Statement of Dr. Andrea M. Matwyshyn
Assistant Professor, Legal Studies and Business Ethics, The Wharton School, University of Pennsylvania/ Affiliate, Center for Technology, Innovation and Competition, University of Pennsylvania Law School/ Affiliate Scholar, Center for Internet and Society Stanford Law School

Before the
Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy and Commerce
U.S. House of Representatives
July 18, 2013

Chairman Upton, Ranking Member Waxman, and distinguished members of the Committee, it is my honor to be here with you today to discuss the future of data security regulation in the United States. My testimony today reflects my academic work and the cumulative knowledge that I have acquired during the last fourteen years as a corporate attorney and academic researching and studying the legal regulation of data breaches and information security policy. It further reflects practical knowledge obtained through long-standing relationships with insiders at Fortune 100 technology companies, consumer rights advocates, and independent information security professionals. The proposals I offer today reflect my consultations with experts in each of these impacted communities.

During the last decade, awareness of information security has dramatically increased among both consumers and companies, and state data breach notification statutes have contributed to this improvement. However, the field of information security is still in its early years, and the overall level of information security knowledge and care that currently exists in the United States is unsustainably poor. Consumer confidence in the data stewardship capabilities of both companies and government agencies is eroding, and dramatic information security improvements are necessary throughout the public and private sector. It is this context that frames the legal and policy conversation around data breach notification.

- The dominant objections from the business community with respect to the current state-level data breach notification regime arise from definitional ambiguities and interstate variation in regulatory filing requirements. Both objections can be resolved through a federal paradigm that (1) clearly defines a reportable breach as the unauthorized access of *any* protected information connected with a consumer login credential and (2) offers a centralized, publicly available Federal Trade Commission-managed filing registry. This approach simultaneously cuts compliance costs and provides efficient notice to regulators and consumers.
- A legal distinction should be drawn between data breach disclosure regulation and information security conduct regulation. Federally streamlining data breach notification should not preempt states' rights to regulate information security conduct - both with respect to sanctions for a failure to disclose or correctly notify consumers and with respect to inadequacy of information security measures.

- Limiting states' rights to impose liability for information security misconduct will further erode consumer trust and damage innovation in the United States.

* * *

Fortune 100 corporate executives tasked with data breach notification compliance have repeatedly voiced two dominant concerns regarding their compliance experiences with state data breach notification statutes – (1) definitional ambiguities and variation in state statutes around which information triggers a breach notification and (2) inconsistent filing requirements across state level agencies. As such, should Congress wish to author a federal data breach notification law, I propose a four-pronged approach.

(1) Reframe notification around a straightforward bright line rule - unauthorized access to consumer login credentials or any protected consumer-connected information.

Because of the definitional ambiguities around which types of "information" compromise trigger breach notification, a streamlined norm is emerging among the most sophisticated technology companies: when a consumer login credential[1] or *any* previously protected data connected with a consumer may have been accessed by an unauthorized individual, these sophisticated information technology companies are erring on the side of data breach notification. Although this standard may reach above the standards demanded by most current state level statutes, in practice, it is a more cost-efficient compliance standard. It creates a bright-line rule that intuitively maps onto logical structuring of information security measures inside the company.[2] Also, because this bright line rule of notification is consistent with widespread technology practices, reports by digital forensic investigators can serve as the primary basis for breach notification filings and require less supervision (and expense) of legal counsel.

Companies understand this bright line – it maps onto the way they value the information themselves. Information value is created through a combination of scarcity and context. Specifically, companies that license databases of consumer information create value by protecting and only selectively disclosing their information. The rarer a particular piece of information, the more potentially valuable it is. Perhaps counterintuitively, consumer information that may seem superficially irrelevant, such as my favorite flavor of ice cream, may in reality be my most valuable information. For example, a consumer may use her favorite flavor of ice cream as her security question for her bank website. While this information may seem trivial on its face, the context of its use as a security question generates a tremendous value for a criminal seeking to compromise her bank account. If her favorite flavor of ice cream is the information least widely known about her and if she use it as the answer to her bank account

[1] A consumer login credential refers to a user id and password.

[2] A company engaging in prudent information security structuring of its information creates multiple technological barriers between the databases that contain consumer credentials and information and the rest of the corporate network. Specifically, when a company structures its systems in a reasonable manner to protect consumer information, the information which is bound up with login credentials is frequently redundantly protected. Best industry practices create barriers whenever possible between the sections of the network that contain consumer login credentials and derivative information and those parts of the network that do not. Thus, when an intrusion is detected, if information security measures in place are rigorous, the intruder may compromise the network more broadly but may not necessarily access consumer information. Not every security compromise will result in a data breach notification.

security question, it becomes the key to an identity thief emptying her bank account. Thus, all consumer-connected information is valuable information in data breaches and should trigger notification requirements. Treating different types of consumer information differently – government identifiers versus email addresses versus purchasing preference information – ignores this role of scarcity and context in creating valuable information. A data breach notification regime that defines a breach as the compromise of consumer login credentials or any consumer-connected information better mirrors business reality.

(2) Encryption exemptions are not useful.

Although certain states offer encryption exemptions in their statutes, these exemptions are plagued with definitional ambiguities that confound technologists and compliance personnel. They should be eliminated. Regardless of whether information is encrypted, depending on the methods and operational practices used to encrypt, it may be simple for thieves to decrypt stolen data. Compliance personnel at sophisticated technology companies believe that blanket encryptions exemption gives a pass to companies with weak security, unfairly disadvantaging sophisticated companies who invest in state-of-the-art security and implementation. Indeed, sophisticated companies now compete on quality of security.[3]

(3) Create a centralized, publicly available data breach notification registry under the Federal Trade Commission.

