April 9, 2015

The Honorable Fred Upton
Chairman
Committee on Energy and Commerce
125 Rayburn House Office Building
United States House of Representatives
Washington, D.C. 20515

The Honorable Frank Pallone
Ranking Member
Committee on Energy and Commerce
2322A Rayburn House Office Building
United States House of Representatives
Washington, D.C. 20515

Re: Data Security and Breach Notification Act of 2015

Dear Chairman Upton and Ranking Member Pallone:

We, the undersigned privacy and consumer advocates, write in opposition to the Data Security and Breach Notification Act of 2015, currently under consideration by the House Energy and Commerce Committee. We are pleased that the Committee is committed to improving data security and breach notification protections, particularly given the significantly harmful impact that data breaches can have on American consumers.

Unfortunately, the bill as currently drafted would actually *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. Unless it can be substantially improved in a number of ways, the bill would do more harm than good, and we therefore must urge you to oppose it.

First and foremost, the bill would eliminate stronger existing state protections and prevent future state innovation. The Data Security and Breach Notification 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 eliminate existing protections in nine states for health information that is not already protected by the Health Insurance Portability and Accountability Act. It would also 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. Thus,

the bill would significantly set the nation back in its data security and breach notification efforts.

The bill would eliminate critical flexibility to adapt data security and breach notification standards to address shifting threats. The Act would likely prevent states from innovating to protect their citizens by passing notification requirements for new data sets as new security threats evolve 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.

Further, the bill 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. It also protects cable and satellite subscribers' information, including their viewing histories. But as with email login information and health records, this bill is too narrow to cover all telecommunications usage information, and it would not protect cable and satellite viewing histories at all. The bill would simply eliminate data security and breach notification protections for sensitive information about use of these services. In addition, the breach notification and data security protections in this bill are weaker than existing law under the Communications Act.

The bill would tie breach notification to a financial harm trigger much narrower than existing laws in the majority of states. The trigger standard set forth in the bill is weaker than the laws in 33 states and the District of Columbia—which it would invalidate. There are many non-financial harms that can result from a data breach, such as harm to dignity from the compromise of nude photos, or harm to reputation from the compromise of personal email. A breach could even lead to physical harm, such as if logs of a domestic violence victim's calls to a support hotline were to fall into the wrong hands. By weakening the trigger standard in the overwhelming majority of states, this law would cause consumers to stop receiving notifications about breaches that they currently have a right to hear about today—breaches that could lead to physical or emotional harm.

The bill has weaker enforcement provisions than many existing laws. By tying penalties to the number of days an illegal practice was in effect (as opposed to the number of consumers affected), the bill would limit state attorneys general from obtaining meaningful relief in many data security cases. Furthermore, the Act does not offer a private right of action that would allow consumers to take direct action

to protect themselves without waiting for regulators. Today, seventeen states' laws include such a right. This bill would eliminate these protections and, again, prevent states from enacting new ones. Private rights of action buttress enforcement by state and federal officials and play an important role in encouraging fair markets.

The Data Security and Breach Notification Act of 2015, contrary to its name, offers little new to protect consumers. State data breach notification laws have been an incredibly helpful state innovation to deter and draw attention to bad data security practices and alert consumers to the potential for fraud or phishing schemes. However, notice is after the fact; it does not prevent data breaches from occurring. While we support reasonable data security requirements in the bill, the FTC and state attorneys general already enforce existing consumer protection law (as well as dedicated data security statutes in several states) to require the same. Rather than replacing state breach laws with a weaker single standard and preventing states from taking stronger measures, a federal bill that addresses notice 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, data access requirements, and comprehensive privacy legislation.

Unless and until the Committee 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 and Breach Notification 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
Consumer Action
Consumer Federation of America
Consumer Watchdog
Consumers Union
Electronic Frontier Foundation
National Consumers League
New America's Open Technology Institute
Privacy Rights Clearinghouse
Public Knowledge
U.S. PIRG