Federal Data Breach Policy Proposal

Madeleine Barowsky

Elizabeth Dethy

Nathaniel Fruchter

for 6.805 Foundations of Information Policy

Massachusetts Institute of Technology

December 9, 2017

"A data breach is the perfect storm. It destroys customer loyalty, ruins corporate reputations, absorbs employee time and scarce resources, and opens the door to regulatory actions and lawsuits."
—Kivu.com[1]

Rep. Matsui (D-CA): *"Can you please describe to me how Equifax complied with the state law?"*

Mr. Robert Smith (former Equifax CEO): *"I just don't have specific knowledge as it relates to the state of California."*
—House Committee on Energy and Commerce Hearing (10/3/2017)[2]

1 *Data protection in the United States: overview — Practical Law* 2017.
2 *Oversight of the Equifax Data Breach: Answers for Consumers* 2017.

CONTENTS

LIST OF TABLES

1 EXECUTIVE SUMMARY

In 2016 the Identity Theft Resource Center reported the occurrence of 1093 public data breaches compromising at least 36 million records[1]. Data breaches are a pervasive, underreported problem[2]. While many know of the high-profile data breaches at Equifax and Yahoo, it is not just technology companies and data brokers that are affected. Local school districts[3] and dentists[4] also suffer data breaches. Breaches of every size and scope create social and monetary harms for victims. These harms are exacerbated by the patchwork of state and federal laws that deal with breach notification, breach recourse, and information security standards.

Data breaches impact individuals' liberties and put them at risk of identity theft, financial fraud, and other painful actions. The United States government has an avowed interest in protecting individuals from these harms due to the irresponsible actions of others. Despite existing legislation to achieve these aims, the current policy landscape does not protect individuals from damages suffered in the event of a data breach.

In this paper, we examine the current shortcomings of existing data breach laws in the United States and provide a holistic approach to data breach policy. It is imperative that all data handlers are prepared to investigate, contain, and respond to a breach when it occurs. It is not sufficient to assume that voluntary security measures an organization undertakes to protect personal information will be enough to eliminate the possibility of a data breach.

Failure to tackle the root causes of security breaches, lack of enforcement and citizen recourse, and narrow, state-based scope limit the efficacy of existing data breach laws. Existing laws do not incentivize strong security practices explicitly; rather, they focus singularly on notifying consumers. This solely reactive approach cannot address the complexity, scale, and severity of personal data breaches. Furthermore, each state has passed its own data breach notification law and differences in the details between states form a confusing regulatory regime.

The definitions each state law uses for personal data and covered entity are mostly limited to health and financial data handled by corporations, too specific to fully regulate the innumerable data breaches that impact people every

1 *Data Breach Reports 2016 End of Year Report.* 2017. Technical report. Identity Theft Resource Center, January. Accessed October 5, 2017.

2 The CEO of the Identity Theft Resource Center asserted that they "are extremely confident that breaches are undiscovered and under-reported, and... don't know the full scope." Olga Kharif 2017.

3 Tanya Roscorla 2016.

4 Rob Meaglia 2013.

day. Our proposed policy broadens "personal data" to include user-supplied content data and applies to commercial, charitable, and governmental organizations who handle such information (see C).

Market pressures that penalize insecure organizations and reward those with good data protection practices are insufficient in getting corporations to adhere to better security standards. Further, they do not apply to government agencies or nonprofits—despite extensive use by these groups of personal data. Without regulation that notifies the public of a breach, organizations will hide cyber incidents to avoid financial and reputational harm.

This proposal presents four main contributions for a federal standard for data breaches in the United States. First, timely and clear notification to affected persons remains a key element along with standards about notification deadlines, formats and content. Secondly, we propose pre-breach practices to force data handlers to regularly review security and risk management strategies. Thirdly, we propose post-breach practices for increased transparency between data handlers, the FTC, and affected individuals. Finally, we expand the definition of personal data to include user-supplied content in addition to health and financial data, and place businesses, government agencies, and nonprofits all under the umbrella of covered entities.

As preparation is essential for a coordinated and effective response, we propose two **pre-breach practices**. These protocols encourage organizations to evaluate their data landscape, assess risks posed by their current security posture, think realistically about the aftermath of a breach, and take steps to improve their cybersecurity preparedness.

- Organizations will be required to file a *Data Breach Action Plan* with the regulatory authority (including an inventory of personal data, how the entity will monitor for and investigate a breach, details of notification method and content, and potential actions for consumers to mitigate harms or seek damages)
- Disseminating *cybersecurity recommendations* for specific tools, checks, or strategies. We are not aiming for a checklist: security is asset-based and evolves, so attempts to prescribe one-size-fits-all standards may actually desensitize organizations to certain risks.

We advocate for the expansion of the FTC's authority by defining a violation of our proposal as an unfair or deceptive act under the FTC's jurisdiction (Data Security and Breach Notification Legislation: Selected Legal Issues). This would allow the Commission to investigate, levy fines, or enter consent decrees with organizations who do not comply. We also set statutory damages on a per-record basis, making the risk of insecure data practices tangible to covered entities and giving individuals more avenues towards restitution.

Following discovery of a breach, we require organizations to

- Immediately notify the regulatory authority. The FTC will not publicly disclose the event and will, in consultation with relevant agencies,

make determinations about whether notification must be delayed for reasons of national security.

- Adhere to their filed breach response plan, keeping the authorities aware of major deviations.

We set a tiered notification standard to remove the vagueness present in other laws about sending notice within a "reasonable" timeframe. The technical complexities of investigating a data breach necessitate evidence-based tiers that consider the type of data stolen and the scale and cause of the compromise when setting notification manner and timeline.

It is important for issues of consumer protection and national security that the regulatory agency is aware of unfolding breaches. Holding organizations to the standard they set incentivizes them to keep their breach response plan thorough and up to date.

The combination of these best practices, transparency efforts, and regulatory frameworks will benefit individuals and data handlers alike by decreasing the incidence of data breaches and empowering affected bodies to act swiftly in response.