information and biometric data. Alternatively, Congress could establish agency rulemaking authority to redefine the category of protected information as appropriate to meet new threats. The Committee should not advance any data security and breach notification legislation that is not adaptable in one of these ways.

D. Federal Legislation Should Include Enforcement Authority for State Attorneys General

In the event the Committee ultimately approves a bill that preempts state data security and breach notification laws, the Committee should ensure that any such bill nevertheless includes both a requirement to notify, and an enforcement role for, state attorneys general. At a minimum, state attorneys general should have the authority to bring actions in federal court under the new federal standard.

State attorneys general play a critical role in policing data security and guiding breach notification to match the needs of their own residents. In addition, state attorneys general 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.[45] Each data breach affected, on average, 74 individuals.[46]

Federal agencies are well equipped to address large data security and breach notification cases, but could be overwhelmed if they lose the

---

[45] 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.

[46] *Id.*

complementary consumer protection support of state attorneys general in thousands of small cases each year. To ensure that consumers receive the best protection they possibly can—even when they are among a small handful of individuals affected by a breach—state attorneys general must be given the ability to help enforce any new federal standard.

E. Federal Legislation Narrowly Designed for Data Security and Breach Notification Should Be Crafted Not to Preempt a Wide Range of Privacy and General Consumer Protection Laws

Federal legislation also must be careful not to invalidate a wide range of existing consumer protections, including provisions that are at times used to enforce data security, but that are also used to provide other consumer or privacy protections. For example, the preemption provisions of some legislative proposals we have seen extend only to securing information from unauthorized access,[47] but as a practical matter, it will be exceedingly difficult to draw the line between information security and breach notification on the one hand, and privacy and general consumer protection on the other.

Generally speaking, "privacy" has to do with how information flows, what flows are appropriate, and who gets to make those determinations. Data or information "security" refers to the tools used to ensure that information flows occur as intended. When a data breach occurs, both the subject's privacy (their right to control how their information is used or

---

[47] H.R. 2205 would preempt requirements or prohibitions imposed under state law with respect to "safeguard[ing] information relating to consumers from (A) unauthorized access; and (B) unauthorized acquisition." H.R. 1770 would preempt state law "relating to or with respect to the security of data in electronic form or notification following a breach of security." It would supersede several sections of the Communications Act insofar as they "apply to covered entities with respect to securing information in electronic form from unauthorized access, including notification of unauthorized access to data in electronic form containing personal information."

shared) and information security (the measures put in place to facilitate and protect that control) are violated.

Privacy and security are thus distinct concepts, but they go hand in hand. From the consumer's perspective, a data breach that results in the exposure of her call records to the world is a terrible violation of her privacy. But the cause of the privacy violation may be a breakdown in security.

Accordingly, agencies enforcing against entities for security failures cite both privacy and security at the same time. For example, in the complaint it filed in June 2010 against Twitter for failing to implement reasonable security, the Federal Trade Commission argued that Twitter had "failed to provide reasonable and appropriate security to: prevent unauthorized access to nonpublic user information *and honor the privacy choices exercised by its users in designating certain tweets as nonpublic*."[48]

Not only does enforcement often address privacy and security simultaneously, but many laws that protect consumers' personal information could also be thought of in terms of both privacy and security. For example, in California, the Song-Beverly Credit Card Act prohibits retailers from recording any "personal identification information" of a credit cardholder in the course of a transaction.[49] In Connecticut, Section 42-470 of the General Statutes prohibits the public posting of any individual's Social Security number.[50] These laws could be framed as both privacy and data security laws. State-level general consumer protection laws prohibiting unfair and deceptive trade practices (sometimes known as "mini-FTC Acts") are also used to enforce both privacy and security.

Because each of these examples highlights a circumstance where privacy and security regulations are blended together, legislative proposals that may intend to leave intact privacy laws could nevertheless unintentionally eliminate privacy-oriented consumer protections that have a

---

[48] *Twitter, Inc.*, Complaint, para. 11 (2010), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2010/06/100624twittercmpt.pdf (emphasis added).
[49] Cal. Civ. Code § 1747.08.
[50] Conn. Gen. Stat. § 42-470.

data security aspect. Congress should therefore carefully tailor the scope of preemption in any data security and breach notification legislation it advances to avoid invalidating numerous privacy protections.

Conclusion

I am grateful for the Committee's attention to this important issue, and for the opportunity to present this testimony.