United States Naval Academy

MIDN Dennis Devey
MIDN Sydney Frankenberg

Standardization, Certification, and Enforcement:

Leveraging Market Effects to Incentivize Data Protection on a National Scale

September 30th, 2016

Executive Summary:

The low priority society has placed on data protection has led to a series of negative externalities that have been accepted as the status quo. This proposal addresses those problems with a series of legislative acts that will create positive market pressure in favor of high standards for data security. The first piece of legislation is the National Data Protection Act, which will set a minimum national baseline for data security measures, in addition to standardizing breach notification laws. Coupled with the Data Protection Act is the Security Compliance Incentive Program (SCIP), which provides financial and legal motivation for corporations to adopt strict security standards. SCIP will incentivize early adopters by providing legal immunity from civil litigation for companies that are certified as compliant in the event of a data breach, in addition to making the initial cost of achieving compliance tax deductible. In addition, SCIP requires all certified companies to only do business with SCIP certified vendors and service providers, which will result in a cascading network effect as companies adopt the standards in order to remain competitive. A Bureau of Data Protection will be created under the auspices of the Federal Trade Commission, which will have the authority and resources required to spearhead adoption, guide policy, and enforce compliance. Creating a clear, effective national standard and incentivizing compliance with a more rigorous optional certification, coupled with the creation of a bureau capable of enforcement, will produce a public good and result in a correction of the market.

Economics of Security:

Government intervention in economic issues becomes justifiable when it is clear that the marketplace can no longer safely provide a public good. As a non-rivalrous and non-excludable resource, the Internet has taken on this role. A large information asymmetry exists because data holders have access to better information than consumers. The public is ignorant of how their information is protected and what safeguards are, or are not, in place. Furthermore, a moral hazard exists because data holders do not bear the cost of data losses --the uninformed public does. Essentially, companies behave differently than they would if they were fully exposed to the risk.

A great deal of published literature is dedicated to the technical failings of cyber security and the failures caused by specific software's inherent insecurities. This perspective fails to account for the economic complexities of implementing proper security, most prominently the unequal distribution of risk that is caused by unsafe data protection practices. Effectively addressing this market failure will require shifting the burden of the negative externalities associated with data breaches back to corporations.

Businesses have insufficient financial incentives or motivation to protect users' data; however this short-sighted thinking places the burden on consumers who largely lack the information and education necessary to take steps to safeguard their own information. Large corporations focus on reducing expenses and growing revenues in order to provide value for their stockholders. Data protection is not naturally a revenue earner; it is an expense that companies driven by capital investment are reluctant to embrace. The consequences of a breach are minimal, with remediation costs offset by insurance and tax deductions applied to the expenses stemming from a breach. Societies with limited regulation allow businesses to evolve quickly and encourage the development of incredible innovation and technology, but a lack of regulations also means that new challenges arise faster than governments can deal with them. When productivity drives the market, the acceleration of technology outpaces government regulation.

Free markets without regulation can expose the public to unacceptable levels of risk if there is nothing to hold businesses accountable for their actions. However, too much regulation can hurt the economy because unfunded mandates are a tax on the supplier. There must be a framework of incentive and regulation that provides consumers with confidence in the marketplace and that also incentivizes companies to protect data. It must also hold companies who do not comply with these standards accountable both financially and legally for derelict stewardship of data. There is an inherent risk of loss of growth and GDP from a lack of consumer confidence and a choking of the economy from reduced

access to funds. The key is to find the correct balancing between incentives and regulations. The bottom line is that the government needs to rethink its approach to cyber security law and to provide incentives for companies to invest in data protection.

Overview:

Establishing a national standard for data protection and breach notification with the National Data Protection Act (NDPA) is the highest priority. Formalizing a standard baseline that all data holders across industry will be held to elevates the minimum acceptable amount of security to a reasonable and responsible level. Creating and enforcing a national standard will enable non-compliant companies to be identified as such and hold them responsible for poor security before a breach happens. Continued failure to comply will result in a fine. In the event of a breach due to lax security, there will be set fines for the scale and consequence of the data lost, and the plaintiff will be exposed to expensive litigation.

