Correcting Market Failure Through the Expansion of Federal Trade Commission Authority

Cyber Security Awareness Week Policy Competition Proposal
September 30, 2016

University of Illinois College of Law
Magdala Boyer
Michael Burdi
Matthew Chang
Kathleen Kramer
Matthew Loar
Mark Nagel
Bradley Williams

I. Introduction

This proposal, written by students at the University of Illinois College of Law, proposes that Congress should give authority to the Federal Trade Commission (FTC) to engage in rulemaking to establish high cybersecurity policies for corporations. This proposal further suggests providing corporations with a federal cyber insurance program. Corporations that join this federal cyber insurance program will be required to meet the FTC's high standards. But, corporations will be indemnified by the policy if data breaches occur. If corporations do not choose to participate in the federal cyber insurance policy, the FTC may penalize their actions as unfair or deceptive practices.

Part II of this proposal explains why the FTC should engage in rulemaking. Part III of this proposal reviews how Congress empowers the FTC to bring action against unfair or deceptive practices and why the Agency is suited for enforcement of our proposal. Part IV proposes a recommendation to create a federal cyber insurance policy that would indemnify parties if they meet high cybersecurity standards set by the FTC. Part V describes alternative mitigating factors that are likely to occur in response to the creation of the FTC's rulemaking capabilities. Finally, Parts VI and VII outlines existing cybersecurity policies in the marketplace and current issues for consumers seeking tort remedies in data breaches, emphasizing the need for our proposal to be accepted.

II. Rulemaking

In order to create a standard suited for a particular time, the FTC should engage in rulemaking. These rulemaking procedures should follow the procedural requirements of informal/notice and comment rulemaking prescribed by the Administrative Procedure Act (APA).[i] By engaging in rulemaking, the FTC will be able to (1) provide proper notice to

companies and (2) consider comments sent in from a wide variety of stakeholders, including consumers that are harmed by data breaches.

An important tenet of informal rulemaking is the fact that it provides for notice to affected parties.[2] In this scenario, interested parties will include a large grouping of people, including consumers and businesses that store, transmit, or receive personal information. Notice requirements under the APA mandate that in certain cases that notices of proposed rules are posted in the Federal Register, allowing for a simple and easily accessible way to view a new proposed standard. This greatly increases public access while legitimizing the process of rulemaking that will have important effects on how organizations operate when dealing with customer information.

The comment procedure is also important in this context. Once organizations are aware of the FTC's proposed standard, they are able to comment on it, making it incumbent upon the agency to consider it.[3] This system creates a discourse where interested stakeholders can address issues that a standard might bring up, or relevant alternatives that the agency might need to consider in its final rule. In the context of data practices, this discourse is important because it allows a wide range of technical specialties to discuss implications of the proposed standard.

Notice and comment rulemaking will thus provide a reasonable way to create a new standard. Once a standard is created, it also can be amended to change with new developments in technology and/or the agency's prerogative, following the applicable notice and comment guidelines outlined in the APA.[4]

III. FTC Enforcement via Statutory Liability

A market correction in favor of greater security is not likely to be produced from tort liability. Statutory liability, however may provide adequate pressure. We propose investing authority in the FTC to seek civil damages under such a statutory liability regime.

The FTC is empowered to bring actions for "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices."[5] Using this authority, the FTC has successfully brought suits against businesses that have lost consumer information in data breaches. [6] The theories under which the FTC has enforced data protection have been connected to unfair methods of competition or deceptive practices on the part of the breached business.[7] Thus, using existing authority the FTC likely could not reach a business who lost consumer information in a breach but did not engage in unfair methods of competition or deceptive practices. Furthermore, the FTC Act exempts many types of businesses from the FTC's enforcement authority in section 45(a)(1).[8] Common carriers and banks, for example, are exempted from the FTC's enforcement authority.[9]

To create a market correction by imposing statutory liability, the FTC must be granted two kinds of additional authority. First, the FTC must be empowered to bring actions for any data breach regardless of whether or not the breach involved unfair methods of competition or deceptive practices. Second, the FTC must be granted authority to bring actions against any business that has been breached, regardless of whether or not that business is a common carrier, bank, or is otherwise exempted from the FTC's existing authority.

