December 7, 2015

The Honorable Jeb Hensarling
2228 Rayburn HOB
Washington, DC 20515

The Honorable Maxine Waters
2221 Rayburn HOB
Washington, DC 20515

Re: H.R. 2205 – Data Security Act of 2015

Dear Chairman Hensarling and Ranking Member Waters:

We, the undersigned privacy and consumer advocates, write in opposition to H.R. 2205, currently under consideration in the House Financial Services Committee. We are pleased that many members in the House are committed to improving data security and breach notification protections, particularly given the significantly harmful impact that data breaches can have on American consumers.

While the substitute bill that has been offered by Representative Neugebauer addresses some of the concerns we have voiced with a previous version of the bill, unfortunately it would still *weaken* consumer protections in a number of ways, and eliminate protections altogether for some categories of personal information. It also does not improve the level of protection for consumers, as most states already require notification in the event of a data breach, and federal and state consumer protection law already requires reasonable data security practices. On balance, H.R. 2205 would do consumers far more harm than good, and we therefore must urge you to oppose it.

First and foremost, H.R. 2205 would eliminate stronger existing state protections and prevent future state innovation. The Data Security Act of 2015 would supersede all state laws on data security and breach notification—including those protecting personal information not covered by this bill. For example, the legislation would squelch new and developing laws in several states extending data security and breach notification protections to online account login information, including email accounts and cloud photo storage. The bill does not cover information about an individual's geographic location or electronic communications. Biometric data is covered but only to the extent that it can be used to gain access to financial accounts. It is unclear whether "medical information" would include the broad range of data that is collected about individuals' physical or mental health through websites and wearable devices.

Thus, the bill would significantly set the nation back in its data security and breach notification efforts. As explained in July by 47 state and territorial attorneys general in a letter to congressional leaders, "Preempting state law would make consumers less protected than they are right now." According to the letter, "Our constituents are continually asking for greater protection. If states are limited by federal legislation, we will be unable to respond to their concerns."[1]

H.R. 2205 would eliminate means of redress currently available to consumers in many states. Not only would this bill eliminate stronger existing state protections, but it would also eliminate virtually all avenues of redress for consumers. For example, the law in some states currently provides consumers with a private right of action, and enables state attorneys general to seek restitution on behalf of consumers harmed by data breaches. But if this bill were to pass, state attorneys general would be limited to seeking civil penalties and injunctive relief, even in cases where consumers suffer extensive harm as a result of a breach of highly sensitive information. This would provide harmed consumers with no relief.

H.R. 2205 would eliminate critical flexibility to adapt data security and breach notification standards to address shifting threats. The bill would prevent states from innovating to protect their citizens as new security threats evolve by passing notification requirements for new data sets or developing other, non-breach related, data security rules. It also does not include a compensating mechanism, such as agency rulemaking, that would provide a streamlined process by which data security and breach notification protections could be extended to types of information that become the basis for widespread attacks in the future. In the era of the Internet of Things and ever-expanding cloud services, it would be a crucial mistake to hamstring states' ability to quickly innovate new protections for their citizens.

Further, H.R. 2205 would eliminate key protections under the Communications Act for telecommunications, cable, and satellite records. The Communications Act contains very strong data security and breach notification protections for information about customers' use of telecommunications services, such as phone call histories and location data. It also protects cable and satellite subscribers' information, including their viewing histories. But as with email login information and photos, this bill is too narrow to cover that information. It would

[1] Letter to Congressional Leaders from the National Association of Attorneys General (NAAG) (July 7, 2015), *available at* http://bit.ly/1LTmWVY.

simply eliminate crucial federal data security and breach notification protections for telecommunications usage information and cable and satellite viewing histories.

H.R. 2205 would tie breach notification to a "harm trigger" that is much narrower than existing laws in the majority of states. The trigger standard set forth in the bill is weaker than the laws in seven states and the District of Columbia—which it would invalidate. There are many negative consequences that can result from a data breach, such as harm to dignity from the compromise of nude photos, damage to one's reputation from the compromise of personal email, or harm to family integrity by the publication of private conversations between parents and children. A breach could even lead to physical danger, such as if logs of a domestic violence victim's calls to a support hotline were to fall into the wrong hands.

While there should be reasonable exceptions to a notification duty in situations where the data has been rendered unusable, such as when it has been encrypted, it should not otherwise be up to the breached entity to decide if harm is likely to occur. By creating a national trigger standard, this law would cause some consumers to stop receiving notifications about breaches that they currently have a right to hear about today.

The Data Security Act of 2015, contrary to its name, does not offer consumers meaningful new protections. H.R. 2205 goes beyond the reasonable data security standard required under many federal and state legal frameworks to require that covered entities "develop, implement, and maintain a comprehensive information security program." This is a step forward. However, because the bill covers such a narrow category of protected information, such security plans would only be required of entities that handle information falling into that category. At the same time, the bill would in fact eliminate data holders' existing duty to adopt reasonable security measures to protect broad categories of information falling outside the purview of the bill, but that consumers nevertheless consider personal or sensitive, such as photographs, call logs, children's conversations with their toys, **a**nd cable viewing histories. In addition, eliminating existing state protections and state enforcement would deal a devastating blow to consumer protection.

Rather than replacing state laws with a weaker standard and preventing states from taking stronger measures, a federal bill should offer *greater* protections than exist under the law today. This could include an expansion of the definition of personal information meriting breach notification (as some states have already done),

affirmative data security program requirements that apply to all private and sensitive information, data access requirements, and comprehensive privacy legislation.

Unless and until the House can improve this bill to offer consumers something new, rather than just retreading old ground and prohibiting states from acting to protect their citizens, we urge you to oppose the Data Security Act of 2015. We look forward to working with you to address the issues we have raised.

Respectfully submitted,

Center for Democracy & Technology
Center for Digital Democracy
Center for Economic Justice
Common Sense Kids Action
Consumer Action
Consumer Federation of America
Consumer Watchdog
Consumers Union
National Association of Consumer Advocates
National Consumer Law Center (on behalf of its low-income clients)
New America's Open Technology Institute
National Consumers League
Privacy Rights Clearinghouse
Public Citizen
Public Knowledge
U.S. PIRG
World Privacy Forum