Application to Present Research at PrivacyCon 2018

November 17th, 2017

Please find enclosed our application to present at the 2018 FTC PrivacyCon. Our submission is composed of this cover page along with an extended abstract describing our work on future data breach liability and notification schemes in the United States context.

This work was done as part of *Foundations of Internet Policy*, a class at Massachusetts Institute of Technology and is being submitted to PrivacyCon with the permission of the instructors.

Contact Information

Madeleine Barowsky
Undergraduate Student
Wellesley College Computer Science and Mathematics Departments

Elizabeth Dethy
Graduate Student
MIT Electrical Engineering and Computer Science Department

Nathaniel Fruchter
Graduate Student
MIT Technology and Policy Program and Internet Policy Research Initiative

Extended Abstract

The United States government has an avowed interest in protecting individuals' liberties and shielding them from identity theft, financial fraud, and other painful outcomes caused by the irresponsible actions of others. Data breaches impact all of these tenets, leaving people vulnerable to social and monetary harms.

The prevalence and impact of data breaches have continued to grow over the last decade. Most recently, an attack at Equifax compromised the Social Security numbers and credit data of 143 million Americans. A 2013 attack at Target affected 110 million credit cards, despite the company being in compliance with industry cybersecurity standards. Another 2013 attack at Yahoo compromised names, email addresses, and more for all 3 billion of its user accounts. The full magnitude of the Yahoo breach was only publicly revealed in October 2017, years after it happened and too late for people to take remedial action to secure other accounts. Incidents in 2015 at the Office of Personnel Management (OPM) and infamous dating website Ashley Madison exposed, respectively, security clearance forms for prospective and current government employees and credit card and user account information for a sensitive service.

Our research extrapolates lessons from a number of recent notorious incidents, using the knowledge to inform novel policy that both synthesizes prior legislation, expands the categories of covered entity and personal data, and introduces new ideas to incentivize data breach prevention.

More specifically, this paper examines the current shortcomings of existing data breach laws in the United States and provides a holistic approach to data breach policy that includes *pre- and post-breach requirements for prevention and response in addition to tailored notification regulations.* We argue it is insufficient to assume that voluntary security measures an organization undertakes to protect personal information will be enough to completely eliminate the possibility of a data breach. Thus, it is imperative that companies, government agencies, and all data handlers are prepared to investigate, contain, and respond to a breach when it occurs.

Problems With Current Market and Regulatory Regimes

There are immense financial costs from a breach to the data handler. They may endure customer churn, lost intellectual property and competitive advantage, and internal organizational shakeups and must pay steep fees for cybersecurity, legal, and public relations experts. Given these costs, economics dictates that companies will invest in preventative security to reduce the risk of a data breach—why is federal regulation necessary at all if the private market can correct insecure practices?

Although there may be some market pressures that penalize insecure organizations and reward those with good data protection practices, they do not apply to information brokers (e.g. Equifax), government agencies, or nonprofits—despite extensive use by these groups of personal data. Furthermore, without a requirement to notify the public of a breach, organizations will hide cyber incidents to avoid financial and reputational harm. The market cannot punish insecure companies and reward proactive ones if it does not have an accurate picture of how many incidents each experiences. Thus, even if there is some positive balancing effect from customer churn and exorbitant costs, federal regulation is needed to ensure that breaches are adequately reported and publicized.

The efficacy of existing data breach laws is limited by failure to address the root causes of security breaches, lack of enforcement and citizen recourse, and their narrow, state-based scope. Existing laws focus singularly on notifying consumers when unencrypted personal information has been accessed by an unauthorized third party instead of incentivizing strong security practices to begin. This solely reactive approach is outdated; it cannot address the growing complexity, scale, and severity of personal data breaches. Furthermore, each state has passed its own data breach notification law. While they are similar in overarching policy, the differences in details form a confusing regulatory regime. If rules do not overlap exactly, organizations must comb through each state's legal code to determine precisely what counts as personal data and what breach notification, if any, is required.

Most states drew inspiration from California's *S.B. 1386*, which was the first of such legislation and the basis for similar laws in other states. However, because California's legislation was rooted in preventing identity theft, it was limited in purview to businesses and identification or financial account data. While its definition of personal data was adequate in the early 2000s when S.B. 1386 was enacted, we see with the OPM and Ashley Madison hacks that serious harm can arise even when breached data is not purely financial.