A new statutory grant of authority to the FTC to bring civil actions against businesses for data breaches must be granted as a new and separate authority. Without reference to the existing authority to bring actions for unfair competition or deceptive practices this new authority will not be subject to the same exemptions. Thus, a new and separate statutory authority for the FTC

accomplishes both necessary grants of power to bring actions against all types of businesses when the business' consumer data is breached.

IV. Federal Cyber Insurance Program

It is not clear, however, that the adoption of a cybersecurity standard and enforcement activity by the FTC would be sufficient. Many small and mid-size businesses handle personal information, but they may slip "under the radar" and avoid enforcement actions. Furthermore, regulatory imposition of a cybersecurity standard may be used to show negligence *per se* in private suits over data breaches, if the defendant is shown to not be in compliance.

Prudent companies, therefore, in addition to reducing their collection of personal information and increasing their security efforts, will want to insure against the risk of fines or judgments. The nascent cyber-insurance industry, however, may not be able to satisfy this demand. Currently insurance companies refuse to insure for more than the relatively-small sum of $20 million, and businesses are forced to stack multiple policies to adequately cover their risk.[10] The private sector may not be willing or able to cover the increased risk of liability from our proposals.

We further propose, therefore, that a federal cyber insurance program be created, loosely modeled on FDIC deposit insurance.[11] Like FDIC deposit insurance, but unlike private cyber-insurance, the purpose of this program would not be to indemnify the business against realized losses after a lawsuit, but rather to protect consumers.[12] After a breach, the insurance program would provide affected consumers with credit monitoring and indemnify them against losses from fraud fairly traceable to the breach. This program would be funded by assessments charged to the member companies. To qualify for membership, the company would have to be regularly audited by the program in order to establish their compliance with the cybersecurity standard.

Companies could advertise their membership to give consumers confidence that their data was protected. They would be motivated to seek membership because it would not only guard against tort liability by proactively making affected consumers whole, but the regular audits would also provide strong evidence that the company is in compliance with the cybersecurity standard and thus make FTC enforcement action unlikely.

As an alternative, Congress may opt instead to create a program of federally-funded reinsurance for private cyber-insurance policies. Armed with the cybersecurity standard, the private insurers may establish a more-robust auditing scheme for their policyholders. The resulting increase in actuarial confidence combined with the reinsurance program could prod the insurers to write larger policies that adequately cover the risk.

V. Additional Actions to Mitigate Market Failure

In addition to the adoption of a cybersecurity standard, there are other actions that could mitigate the market failure. One of these methods would include efforts to nurture the industries and areas of technology that contribute to cybersecurity. Creating an environment for cybersecurity companies to thrive could increase other companies' abilities to provide their consumers with better security. With the adoption of a cybersecurity standard, we anticipate that companies involved with cybersecurity such as penetration testing companies will grow. As more businesses begin to adopt the cybersecurity standard, we want to ensure that they are not hit with an undue regulatory burden. This burden can be alleviated by encouraging and incentivizing growth in cybersecurity companies and private security consultants, thereby making it easier for businesses to adopt the cybersecurity standard. While we expect such companies and consultants to arise in the event of the promulgation of a cybersecurity standard,

focusing on the growth of such actors could help reduce the risk of a market failure resulting from a lack of technical cyber expertise in the market.

The cybersecurity standards will inevitably have to be updated as society outgrows them. This opens up the possibility of another market failure if there are not enough goods or services to meet the cybersecurity needs in the future. As such, we propose investing in and encouraging private firms to continue developing cybersecurity technologies. This could take the form of tax breaks, research funds, or even just facilitating collaboration. "[O]pponents of government cybersecurity regulations [have] claim[ed] that government mandates will actually hamper cybersecurity and other innovations in the private sector."[13] Actively encouraging such innovation could help to alleviate these fears. Others have noted "that cybersecurity regulations would impose substantial costs, which the private sector would be incapable of meeting profitably."[14] This may or may not be true, but the current landscape has proven insufficient to correct these market failures, and in an effort to further alleviate any concerns, we propose investing in cybersecurity companies to develop effective cybersecurity systems.

