TO: Chairman Fred Upton and Ranking Member Frank Pallone
RE: Data breach legislative proposals
DATE: February 5, 2015

Dear Chairman Upton and Ranking Member Pallone,

We, the undersigned, submit the following in response to the recently announced "Personal Data Notification & Protection Act."[1] We are pleased that the President is committed to protecting the privacy and security of individuals' personal information. As the legislative proposal stands now, however, it would do more harm than good. With this in mind, below is a summary of our concerns with the proposal and our general recommendations for data breach legislation.

First and foremost, the President's proposal is problematic because it would eliminate many existing state protections and prevent future state innovation. The Personal Data Notification & Protection Act would supersede all state legislation on data breach notification — including state laws covering personal information not addressed in the President's bill or that provide other data security requirements. For example, the legislation would eliminate existing state protections for paper and other analog records (the President's bill only covers "computerized" data). Moreover, recent state laws to mandate health information and online account breach notification would be eliminated. The Act would also 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. Thus, the bill would significantly set the nation back in its data security and breach notification efforts.

Further, data breach legislation should not eliminate existing protections at the Federal Communications Commission. Although the President's proposal would not have this effect, a number of proposals from Congress would. The Federal Communications Commission (FCC) has data breach regulations in place governing providers of voice service, including providers of voice-over-IP (VOIP) that use telephone numbers (rather than pure "over the top" voice communications). The FCC also has rules protecting telecommunications and cable privacy. These important consumer protections should remain in place. A bill designed to expand the privacy protections of Americans should not eliminate existing privacy protections.

The President's proposal's 30-day notification period is longer than in many states. Many state laws require businesses to notify as soon as possible. Some states impose fines of up to $1,000 per day for each day that the business delays in notifying customers after the notification period has ended. The Personal Data

[1] Online: http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf.

Notification & Protection Act not only gives companies 30 days to notify, but allows for this time period to be extended an additional 30 days in certain circumstances. [2]

The President's proposal provides no direct remedy for consumers. The Act does not offer a private right of action, allowing consumers to take direct action to protect themselves without waiting for regulators. Today, seventeen states' laws include such a right. The President's 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 Personal Data Notification & Protection Act offers nothing 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. 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. We urge the administration to update its proposal to offer consumers something new, rather than just retreading old ground and prohibiting states from acting to protect their citizens.

For more information contact:

Justin Brookman
Center for Democracy & Technology
202.407.8812
justin@cdt.org

Alex Bradshaw
Center for Democracy & Technology
202.407.8822
alex@cdt.org

Respectfully Submitted,

Center for Democracy & Technology
Center for Digital Democracy
Consumer Action

---

[2] The extended notice period would prove harmful to citizens in numerous states. For example, California's health data breach laws provide for a shorter breach notice period. Preempting such laws to allow for longer periods between breach and consumer notification would significantly harm victims of medical identity theft. A 30 day notice period can lead to serious medical consequences and may prove devastating for victims of this crime.

Consumer Federation of America
Consumer Watchdog
National Consumers League
New America's Open Technology Institute
Public Knowledge
Privacy Rights Clearinghouse
U.S. PIRG