Studies have shown that notification laws decrease identity theft caused by data breaches by 6.1% (Romanosky et al. 256), yet the messy patchwork of state-by-state legislation poses a significant administrative burden for companies (Peters 1171). Additionally, state data breach laws can, and do, quietly change at any time. As has come to light with Equifax (Oversight of the Equifax Data Breach, 2017), some organizations may choose to remain willfully uninformed and hope their lack of compliance goes undiscovered. According to a vice president at CompTIA, the costs data handlers face provide "no additional protection for consumers" ("What Are the Elements of Sound Data Breach Legislation?" § 530-533) since each state implements different requirements and definitions. Individuals, once notified, can take informed steps to protect their finances and credit. under the current regime, they face an uphill battle if they want to bring a civil suit against the potentially negligent organization (Peters 1175). Therefore, a federal regulatory solution is required that applies notification requirements across all types of personal data and organizations.

A Future Liability and Notification Scheme

Our proposal presents a federal standard for data breaches in the United States. Timely and clear notification to affected persons remains a key element, but we advocate for two enhancements to the current notification scheme: a tiered notification standard and a new requirement for data handlers to provide regulatory authorities with a detailed action plan to follow in the event of a breach. The technical complexities of investigating a data breach necessitate a tiered notification policy that considers the type of data stolen and the scale and cause of the compromise when setting notification manner and timeline.

Each covered entity must submit a *Data Breach Action Plan* to the Federal Trade Commission to follow in the event of a data breach. The document must include the timeline within which notification will be made to consumers, type of data the organization handles, and potential actions for consumers to mitigate harms or seek damages. See Appendix I for a mock-up of a breach notice. Organizations must also have procedures in place to notify individuals whose data has been compromised according to the Action Plan's proposed notification strategy.

We take a slightly different tack than many state notification laws. In addition to requirements about accountability, notification deadlines, formats, and contents, our legislation aims to mitigate the worst effects of breaches before they occur. This is done first by forcing data handlers to regularly review their security and risk management strategies when they prepare and update their Data Breach Action Plans and second, via *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.

Both of these protocols encourage organizations to evaluate their data landscape, assess the risks posed by their current security posture and think realistically about the aftermath of an incident, and take steps to improve their cybersecurity preparedness.

Regulatory Requirements and Authorities

To give these laws teeth, we advocate 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 it to investigate, levy fines, or enter consent decrees with organizations who do not comply. We also provide a framework for civil statutory damages at a *per-breached-record* level and aim to resolve some of the legal uncertainty surrounding standing and jurisdiction for individuals that wish to pursue recourse through the courts.

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.

Therefore, following discovery of a breach, we require covered entities to:

- Immediately notify the regulatory authority. The body will not publicly disclose the event and will, in consultation with relevant agencies, make determinations about whether consumer notification must be delayed for reasons of national security.
- Adhere to their filed breach response plan, keeping the authorities aware of major deviations.

We believe that 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.

Appendix I: Model Data Breach Notification

This appendix contains a model data breach notification form which follows the guidelines in our full paper.

SAMPLE NOTICE OF DATA BREACH

Why am I receiving this document?

This notice is being sent by **Equifax, Inc.** to inform you that a data breach occurred. Equifax holds your personal information in its computer systems which was accessed in an unauthorized manner. The United States government requires that affected individuals receive a notice like this one.

1. Basic information about this incident.

What organizations were affected?

Equifax, Inc.
Equifax Canada

When did the breach occur?

May 2017 - July 2017

How many individuals were affected?

At least 143,000,000

When was this notification sent?

September 7, 2017

2. Why did this happen?

Why did this breach occur?

Equifax believes that criminals exploited a website application vulnerability to access files. Criminals were able to use this vulnerability because the application was not properly maintained.

What data was accessed?

We believe **names, Social Security numbers, birth dates, and addresses** were accessed.

Additional information may also have been accessed in these circumstances:
if you have used Equifax credit dispute services: **your dispute documents**
if you have purchased products from Equifax: **your credit card number**

3. How does this impact me?

What problems could happen because of this data breach?

The release of your **name, Social Security numbers, birth dates, and address** increases your risk of identity theft. The most common identity theft crimes involve opening fraudulent financial accounts in your name.