One last indirect method of encouraging growth in cybersecurity companies would be to increase collaboration. President Barack Obama has already initiated some mechanisms to such an end, signing an executive order that encourages sharing of information between industry and government in an attempt to increase collaboration and keep up with cyber threats.[15]Further encouragement would be necessary to ensure innovation is not hampered and to allow for the standards to rise as necessary.

VI. Creation of New Standards

Under this proposal, the FTC would be given the statutory authority for determining cybersecurity standards as well as unfair or deceptive business practices. The need to promote

better data security practices over time suggests that whatever standards that the FTC may promulgate should not be immune to change. As a starting point for the FTC, however, some commonly used and thoroughly-tested standards suggest themselves. Existing industry standards, like the Payment Card Industry Data Security Standard (PCI), already contain many data security practices that the FTC may want to further develop. PCI applies to parties who accept or process payment cards, a standard broad enough to encompass a huge array of businesses. PCI's security standards include good cybersecurity practices that are effective, yet simple enough for a small family business to implement as well as a large corporation. These include requirements to maintain firewalls, to change all manufacturer default password, to restrict the number of parties who might have access to cardholder data, and to regularly test network resources.[16]

PCI regularly publishes guidelines to help affected parties understand each requirement. For example, the requirement to maintain a firewall configuration more specifically requires that public access between the internet and any component in the cardholder data environment be prohibited.[17] Similarly to our proposal, PCI uses 'qualified assessors' to assess compliance with its expansive requirements.[18] Well-developed standards like PCI serve as a good model for a standard that the FTC might promulgate, though unlike PCI, the FTC would not be limited to a particular industry or transaction type.

Another potential starting point for security standards would be NIST's Cybersecurity Framework. Many of the parties that would be affected by our proposed standards regime would have already become familiar with the NIST's Framework, as it has been at the center of data security discussions for years. As a foundation for a potential FTC data security standard, the Framework would be highly effective. At highest level, the Framework functions as a simple checklist of potentially vulnerable areas, with each step supplemented by an array of documents

to guide improvements in security.[19] Despite receiving much praise for its comprehensiveness, the NIST Framework has not reached high enough adoption levels that consumer data is adequately protected. Critical industries, like financial institutions, have adopted the Framework at a rate as low as 29%.[20] As a voluntary approach, assessing the true rate of adoption and of industry preparedness is difficult, as companies may choose to adopt certain parts of the Framework or none at all.[21]

Since indemnification of breach liability is contingent on the complete adoption of a comprehensive set of cybersecurity standards, our proposal will better promote the complete adoption of security standards, and provide a better picture of which industries are adequately prepared for cyber threats. While industry-developed standards and the NIST Framework might provide a good initial set of standards for the FTC to promulgate, ensuring the continued development of better security practices will come from continued investment and FTC rulemakings.

VII. Inadequacy of Tort Liability

To correct market failure, the United States government could create tort liability to incentivize companies to implement stronger cybersecurity measures. One of the primary purposes of tort law is to redress consumer harms when a company has definitively harmed him or her or acted such that harm is certainly impending.[22] For companies failing to maintain secure infrastructures to protect consumer data, consumers could sue companies under a theory of negligence (for failing to meet a duty or standard of care) or under a theory of strict liability (holding companies liable for any injuries).[23]

However, United States Federal Circuit Courts of Appeals have split when deciding whether corporations should be held liable for consumer data breaches under tort law. The issue

is whether customers have standing to sue[24] for harm that is "certainly impending."[25] Some courts have ruled that the consumers' harms are "immediate and real," justifying standing to bring suit.[26] The Seventh Circuit, for example, held consumers victimized in a data breach had standing to sue[27]: In a case involving consumer credit card information stolen in a cyber-attack from a high-end department store, the court reasoned that a reasonable likelihood existed that consumers would be subjected to future fraudulent charges to survive a motion to dismiss. However, other courts have ruled that consumers' possible future harms are not sufficient to establish standing.[28] The Third Circuit, as a counter-example, held that consumers cannot establish standing when they "have not suffered any injury" and "there has been no misuse of the information, and thus, no harm."[29] While most Circuits have embraced the Seventh Circuit's approach, reasoning that consumers have been injured-in-fact to establish standing, the Supreme Court has not yet resolved this circuit split.[30]