One of the greatest frustrations voiced by data breach compliance personnel relates to variation across state statutes in designating a state level regulator for notification: compliance personnel must file numerous forms with various different state level regulators. Through the creation of a public, national data breach notification registry maintained by the Federal Trade Commission, compliance personnel would only need to engage in one regulator notification. This centralized filing should contain, at a minimum, the following information:

a. A consumer-friendly description of the breach written in plain English
b. Date of start of breach (if known)
c. Length and extent of intrusion
d. Date of detection
e. Name and contact information of the forensic investigator/head of incident response
f. Date of consumer notification
g. Total records impacted
h. Total people impacted
i. States of residency of impacted consumers and the number of records per state
j. Manner of notice provided to consumers (written, electronic, telephone, other)
k. Services offered to impacted consumers
l. Type of attack/ technical description of breach (hacking, inadvertent disclosure, stolen or lost hardware, insider wrongdoing, other)

[3] Nevertheless, on a uniform data breach disclosure form, it would be logical to include a line item asking whether the data was encrypted and which software was used to carry out this process. Through this additional disclosure consumers and regulators will be able to assess which companies are obviously not engaging in state-of-the-art information security practices.

m. Presence of encryption and identification of the version of software used
n. Description of acquired information
o. Cause of breach
p. Description of completed or planned improvements to information security in response to the breach
q. Name and contact information for a designated individual at the company to answer consumer questions.
r. Dates of previous breach notifications in the last five years

Through the creation of a centralized data breach notification registry, appropriate state level regulators can easily access information at their discretion. Meanwhile, the compromised entity only needs to engage in a single regulatory filing, plus any direct consumer notification – a dramatically streamlined and more cost-effective process. Further, consumers will be better served than they are through the current notification regime. Reporters and data privacy advocates will be able to better identify new data breaches and analyze their severity and impact more quickly. Therefore, the regulatory purpose for data breach notification statutes -- advising consumers of the existence of a breach which may be relevant to their preservation of digital identity – would be buttressed under this proposed approach.

(4) Do not preempt enforcement authority of state regulators.

Two fundamental assumptions of the model above for the federal harmonization of data breach notification are, first, the division between disclosure regulation and conduct regulation, and, second, preserving state enforcement authority. Data breach notification obligations implicate different policy and legal questions than does an assessment of the underlying appropriateness of the security conduct leading up to the breach. These two questions should remain distinct. In many legal regimes in the United States, the notification function of filings stands distinct from any liability imposition for underlying misconduct.[4] In securities law, for example, overlapping regulatory functions exist on both the federal and state level. Multiple regulators successfully collaborate to ensure consumer protection and market stability. Just as the Securities and Exchange Commission prescribes the appropriate format for public companies' periodic filings while preserving the possibility of enforcement action by state regulators, so too the Federal Trade Commission (and any other agency that considers a need for information security disclosure to exist in specific economic sectors) can prescribe a standardized data breach notification filing form.

Just as in the securities regulation context, a clear distinction should be drawn between disclosure liability and conduct liability data security regulation. While it is logical for Congress (and state agencies) to impose fines on companies who fail to submit data breach notification filings in a timely manner,[5] these fines are fundamentally different from and disconnected from the broader questions of the reasonableness of the underlying information security conduct

[4] For example in securities regulation, publicly traded companies are required to file periodic filings offering additional information to the market with respect to their important business activities. These notification obligations carry their own penalties for failure to timely perform these statutory obligations. However, any material misstatements or omissions that may exist in the filings are governed separately under both state and federal law.
[5] Similarly it would be reasonable to impose liability for any false or omitted information in those filings

implicated in the breach. As such, while Congress may wish to at this juncture address notification harmonization, *it would be unwise and damaging to technology innovation in the United States to limit liability for information security inadequacy.* Bolstering consumer confidence in technology-mediated business requires a safety net of legal protection and trust in data stewardship. A limitation of liability would instead allow companies to plan to financially absorb information security losses rather than working to improve their internal information security practices.

Information security inadequacy in our economy among both public and private entities is rampant. Because of the nature of information vulnerability, a database that is shared by a company with trusted partners is only as secure as the lowest level of information security implemented by any trusted partner in possession of that database. Therefore, it is essential that the highest possible floor of information security be created across various entities in the economy. Further, any federal limitation of liability for unreasonable information security conduct would actively damage the attempts of regulatory agencies such as the Securities and Exchange Commission to force companies to engage in significant improvements in information security.[6]

I urge Congress to encourage better disclosure in information security conduct, however, I also urge Congress to avoid prematurely limiting the negative legal incentives for corporate self-improvement in information security conduct. The best course of action with respect to any consideration of limitation of liability is one exercising deference to federalism concerns and states' regulatory interests in redressing the harms of their citizens for information security harms. Determining the best legal regime for addressing information security breach liability still requires extensive experimentation on the state level to arrive at an optimal framework. Different states engage with consumer protection questions in different ways, and no national consensus currently exists with respect to the best course of action for information security liability. The field of information security law is very young, and best practices of conduct continue to evolve rapidly. Similarly, legal scholarship offering guidance is still scarce. Information security experts are only beginning to create a community and professionalize. A broader social and scholarly conversation on information security policy is desperately needed, and it requires time to develop. At this juncture I believe strongly that it is dramatically premature and undesirable to federally limit liability for information security misconduct demonstrating a lack of due care. A centralized disclosure system and deference to federalism concerns present the best course of action at present.

[6] In October 2011 the Securities and Exchange Commission introduced guidance which required public companies to assess and disclose material breaches of information security. To date the Securities and Exchange Commission has expressed displeasure with the level of corporate disclosure happening in connection with this guidance.