Written Testimony of Laura Moy
Senior Policy Counsel
New America's Open Technology Institute

Before the House of Representatives Financial Services Committee

Hearing on
Protecting Consumers: Financial Data Security in the Age of Computer Hackers

May 14, 2015

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

Thank you for working to address data security and data breaches, and for the opportunity to testify on this important issue. I represent New America's Open Technology Institute (OTI), where I am Senior Policy Counsel specializing in consumer privacy, telecommunications, and copyright. New America is a non-profit civic enterprise dedicated to the renewal of American politics, prosperity, and purpose in the digital age through big ideas, technological innovation, next generation politics, and creative engagement with broad audiences. OTI is New America's program dedicated to technology policy and technology development in support of digital rights, social justice, and universal access to open communications networks.

I have been invited here today to present my views as a consumer and privacy advocate. Consumers today share tremendous amounts of highly personal information with a wide range of actors both online and offline. Consumers can benefit enormously from sharing personal information, but distribution of personal information beyond its original purpose can lead to financial, emotional, or even

physical harms. In recognition of those possible harms, 47 states and the District of Columbia currently have data breach laws on the books, several states have specific data security laws, and many states also use general consumer protection provisions to enforce privacy and security.

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. Federal agencies, as well, are successfully enforcing the data security and breach notification authorities they currently have. Consumers would therefore be best served by a federal bill on this subject that is narrow, and that merely sets a floor for disparate state laws—not a ceiling.

But in the event 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. As this Committee considers legislative proposals for a federal data security and breach notification standard, we at the Open Technology Institute urge the consideration of several elements that could ultimately be the difference between legislation that helps consumers, and legislation that harms them.

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 not eliminate important protections under the Communications Act for telecommunications, cable, and satellite records,

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

6) should be crafted in such a way as to avoid preempting privacy and general consumer protection laws.[1]

## 1. 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 the bill currently before this Committee, and other bills the Committee might consider, may 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

---

[1] These points are closely related to concerns we have previously highlighted elsewhere. *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, *available at* http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-Wstate-MoyL-20150318.pdf; Letter to Senators John Thune and Bill Nelson, Feb. 5, 2015, https://cdt.org/insight/letter-to-senate-on-data-breach-legislative-proposals/.

individual could suffer harm to dignity if he stored nude 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.

Many state laws recognize these various types of non-financial harms. Accordingly, 33 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 California,[2] Illinois,[3] Minnesota,[4] Nevada,[5] New York,[6] North Dakota,[7] Texas,[8] and the District of Columbia.[9] The majority of states have a trigger that turns on "harm," "misuse," "loss," or "injury" not specifically financial in nature: Alaska,[10] Arkansas,[11] Colorado,[12] Connecticut,[13] Delaware,[14] Georgia, Hawaii,[15] Idaho,[16] Louisiana,[17] Maine,[18] Maryland,[19] Michigan,[20]

---

[2] Cal. Civ. Code § 1798.29.
[3] 815 Ill. Comp. Stat. § 530/10.
[4] Minn. Stat. § 325E.61.
[5] Nev. Rev. Stat. § 603A.220.
[6] N.Y. General Business Laws § 899aa.
[7] N.D. Cent. Code § 51-30-01, 51-30-02.
[8] Tex. Bus. & Com. Code § 521.053.
[9] D.C. Code § 28-3852.
[10] Alaska Stat. § 45.48.010.
[11] Ark. Code Ann. § 4-110-105.
[12] Colo. Rev. Stat. § 6-1-716.
[13] Conn. Gen. Stat. § 36a-701b.
[14] Del. Code tit. 6, § 12B-102.
[15] Haw. Rev. Stat. § 487N-1.
[16] Idaho Code Ann. § 28-51-105.
[17] La. Rev. Stat. Ann. § 51:3074.
[18] Me. Rev. Stat. Ann. tit. 10, § 1348.
[19] Md. Code Ann. Com. Law § 14-3504.

Mississippi,[21] Montana,[22] Nebraska,[23] New Hampshire,[24] New Jersey,[25] North Carolina,[26] Oregon,[27] Pennsylvania,[28] South Carolina,[29] Tennessee,[30] Utah,[31] Vermont,[32] Washington,[33] and Wyoming.[34]

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 consumers in the majority of states. To address this problem, any legislation the Committee approves 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 not financial in nature, or include a trigger provision as inclusive as the most inclusive state-level triggers.

### 2. 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 legislation proposals on data security and breach notification that define the protected class of personal information too narrowly. A definition narrower than

---

[20] Mich. Comp. Laws § 445.72.
[21] Miss. Code Ann. § 75-24-29.
[22] Mon. Code Ann. § 30-14-1704.
[23] Neb. Rev. Stat. § 87-803
[24] N.H. Rev. Stat. Ann. § 359-C:20
[25] N.J. Stat. Ann. § C.56:8-163.
[26] N.C. Gen. Stat. § 75-61; *see* N.C. Gen. Stat § 75-65.
[27] Or. Rev. Stat. § 646A.604.
[28] 73 Pa. Stat. Ann. § 2302.
[29] S.C. Code Ann. § 1-11-490.
[30] Tenn. Code Ann. § 47-18-2107.
[31] Utah Code Ann. § 13-44-202.
[32] Vt. Stat. Ann. § 2435.
[33] Wash. Rev. Code § 19.255.010.
[34] Wyo. Stat. Ann. § 40-12-502.

