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

Before the House of Representatives Energy & Commerce Committee
Subcommittee on Commerce, Manufacturing, and Trade

Hearing on
Discussion Draft of H.R. ___, Data Security and Breach Notification Act of 2015

March 18, 2015

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

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.

To preserve strong state standards and states' ability to adapt protections to best meet the needs of their own residents, a federal data security and breach notification law should merely set a *floor* for disparate state laws—not a ceiling. But the draft Data Security and Breach Notification Act would eliminate many state laws—as well as some provisions of federal law—that provide stronger consumer protections, in the interest of establishing a single standard nationwide.

In the event that Congress is seriously considering such broad preemption, the new federal standard should strengthen, or at the very least preserve, important protections that consumers currently enjoy. This bill, however, would *weaken* consumer protections in a number of ways, and eliminate protections altogether for some categories of personal information. We are particularly concerned that:

1) the bill's definition of personal information is too narrow,
2) it would condition breach notification on a narrow financial harm trigger,
3) it would replace strong existing information security protections with a less specific "reasonableness" standard,
4) it would supersede important provisions of the Communications Act, and
5) it could invalidate a wide range of privacy laws that do not deal exclusively with information security and data breach.[1]

---

[1] These are many of the same concerns that we voiced in a February 5, 2015 letter to Senators Thune and Nelson. Other signatories to the letter were Center for Democracy & Technology, Center for Digital Democracy, Consumer Action, Consumer Federation of America, Consumer Watchdog, National Consumers

1. The Bill Would Weaken or Eliminate Protections for Information that Falls Outside the Bill's Narrow Definition of "Personal Information"

First, many privacy and consumer advocates are concerned that this bill defines "personal information" too narrowly. This narrow definition, in combination with the preemption provision, would weaken existing protections by eliminating state-level protections for types of information that fall outside of its narrow terms.

For example, under Florida's data security and breach notification law, the definition of personal information includes an email address and password combination, information that could be used to compromise all of an individual's private emails, as well as information in any account that uses an email address as a login ID, because many consumers recycle the same password across multiple accounts.[2] Florida's law also protects a wide range of information about physical and mental health, medical history, and insurance,[3] as do the state laws of California,[4] Missouri,[5] New Hampshire,[6] North Dakota,[7] Texas,[8] Virginia,[9]

League, Public Knowledge, Privacy Rights Clearinghouse, and U.S. PIRG. Letter to Senators John Thune and Bill Nelson, Feb. 5, 2015, https://cdt.org/insight/letter-to-senate-on-data-breach-legislative-proposals/.

[2] Fla. Stat. § 501.171.

[3] Health care and insurance providers are not included in the definition of "covered entity" under this bill; thus, the bill would not preempt laws crafted narrowly to govern data security and breach notification with respect to those entities. However, there are entities other than health care and insurance providers that collect health-related information, and this bill would preempt state laws that cover health information and extend to those entities, without providing comparable coverage under the new federal standard.

[4] Cal. Civ. Code § 1798.29.

[5] Mo. Rev. Stat. § 407.1500.

[6] N.H. Rev. Stat. Ann. § 359-C:20

[7] N.D. Cent. Code § 51-30-01, 51-30-02.

[8] Tex. Bus. & Com. Code § 521.002.

[9] Va. Code Ann. 32.1-127.1C.

and—beginning July 1—Hawaii and Wyoming.[10] Compromised medical information is often a key element in medical identity theft, a rising trend.[11] North Dakota's breach notification law protects electronic signature, date of birth, and mother's maiden name, pieces of information that could be used to verify identity for the purpose of fraudulently creating or logging into an online or financial account.[12]

However, because health and medical information, email/password combinations, and electronic signatures do not fall within this bill's definition of "personal information," this bill does not protect that information, nor protect against the serious harms that breach of that information could lead to. At the same time, this bill would eliminate the state laws that *do* protect that information, substantially weakening the protections that consumers currently enjoy. In other words, today in seven states, companies are universally required to protect health information from data breach, and if this bill passes, consumers in those states will lose that protection.

Relatedly, we are concerned that this bill does not provide the necessary flexibility with respect to personal information to account for changing technology and information practices. Flexibility could be built in by limiting preemption in a manner that allows states to continue to establish standards for categories of information that fall outside the scope of this bill as, for example,

---

[10] *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/.

[11] 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/.

[12] N.D. Cent. Code § 51-30.

Hawaii and Wyoming did just this year.[13] Flexibility could also be created by providing agency rulemaking authority to enable the FTC to redefine personal information to include new categories of information to adapt to changing technology.