After establishing the minimum baseline, the next step is to encourage data holders to implement a high standard of data protection by incentivizing optional compliance with a series of rules and regulations that make up the Security Compliance Incentive Program (SCIP). Any company certified and able to prove full compliance will earn legal immunity from civil litigation if a breach does occur. In addition, they will earn the ability to advertise themselves as a SCIP certified company. In order to remain certified compliant companies will only be allowed to do business with service providers and vendors who are also SCIP compliant. This will encourage positive market pressure towards the adoption of better security measures across the country.

In order to support the new rules and regulations the Bureau of Data Protection (BDP) will be created under the Federal Trade Commission. Modeling their operation off of the Bureau of Consumer Protection, the BDP will spearhead adoption, manage certification, and enforce compliance of the new laws surrounding cyber security.

National Data Protection Act:

The primary goal of the National Data Protection Act (NDPA) is to formalize and standardize the variety of laws that currently apply to cyber security. This act will preempt all existing state data security laws, establishing a single cohesive national standard. The NDPA will force companies to maintain a reasonable level of security, while ensuring uniformity in data protection nationwide. The "reasonable level of security" is intentionally flexible, and will be an upward trending baseline set by Bureau of Data Protection guidelines and case law. By establishing the idea of a reasonable baseline, companies can be held liable for failure to meet it either by BDP enforcement actions or damages lawsuits.

Coupled with the data protection legislation will be the National Breach Notification Provision, which will require companies that lose consumer's personal information to report their findings to the Bureau of Data Protection within 30 days of initial discovery. Personal information is defined as a name coupled with any government issued unique identity, such as a social security or driver's license number, or any financial or medical information. An exemption for this mandate will be made if a breached company is able to prove that all data accessed was encrypted. Initial breach reports will be sent to the BDP within 30 days, and affected individuals must be notified within 45 days. These deadlines can be extended at the request of law enforcement and companies so that they can properly assess the scope of the breach and insure they are able to restore the integrity of the data. We would propose a reasonable risk of harm threshold which would only require notification if it was determined that the information breached was liable or would be exploited. Companies would be required to document their risk of harm determinations. This will provide numerous benefits, the most important of these being the implementation of a national standard that simplifies post breach response by clearly delineating what is required of a company. Failure to comply will result in fines and the potential for civil liability.

A company reported to the BDP as out of compliance with the NDPA will have the opportunity to become compliant before a breach occurs. That company will be informed of their failures and instructed to mitigate the issues. The longer a company remains insecure, the mores fines they will be subject to and if a company is breached while they are not NDPA certified, they will be subject to more significant fines, levied by the BDP. The tiered fine structure will take into account the number of accounts affected and the value of the personal data stolen. In addition to regulatory fines, non-compliant companies will be especially exposed to the threat of lawsuits, having been found to not meet industry

minimums, and will be forced to into costly civil litigation over claims of gross negligence.

Security Compliance Incentive Program:

While the National Data Protection Act will establish the minimum level of protection that must be given to data, the Security Compliance Incentive Program (SCIP) will build on that foundation and incentivize the optional adoption of significantly more rigorous security practices. In the event of a data breach any company that is able to prove adherence to the SCIP standards will be provided legal immunity from civil litigation. More importantly in terms of addressing market pressures, in order to be SCIP compliant a company must require any service provider or vendor that does business with them to be SCIP compliant. This requirement will create an exponential spread of positive security practices, as larger corporations who desire the benefits of the program will require their subsidiaries and service providers to adhere to the more rigorous standards. Market pressures which previously encouraged prioritizing minimizing cost over security are now reversed, incentivizing strong security as a means to increase operational profit and minimize the costs of a data breach.

The SCIP security standard will be modeled off of the *201 C.M.R. 17: Standards for the Protection of Personal Information of Residents of the Commonwealth* --Massachusetts' comprehensive data protection and privacy law. The law contains a comprehensive list of security program requirements for both physical and digital data which are effective without placing an unreasonable burden or intellectual mandate on companies which implement it. Instead, while the requirements require more advanced security, each company is able to tailor the implementation independently. In addition to the security controls, the SCIP security standard will require regular training on cyber security for all personnel and data security training for all personnel who come into contact with consumer data.