Due to this circuit split, this proposal argues that the FTC should be provided an enforcement mechanism to fine corporations rather than imposing strict liability. Under this proposal, the Federal Trade Commission would have the statutory authority for determining cybersecurity standards as well as unfair or deceptive business practices. By authorizing the Federal Trade Commission to find companies not meeting these rules, consumers' injuries are guaranteed to be redressed, regardless of what jurisdiction they reside in at the time of their injury.

VIII. Conclusion

Congress should grant the FTC authority to engage in rulemaking to establish strong cybersecurity policies for corporations to meet. To incentive corporations to meet these high standards, the federal government will also provide reasonable cyber insurance. Both

corporations and consumers will benefit from enacting our proposal because higher cybersecurity protection means less data breaches and consumers harmed.

References

[i] 5 U.S.C. § 553(b)–(c) (2012).

[2] *Id.*

[3] *Id.*

[4] *See id.*

[5] Federal Trade Commission Act 15 U.S.C. § 45(a)(1) (2012).

[6] *See*, *e.g. F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236 (2015).

[7] *See, e.g.*, *Id.*

[8] 15 U.S.C. § 45(2) (2012).

[9] *Id.*

[10] *A Buyer's Guide to Cyber Insurance*, McguireWoods (Oct. 2, 2013), https://www.mcguirewoods.com/Client-Resources/Alerts/2013/10/Buyers-Guide-to-Cyber-Insurance.aspx.

[11] *FDIC: Insurance Program*, Federal Deposit Insurance Corporation, https://www.fdic.gov/about/strategic/strategic/insurance.html (last visited Sept. 29, 2016).

[12] *Id.* ("When [banks] fail, the FDIC ensures that the financial institution's customers have timely access to their insured deposits and other services.").

[13] Amitai Etzioni, *The Private Sector: A Reluctant Partner in Cybersecurity*, Geo. J. Int'l Aff. (2014).

[14] *Id.*

[15] Sarah Buhr & Alex Wilhelm, *Obama Sign Executive Order Encouraging Private-Sector Companies to Share Cyber Security Information*, TechCrunch (Feb. 13, 2015), https://techcrunch.com/2015/02/13/obama-cyber-security/.

[16] PCI DSS Quick Reference Guide, PCI Standards Council, 9 (accessed Sept. 29, 2016), https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf?agreement=true&time=1475267678021.

[17] *Id.* at 12.

[18] *Id.* at 10.

[19] Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0, National Institute of Standards and Technology, 20-35 (Feb. 12, 2014).

[20] Roy Urrico, Few Adopt NIST Cybersecurity Framework: Survey, Credit Union Times (Mar. 29, 2016), http://www.cutimes.com/2016/03/29/few-adopt-nist-cybersecurity-framework-survey.

[21] James A. Lewis, NIST Cybersecurity Framework, Center for Strategic & International Studies (Apr. 16, 2014) https://www.csis.org/analysis/nist-cybersecurity-framework.

[22] U.S. Const. art. III, § 2, cl. 1.

[23] *See, e.g.*, 28 U.S.C. § 1332(d) (allowing for various forms of relief for disclosing customer information in class action lawsuits).

[24] Hollingsworth v. Perry, 133 S.Ct. 2652, 2661 (2013) (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992).

[25] Clapper v. Amnesty Int'l USA, 133 S.Ct. 1138, 1147 (2013).

[26] Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 693 (7th Cir. 2015).

[27] *Id.* at 694.

[28] Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011).

[29] *Id.*

[30] *See generally* Galaria v. Nationwide Mut. Ins. Co., 2016 WL 4728027 (6th Cir. 2016); Krottner v. Starbucks Corp., 628 F.ed 1139 (9th Cir. 2010).