2. The Bill Would Weaken Existing Protections by Tying Breach Notification to a "Harm Trigger"

Second, we are concerned that this bill weakens existing consumer protections because it allows covered entities to avoid notifying customers of a breach if they determine that there is no risk of financial harm. Harm triggers 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, the 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, the trigger standard set forth in the bill is far too narrow, as it ignores the many non-financial harms that can result from a data breach. For example, an 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, many states 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. For example, there is no harm

---

[13] *See supra* note 10.

trigger at all in California,[14] Illinois,[15] Minnesota,[16] Nevada,[17] New York,[18] North Dakota,[19] Texas,[20] and the District of Columbia.[21] The majority of states have a trigger that turns on "harm," "misuse," "loss," or "injury" not specifically financial in nature: Alaska,[22] Arkansas,[23] Colorado,[24] Connecticut,[25] Delaware,[26] Georgia, Hawaii,[27] Idaho,[28] Louisiana,[29] Maine,[30] Maryland,[31] Michigan,[32] Mississippi,[33] Montana,[34] Nebraska,[35] New Hampshire,[36] New Jersey,[37] North Carolina,[38] Oregon,[39] Pennsylvania,[40] South Carolina,[41] Tennessee,[42] Utah,[43] Vermont,[44] Washington,[45] and Wyoming.[46]

---

[14] Cal. Civ. Code § 1798.29.
[15] 815 Ill. Comp. Stat. § 530/10.
[16] Minn. Stat. § 325E.61.
[17] Nev. Rev. Stat. § 603A.220.
[18] N.Y. General Business Laws § 899aa.
[19] N.D. Cent. Code § 51-30-01, 51-30-02.
[20] Tex. Bus. & Com. Code § 521.053.
[21] D.C. Code § 28-3852.
[22] Alaska Stat. § 45.48.010.
[23] Ark. Code Ann. § 4-110-105.
[24] Colo. Rev. Stat. § 6-1-716.
[25] Conn. Gen. Stat. § 36a-701b.
[26] Del. Code tit. 6, § 12B-102.
[27] Haw. Rev. Stat. § 487N-1.
[28] Idaho Code Ann. § 28-51-105.
[29] La. Rev. Stat. Ann. § 51:3074.
[30] Me. Rev. Stat. Ann. tit. 10, § 1348.
[31] Md. Code Ann. Com. Law § 14-3504.
[32] Mich. Comp. Laws § 445.72.
[33] Miss. Code Ann. § 75-24-29.
[34] Mon. Code Ann. § 30-14-1704.
[35] Neb. Rev. Stat. § 87-803
[36] N.H. Rev. Stat. Ann. § 359-C:20
[37] N.J. Stat. Ann. § C.56:8-163.
[38] N.C. Gen. Stat. § 75-61; *see* N.C. Gen. Stat § 75-65.
[39] Or. Rev. Stat. § 646A.604.
[40] 73 Pa. Stat. Ann. § 2302.
[41] S.C. Code Ann. § 1-11-490.
[42] Tenn. Code Ann. § 47-18-2107.

This bill constitutes a step backwards for many consumers in the above-named 33 states and the District of Columbia. The bill should leave room for states to require notification even in circumstances where the harm is not clear or is not financial in nature. Barring that, at the very least the bill's trigger provision should be as inclusive as the most inclusive state-level triggers.

3. The Bill's "Reasonableness" Security Standard Would Eliminate More Specific Data Security Protections Without Offering Consumers New Protections

Third, we are concerned that the bill's general "reasonableness" security standard, in combination with preemption provisions, would replace the more specific security standards set forth in many state laws and the FCC's rules implementing the Communications Act.

For example, Nevada's data security law requires covered entities that accept payment cards to abide by the Payment Card Industry Data Security Standard.[47] The data security regulations of Massachusetts set forth a number of very specific data security requirements.[48] The Communications Act grants the FCC rulemaking authority with respect to the information of telecommunications, cable, and satellite subscribers. The FCC's robust rules promulgated under that authority require telecommunications carriers to, among other things, train personnel on customer proprietary network information (CPNI), have an express disciplinary process in place for abuses, and annually certify that they are in

---

[43] Utah Code Ann. § 13-44-202.
[44] Vt. Stat. Ann. § 2435.
[45] Wash. Rev. Code § 19.255.010.
[46] Wyo. Stat. Ann. § 40-12-502.
[47] Nev. Rev. Stat. § 603A.215.
[48] 201 Mass. Code Regs. 17.03–17.04.

compliance with the CPNI rules.[49] The specific requirements of states such as Nevada and Massachusetts, along with the specific data security requirements imposed by the FCC, would all be eliminated by this bill and replaced with the less specific "reasonableness" standard.

Perhaps more significant, consumers residing in states that have no data security law on the books would not gain any new protections for their personal information from this bill, beyond what is already required under § 5 of the Federal Trade Commission Act as interpreted by the FTC. Since 2002, the FTC has brought over fifty cases against companies for failing to implement security measures that are "reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[50] The standard in this bill is the same as the standard that is already vigorously enforced by the FTC under its existing authority.

