Testimony of

The Honorable Jon Leibowitz

Co-Chairman, 21st Century Privacy Coalition

on

"Discussion Draft of the Data Security and Breach Notification Act of 2015"

before the

House Energy & Commerce Committee

Subcommittee on Commerce, Manufacturing, and Trade

March 18, 2015

Chairman Burgess, Ranking Member Schakowsky, other distinguished Members of the Subcommittee, thank you for inviting me to testify at this important hearing. Let me first congratulate Chairman Burgess on his new role. He and I have worked together in the past on FTC-related health care issues, and he brings a wealth of expertise and a commitment to consumer protection to this Subcommittee. And Ranking Member Schakowsky brings a deep devotion to consumer issues going back her work at Illinois Public Action. Just as importantly, both of you are committed to finding practical solutions to real problems, which is why you will almost certainly develop many bipartisan initiatives going forward.

My name is Jon Leibowitz and, along with former Representative Mary Bono, I serve as co-chair of the 21st Century Privacy Coalition. Our group is comprised of the nation's leading communications companies, which have a strong interest in modernizing privacy and data security laws to bolster consumers' trust in online services and confidence in the privacy and security of their personal information.

You do not have to be the former Chairman of the Federal Trade Commission ("FTC") to be aware of the explosion of data breaches over the past several years. While some of the high-profile breaches make headlines, others do not. Forty-three percent of respondents in an annual survey by the Ponemon Institute reported experiencing some sort of data breach in 2014, and the Bureau of Justice Statistics estimates that 7% of all U.S. residents ages 16 and older were victims of identity theft in 2012. Unauthorized access to personal information is a problem that affects businesses and consumers in all fifty states. In our increasingly interconnected nation and world,

few, if any, businesses operating online only serve customers in one state, and breaches thus have an impact that transcends state boundaries.

That is why our coalition commends Representatives Welch and Blackburn for releasing the Data Security and Breach Notification Act. We also commend the FTC for supporting data breach legislation for more than a decade, and the Obama Administration for reaffirming its commitment to data breach legislation earlier this year.

The United States needs a uniform, national framework that will provide consumers with clearer protections and businesses with greater certainty. Consumers in Texas deserve the same degree of protection as consumers in Illinois, and only Congress can ensure that all consumers enjoy the same robust protections. By the same token, consumers should be able to rely on the same protections regardless of whether their personal information is held by a communications provider, an edge provider engaged in online commercial transactions, or a brick and mortar retailer processing customer financial data over the Internet.

We believe that legislation should contain several key elements. First, it should require companies to employ reasonable data security protections. While we commend those who have focused more on data breach notification, companies should be utilizing reasonable, effective, and up-to-date information security procedures. But flexibility is critical – there is no one-size-fits-all set of standards that is appropriate for all companies. Hackers are constantly innovating, and companies therefore must have the ability to adapt and respond to the dynamic and constantly-shifting attack vectors and incursion strategies employed by data thieves.

We therefore support the inclusion of the flexible information security provision in the draft legislation, and appreciate the bill's implicit recognition that what constitutes reasonable security measures and practices will vary depending upon the company, the nature of its activities and the data it is safeguarding, the types of threats it faces, and the kinds of reasonable tools and practices available (and appropriate for the size and scale of the company) to meet those threats.

Second, while it is critical that consumers be notified in the case of a data breach that could result in identity theft or other financial harm, Congress should avoid requirements that produce over-notification. If consumers are constantly barraged with notifications about even minor breaches that do not involve financial harm, consumers are likely to ignore notifications, which means that they will not be paying attention when notified of significant breaches. As a result, we agree that notification should only occur if there is a reasonable risk of identity theft or other financial harm. The cyber hackers and data thieves behind the raft of high-profile breaches that we have seen over the past several years are seeking to harvest financial account information, credit card numbers, and identification data, and the draft correctly targets the data that poses the greatest risk of economic harm.

In addition, while consumers should be notified as quickly as possible, there are legitimate reasons why notification needs to be delayed. For example, delay may be necessary to permit law enforcement to conduct a criminal investigation, especially when it may be possible

to catch criminals in the act. Delay may also be necessary to permit a company to evaluate the scope of a breach, or mitigate its impact.

Third, a uniform national framework should be enforced by the Federal Trade Commission as well as State Attorneys General, and should preempt other laws and causes of action. Preemption will ensure the uniformity of the requirements that apply to every company, and the benefits that extend to every consumer. Having to comply with a patchwork of state requirements has created confusion and uneven protection even though a single breach rarely obeys state boundaries.

Moreover, we believe that national data security legislation should also preempt state common law. Once Congress enacts robust, national data security requirements, companies' focus should be on compliance with these requirements. The uniform national framework that is the objective of this legislation would be undermined if class actions can still be brought pursuant to state law. The result would be a continuation of the patchwork of state requirements that provide inconsistent protections for consumers across the United States today.

Duplicative or conflicting federal laws are no less harmful than duplicative or conflicting state laws. The Communications Act's data security requirements are a prime example. There is nothing "unique" about unauthorized access to consumer information held by communications providers. It is the same information as that held by many other players in the Internet ecosystem, which is why the same framework should apply the same law and the same standards to all entities that engage in online activities. The information protected under this legislation

should not be subject to different or duplicative legal regimes just because some companies have historically been subject to certain requirements and others have not. The national policy enacted by this bill should put all companies on equal footing with respect to their data security and breach notification obligations.

The FTC is undoubtedly the preeminent federal agency policing data security. The FTC has a long and extraordinary history of enforcement experience, having brought more than fifty data security cases, over a hundred Do Not Call cases, and numerous other cases for various types of privacy violations. The FTC's Consumer Protection Bureau has a staff of dedicated professionals with decades of experience evaluating the reasonableness of companies' data security practices. And with this legislation, the FTC will gain a powerful new tool to use against companies that do not protect data security—fining authority. The agency currently lacks fining authority for unfair or deceptive acts or practices violations, except against companies that are already under an FTC order.

The Federal Trade Commission should be fully empowered to penalize companies that violate federal data security requirements. Subject to intervention by the FTC, State Attorneys General should also be able to go into court to enforce the new law's requirements.

Mr. Chairman, thank you for holding this hearing today. Our coalition commends the Subcommittee for a draft bill that would create a comprehensive, uniform national data security framework that includes the elements we have referenced in our testimony.

We look forward to working with this Subcommittee as it moves forward with legislation. Given the bipartisan congressional support for data breach legislation as well as support from the President and the FTC, we believe that Congress is poised to enact legislation that better protects consumers, and avoids the pitfalls inherent in today's patchwork of conflicting laws and requirements.

Thank you for the opportunity to testify, and I look forward to your questions.