All companies wishing to participate in SCIP will be required to self-certify and maintain records of their continued compliance. In the event of a breach they will be audited and made to demonstrate that they adhered to all requirements. If a company self certifies but is found to have been non-compliant, they will be subject to major fines and devastating class action lawsuits as penalty for false representation. However, if a company is breached through no fault of its own and all data is kept properly secured, that company will receive the benefits promised by the program.

The primary incentive for companies to adhere to SCIP is the Civil-Litigation Immunity Clause that will limit corporate liability if a breach occurs. The cost of remediating a data breach is eclipsed by the potential cost of a class-action lawsuit, making insulation against a ruinous judgment financially attractive to a company's bottom line. SCIP certification would provide **absolute immunity** from civil-liability for any company that is confirmed to be in full compliance at the time of breach by the Bureau of Data Protection. This complete insulation will limit the ability of victims of a data breach to litigate damages, but if the high standard for security is met, that would be all the affirmative defense needed to get the case thrown out. Absolute immunity from liability in the event of a data breach will be the most powerful incentive for adoption, and the public good of widespread compliance far outweighs that brought by punitive suits against companies that went and above and beyond to defend consumer data.

A critical component of this legislation is that companies that are certified as compliant with SCIP standards will have three years to ensure that all service providers and vendors that come into contact with their consumer data are SCIP compliant. Failure to meet this requirement will result in a loss of certification. As a result of this requirement, service providers and vendors will also improve their security posture in order to remain competitive and eligible to work with SCIP compliant companies. This will result in cascading compliance, as each node in the network will force all surrounding nodes to comply, resulting in an exponential increase in the number of compliant companies. The cascading compliance will result in considerable positive market pressure on businesses, forcing them to either adapt or lose their ability to compete in the marketplace.

Achieving the significant network effects needed to address the market failure will require a critical mass of adopters large enough that those effects begin to cascade. To this end, participation will be incentivized in the first five years of the program by making the initial costs of achieving compliance tax deductible. As the cascading effect begins, there will no longer be a need to artificially incentivize adoption as the state of the market will organically encourage compliance.

Bureau of Data Protection:

At this point in time, FTC data security efforts are handled by the Division of Privacy and Identity Protection. The current organization is far too small to effectively regulate the expansive new

legislation, necessitating a large increase in staff, jurisdiction, and cost. To address these shortcomings this division will be elevated to the Bureau of Data Protection (BDP), bringing with the title the authority and capability to enforce the new laws.

Operating much as the FTC currently does, the BDP will be authorized to perform random audits based on complaints, but the bulk of their work will be auditing companies who have self-reported breaches, making sure that all required data safeguards are in place and were properly implemented. In the event that those standards were not met, fines will be levied against the non-compliant company. In the event that a company claims compliance with SCIP but fails to meet all requirements there is a significantly stiffer penalty.

The BDP will have the ability to accredit independent auditors who can be hired by companies to qualify their self-certification. This will allow companies to preemptively ensure that they will not be found liable in the event of a breach.

While there will be an initial startup cost for the BDP, it will become self-sufficient over time, offsetting expenses by collecting a small fee from each company that wishes to self-certify, as well as using fines of non-compliant companies. The Bureau will have authority over all of industry; however, sectors covered by more stringent data protection standards will remain under the same regulations as before.

Conclusion:

This proposal serves two main purposes. First, to establish a minimum federal standard for data protection and breach notification under the National Data Protection Act that will preempt the convoluted extant state laws. Second, to modify the value placed by the market on security in order to incentivize companies to adhere to more stringent data protection guidelines under the Security Compliance Incentive Program. Creating a cohesive national baseline that all data holders can be held to will minimize the existing negative externalities by shifting the risks associated with data breaches back to data holders while lowering consumer risks. By creating a baseline for data protection standards, this policy seeks to create positive market pressures by heavily incentivizing compliance and counteracting the current lack of emphasis placed on data protection. By rewarding early adopters and building a critical mass through cascading compliance, the market will begin to self-regulate, as companies are forced to secure their data or cease to be competitive.