Because this bill would eliminate detailed state- and communications-sector-specific data security protections to institute a federal standard that does not offer anything new to protect consumers, this bill could actually water down data security requirements. It would be better for consumers if the bill set a nationwide floor at reasonable security, but allowed states and the FCC, at their discretion, to develop more specific requirements beyond that standard, as circumstances demand.

---

[49] 47 C.F.R. 64.2009.

[50] Federal Trade Commission, Commission Statement Marking the FTC's 50th Data Security Settlement at 1 (Jan. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

4. The Bill Would Eliminate Important Communications Act Protections for Telecommunications, Cable, and Satellite Customers

Fourth, we are concerned that this bill would supersede important provisions of the Communications Act that protect the personal information of telecommunications, cable, and satellite customers. Under this bill, some of the 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.[51] It also protects cable[52] and satellite[53] subscribers' information, including their viewing histories. But as with email login information and health records, this bill is too narrow to cover all CPNI, and it would not protect cable and satellite viewing histories at all, so data security and breach notification protections for those types of information would simply be eliminated

The proposed reduction of the FCC's CPNI authority could not come at a worse time for consumers, because the Federal Communications Commission has just voted to reclassify broadband Internet access as a telecommunications service under Title II of the Communications Act, enabling it to apply its CPNI authority to broadband Internet access providers. 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: 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.

---

[51] 47 U.S.C. § 222.
[52] 47 U.S.C. § 551.
[53] 47 U.S.C. § 338.

This bill strives to leave intact the FCC's authority to set privacy controls for the personal information of telecommunications, cable, and satellite customers. But privacy controls are of greatly diminished value when there are no information security standards for the information at stake. For example, under its Title II authority the FCC may clarify that a broadband provider has to obtain a customer's explicit opt-in consent before sharing his browsing history with a third party. In a situation like the recently publicized "permacookie," the FCC could find Verizon in violation of consent requirements for failing to get customers' permission before attaching unique identifiers to their Internet traffic that enabled third parties to learn information about their browsing histories. But under this bill the agency could not impose any security requirements on Verizon to protect customers' browsing histories in the future.

Moreover, as discussed further below, we are concerned that it will be difficult in practice to distinguish information security from traditional privacy, and that as a result this bill would in fact preempt the Communications Act's privacy provisions more broadly.

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. This bill threatens to eliminate core components of those protections.

5. The Bill Would Threaten a Wide Range of Privacy and General Consumer Protection Laws

Fifth, we are very concerned that the preemption language in the bill as currently drafted could eliminate a wide range of existing consumer protections under state law and the Communications Act, including many protections that may be used to enforce data security, but that are also used to provide other consumer or privacy protections. This bill is designed to preempt state law and

supersede the Communications Act only with respect to information security and breach notification,[54] 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.

We generally think of "privacy" as having 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.

Many laws that protect consumers' personal information could thus 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.[55] In Connecticut, Section 42-470 of the General Statutes prohibits the public posting of any individual's Social Security number.[56] 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 arguably constitutes a "law . . . relating to or with respect to the security of data in electronic form or notification following

---

[54] The bill 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."

[55] Cal. Civ. Code § 1747.08.

[56] Conn. Gen. Stat. § 42-470.

a breach of security" consistent with the legislation's preemption language, consumer and privacy advocates are very concerned that this bill could unintentionally eliminate these and other important state-level consumer protections that are not strictly data security protections, but that have a data security aspect.

Similarly, we are concerned that this bill could broadly eliminate the privacy protections of the Communications Act. The bill would supersede the Communications Act insofar as the referenced provisions "apply to covered entities with respect to securing information in electronic form from unauthorized access." It is unclear how this would apply to the FCC's privacy rules, such as the rules that determine when CPNI access is authorized, and when it is not. For example, the FCC's rules require carriers to get customers' express opt-in consent before sharing CPNI with third parties. Complying with the consent rules could thus be considered "securing information . . . from unauthorized access," while sharing information without the appropriate consent could be considered "unauthorized access," or failing to "secure information . . . from unauthorized access." In the Verizon permacookie example discussed briefly above, the FCC could find Verizon in violation of CPNI consent requirements for attaching unique identifiers' to its customers' web traffic, but Verizon could push back and argue that it did not foresee those identifiers being used by third parties for that purpose, and that the issue was therefore one of information security, rather than privacy.

In light of consumer protections that implicate both data security and privacy, such as California's Song-Beverly Credit Card Act and the FCC's CPNI rules, it is important for the subcommittee to reconsider the scope of preemption in this bill to avoid invalidating numerous privacy protections.

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 draft Data Security and Breach Notification Act of 2015 falls short of that balance. However, 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 Subcommittee's attention to this important issue, and for the opportunity to present this testimony.