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's breach notification law, entities must notify consumers of unauthorized access to "[a] user name or email address, in combination with a password or security question and answer that would permit access to an online account."[35] Florida law also covers login information for online accounts.[36] 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 the recent reports regarding Uber accounts that were hacked into, resulting in fraudulent charges to customers for rides they never took. Last week, 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 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.

---

[35] Cal. Civ. Code § 1798.29.
[36] Fla. Stat. § 501.171.

> 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.[37]

A number of state laws also protect information about physical and mental health, medical history, and insurance, including laws in California,[38] Florida,[39] Missouri,[40] New Hampshire,[41] North Dakota,[42] Texas,[43] Virginia,[44] and—beginning later this year as recently passed bills go into effect—Hawaii,[45] Montana,[46] and Wyoming.[47] Attackers use information about health and medical care to facilitate

---

[37] 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.
[38] Cal. Civ. Code § 1798.29.
[39] Several federal data security and breach notification legislative proposals include a carve-out for entities already covered by federal laws that govern health information privacy. However, there are entities not covered by those federal laws that collect health-related information, and several legislative proposals would preempt state laws that cover health information and extend to those entities, without providing comparable coverage under the new federal standard.
[40] Mo. Rev. Stat. § 407.1500.
[41] N.H. Rev. Stat. Ann. § 359-C:20
[42] N.D. Cent. Code § 51-30-01, 51-30-02.
[43] Tex. Bus. & Com. Code § 521.002.
[44] Va. Code Ann. 32.1-127.1C.
[45] *See* Elizabeth Snell, *Wyoming Security Breach Notification Bill Includes Health Information*, Health IT Security (Feb. 23, 2015), http://healthitsecurity.com/2015/02/23/wyo-security-breach-notification-bill-includes-health-data/.
[46] *See* Cynthia Larose, Mintz Levin, *State Data Breach Notification Law Updates* (Mar. 10, 2015), http://www.privacyandsecuritymatters.com/2015/03/state-data-breach-notification-law-updates/.
[47] *See* Snell, *supra* note 45.

medical identity theft, a rapidly growing threat.[48] 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 complications or even physical harm down the road[49]. 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.[50]

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 we have seen this term, including the one before this Committee. At the same time, most proposals we have seen would eliminate all of the above-referenced state laws that

---

[48] Ponemon Institute, *Fifth Annual Study on Medical Identity Theft* 8 (2015), available at http://medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft/; Dan Munro, New Study Says Over 2 Million Americans Are Victims Of Medical Identity Theft, Forbes (Feb. 23, 2015), http://www.forbes.com/sites/danmunro/2015/02/23/new-study-says-over-2-million-americans-are-victims-of-medical-identity-theft/.

[49] *See* Experian, *Prevent Medical Identity Theft*, http://www.protectmyid.com/identity-theft-protection-resources/prevention-tips/medical-benefits.aspx (last visited May 11, 2015) ("When the victim seeks care, he or she could end up with the wrong medical history, wrong blood type, wrong allergies and other false information that could lead to serious problems. Victims may also find that their health insurance benefits have been exhausted due to a long period of misuse.").

[50] N.D. Cent. Code § 51-30.

*do* protect that information, substantially weakening the protections that consumers currently enjoy. We urge this Committee not to approve such a bill.

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

Relatedly, we are concerned that a number of legislative proposals we have seen 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. Right now, states are doing a good job responding to developing threats affecting their residents by adjusting data security and breach notification protections as necessary. Indeed, the fact that medical information is now covered by laws in ten states—including three that just passed bills this year—signals a deliberate response to the growing threat of medical identity theft, of which an estimated 2.32 million adult-aged Americans or close family members were victims during or before 2014, an increase over 2013 of 21.7%.[51]

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.[52] 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

---

[51] Ponemon Institute, *supra* note 48.
[52] 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/.

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 fall outside the scope of federal protection as, for example, Hawaii, Montana, and Wyoming did just this year with respect to medical information.[53] Alternatively, Congress could establish agency rulemaking authority to redefine the category of protected information as appropriate to meet new threats. We urge the Committee not to approve any data security and breach notification legislation that does neither of these two things.

### 4. Federal Legislation Should Not Eliminate Important Protections Under the Communications Act for Telecommunications, Cable, and Satellite Records

Federal legislation should not supersede important provisions of the Communications Act that protect the personal information of telecommunications, cable, and satellite customers. Under some legislative proposals, certain types of private information currently covered under the Communications Act would no longer be protected, and the information that would still be covered would be covered by lesser standards.