The release of your **dispute documents** […]

The release of your **credit card number** […]

4. What should I do now?

You are entitled to free identity theft and credit monitoring.

[…]

You are entitled to additional resources from the State of Massachusetts.

As a resident of Massachusetts, […]

You may choose to pursue additional legal recourse.

[…]

5. Who can I contact to find out more?

You can get updates about the status of your personal information.

You contact **Equifax** by visiting […] or calling […] to obtain more information about what happened to your data as Equifax's investigation progresses.

You can read Equifax's response plan for this breach.

[…]

You can find out more about your rights from the Federal Trade Commission, an independent agency of the United States government.

Please visit […], write to […], or call […]

Appendix II: Compliance Information Sheet

Complying with the New Federal Data Breach Policy

Part I: General Compliance

Do I need to comply with this new policy?

Yes if you are:	a **person**, **company**, **government agency**, **nonprofit**, or any **other body**
	that stores and collects **personal data**
	not for purely personal or household activity

If you meet these requirements, you are a **covered entity** under the new policy.

Do I handle personal data?

Yes if:	you have **content data** or **account credential data**
	1. associated with an identified or identifiable **natural person**
	a. who can be **identified, directly or indirectly** by reference to an identifier b. such as a **name, an identification number, location data, an online identifier** or to **one or more factors** specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person
	2. that is not intended to be public information

What do I need to do if I meet the above two criteria?

You will need to file a **data breach action plan** with the Federal Trade Commission. This plan will need to contain:

1. An inventory of the type of data you handle as a covered entity.
2. Your anticipated timeline for disclosing a data breach to consumers or others you hold personal data on.
3. A listing of mitigating actions that breach victims can take upon receiving your data breach disclosure.

Complying with the New Federal Data Breach Policy
Part II: After a Data Breach

Have I suffered a data breach?

Breach	a **covered entity** and
	had accidental, or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to **personal data**
Not a breach	the data was **unintelligible** (i.e., encrypted with an uncompromised key protected from unauthorized access) or
	the data was accessed for issues of national security or emergency law enforcement or
	not a **covered entity**

How do I notify individuals about the breach?

If you have had a security incident which qualifies as a data breach, you have new obligations to notify the individuals whose personal data you hold. This notification will help victims understand breach circumstances and inform them about potential harms resulting from the breach.

1. **Gather information on the breach.** As part of your response to the breach, you will need to gather certain information to disclose to breach victims.
2. **Inform the FTC.** File a report of your breach with the Federal Trade Commission as soon as you are able to.
3. **Create a breach notification.** We have provided a sample notification in Appendix I for you to use as a template. Your notification must include:
    - The type of data accessed or leaked
    - The cause and timing of the incident (if known or able to legally disclose)
    - An explanation of risks or harms most likely experienced from the breach
    - An explanation of recourse available, along with a link to a FTC-administered resource which describes this in more detail
    - An explanation of where the victim can obtain future updates on the status of their data and risks
4. **Send out the notification.** Paper notifications may be sent to the physical address of the individual, if available. Notifications may also be emailed to individuals if it is the only available means of contact. Depending on the scale and severity of the breach, you may also be required to post the notification in a prominent place on your website, or notify individuals through local mass media.
5. **Keep the FTC updated.** File your notification with the FTC and be sure to update your breach report as your internal security investigations continue.

What should a breach notification look like?

Please consult Appendix I.

Bibliography

"Data Security and Breach Notification Legislation: Selected Legal Issues." Congressional Research Service, 2015. https://www.everycrsreport.com/reports/R44326.html#_Toc439087877.

Oversight of the Equifax Data Breach: Answers for Consumers, § Energy and Commerce (2017).

Peters, Rachael M. "So You've Been Notified, Now What: The Problem with Current Data-Breach Notification Laws." *Arizona Law Review* 56 (2014): 1171–1202.

Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti. "Do Data Breach Disclosure Laws Reduce Identity Theft?" *Journal of Policy Analysis and Management* 30, no. 2 (March 9, 2011): 256–86. https://doi.org/10.1002/pam.20567.

What Are the Elements of Sound Data Breach Legislation?, § Committee on Energy and Commerce (2015). http://docs.house.gov/meetings/IF/IF17/20150127/102842/HHRG-114-IF17-Transcript-20150127.pdf.