The Communications Act protects telecommunications subscribers' CPNI, which includes virtually all information about a customer's use of the service.[54] It also protects cable[55] and satellite[56] subscribers' information, including their viewing histories. But as with email login information and health records, some

---

[53] *See* Snell, *supra* note 45; Larose, *supra* note 46.
[54] 47 U.S.C. § 222.
[55] 47 U.S.C. § 551.
[56] 47 U.S.C. § 338.

bills we have seen this term—including the one currently before this Committee—are too narrow to cover all CPNI, and would not protect cable and satellite viewing histories at all. As a result, data security and breach notification protections for those types of information would simply be eliminated.

Such a reduction of the Federal Communications Commission's CPNI authority could not come at a worse time for consumers, because the FCC has just reclassified broadband Internet access as a telecommunications service under Title II of the Communications Act, enabling it to apply its CPNI authority to broadband providers. Indeed, the FCC just held a public workshop to explore issues associated with the application of the privacy provisions of Title II to broadband.[57] Applied to broadband, the CPNI provisions will require Internet service providers to safeguard information about use of the service that, as gatekeepers, they are in a unique position to collect. This could include information such as what sites an Internet user visits and how often, with whom she chats online, what apps she uses, what wireless devices she owns, and even the location of those devices.

It would not make sense to replace the strong data security and breach protections of context-specific federal laws such as the Communications Act with narrow protections designed to combat identity theft and fraud. While the primary purpose of many data security and breach notification standards is to protect consumers against financial harms, there are other important policy justifications for the data security and breach notification protections of other context-specific laws. For example, the protections of HIPAA strive to protect the relationship between medical patients and medical providers so that patients will be open and candid about their health status and needs so as to facilitate the best medical treatment possible. The protections of attorney-client privilege, as well as attorneys'

---

[57] FCC, *Public Workshop on Broadband Consumer Privacy* (Apr. 28, 2015), https://www.fcc.gov/events/wcb-and-cgb-public-workshop-broadband-consumer-privacy.

ethical obligations to keep client communications confidential, are designed to protect attorney-client relationships so that clients can be candid as they seek legal advice.

Analogously, the data security and breach notification protections of the Communications Act serve to foster citizens' confidence in our communications networks as safe places for the exercise of free and open speech and association. Disclosure of the fact that a person privately called a prenatal clinic, visited an online auction platform for firearms, or ordered an adult film on demand might not lead to financial harm, but if she did not trust that information to be maintained with the highest level of security protections, she might self-sensor her actions.

The consumer protections provided by the Communications Act are of critical importance to consumers, and appropriately overseen by an agency with decades of experience regulating entities that serve as gatekeepers to essential communications networks. Federal data security and breach notification legislation should not eliminate core components of those protections.

## 5. 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 mechanism 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.[58] Each data breach affected, on average, 74 individuals.[59]

Federal agencies are well equipped to address large data security and breach notification cases, but could be overwhelmed if they lose the 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 small breach—state attorneys general must be given the ability to help enforce any new federal standard.

### 6. 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 under state law and the Communications Act, 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,[60] but as a practical matter, it will

---

[58] 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.

[59] *Id.*

[60] 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

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 (his right to control how his information is used or 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 April 8, 2015 Order issued by the FCC adopting a Consent Decree to resolve its investigation into a data breach at AT&T, the FCC explained that "AT&T will be required to improve its *privacy* and data security practices by appointing a senior compliance manager who is *privacy certified*, conducting a *privacy risk assessment*, implementing an information security program, preparing an appropriate compliance manual, and regularly training employees on the company's *privacy policies* and the applicable *privacy legal authorities*."[61] Similarly, in the complaint it filed in June 2010 against Twitter for failing to implement reasonable security, the Federal Trade Commission

---

notification of unauthorized access to data in electronic form containing personal information."

[61] *AT&T Services, Inc.*, Order, para. 2 (2015), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0408/DA-15-399A1.pdf (emphasis added).

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*."[62]

Not only does enforcement often address privacy and security simultaneously, but many laws that protect consumers' personal information could also be thought of simultaneously 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.[63] In Connecticut, Section 42-470 of the General Statutes prohibits the public posting of any individual's Social Security number.[64] 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, consumer and privacy advocates are very concerned that some legislative proposals that may intend to leave intact privacy laws could nevertheless unintentionally eliminate some more privacy-oriented consumer protections that have a data security aspect. We therefore urge the Committee to carefully tailor the scope of preemption in any data security and breach notification bill it approves to avoid invalidating numerous privacy protections.

---

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

## Conclusion

We are not unequivocally opposed to the idea of federal data security and breach notification legislation, but any such legislation must strike a careful balance between preempting existing laws and providing consumers with new protections. The Open Technology Institute appreciates your commitment to consumer privacy, and we look forward to working with you to strengthen this bill and strike a better balance as it moves forward. I am grateful for the Committee's attention to this important issue, and for the opportunity to present this testimony.