Policy Paper: Standardized Data Breach Reports

Alejandro Cuevas, Alexander McCollom, John Barczynski, Kelsey Kretzer

The Role of Knowledge & Critical Thinking in Developing Policy(HONOR 301H)

Presidential Leadership Academy

Professor Christian Brady

Professor Melissa Doberstein

12th December, 2015

Table of Contents

Living in a Data Driven World

In today's digitized world, more information on users and businesses is being generated and stored than ever before. One example of how much data has been recently created is the size of Google's internet search archives, which are estimated to be at 95 petabytes (roughly enough space to store 27 billion songs at the average mp3 size of 3.5 megabytes) (FileCatalyst, Matteson). This amount is even more astounding when it is compared to the size of the library of congress, which is estimated to take up, if entirely digitized, only 30 petabytes of space (Lesk). From the years 1989 to 2007, data storage has increased by roughly 23% per year, which is doubling approximately every 40 months, and this exponential growth is projected to increase in rate (Mearian).

While much of this data is not immediately useful to the common computer-user, companies are able to combine personal data with the increasing amount of "big data" available to them to improve the online experience of the users of its services. By tracking the purchasing habits of users, companies are able to predict the products that users will want before they ask for it, allowing for better shopping recommendations. Some companies, such as Amazon, will even stock their warehouses based off of the collected data for users in their areas so as to minimize shipping times. Search engines such as Google are able to use this data-driven approach to offer search results and advertisements that are custom-tailored to the location, language, and interests of the searcher. These kinds of applications seem like a win-win, as consumers are more likely to have a positive online experience and companies are more likely to sell goods to their consumers.

Personal data is also being used more frequently to improve other tasks as well. With the increase in mobile computing technologies such as smartphones and wearables, consumers are

now able to make use of digital wallets, health trackers, and many more, as there are increasing data points for collection, storage, and processing. They are also able to use retailer websites and consumer rewards programs in order to avoid the hassle of going into stores to receive rewards for customer loyalty. The increased usage of electronic medical records promises more holistic health reviews by doctors, less time filing redundant paperwork, and improved protection against the loss of records due to physical damage. These modernizations especially benefit travelers, as they are now able to receive the same personalized care almost anywhere with an internet connection as though they were at their corner market or local physician.

The increased availability and usage of personal data comes at a price, however. As more data is being created and accessed, the risk of unauthorized access, modification, and usage of personal information also increases. This type of unauthorized access to personal information is called a data breach, and can lead to crimes such as fraud and identity theft, which affected 12.7 million US consumers in the year 2014, costing consumers over $16 Billion (Insurance Information Institute). With these risks, there has been an increased need by legislators to protect the personal information of consumers from those who want to misuse it. Change, now more than ever, needs to happen to address this.

The Beginning of the End

The insinuation of change in the digital world began as early as the 1960s when a developing information technology system emerged. Data, whether it was personal or non-personal, was easily accessible by any person of authority. In this sense, privacy rights were re-evaluated and caused a call to action during the following years in Europe. However, it was not until 1970 that an actual law was enacted to help protect a user's right to his or her information. The State Data Protection Act of 1970 in the German federal state of Hessia allowed "public

authorities to process data in a way that ensured it could not be accessed, amended, retrieved, or destroyed by unauthorized personnel (Rauhofer). This act served as a pioneer for the rest of Europe and the world to hold a degree of concern for the information economy and data privacy in general. Therefore, by the 1980s most European countries took initiative to enact change. By avoiding the practice and implementation of 'data havens', uninterrupted and unregulated refuges for data (Stray), privacy was idealized more as a personal right and responsibility.

Post 9/11 Culture

To live in a risk-free society with the emergence of technological change in the digital world became less practical and reasonable. The more that the Internet became an integral part of everyday life, the more that the existence of real privacy among Internet users became at risk. Therefore, when threatened, certain actions were taken to protect the common good of the people. The significance of September 11, 2001 in regards to the presence of terrorism in America has led to increasing complications and opinions on online privacy and security. Government scrutiny became vital for surveillance and safety purposes to prevent terrorist actions. However, with an increased societal level of fear from the psychological impact of terrorism, citizens rationalized the need for government surveillance online in the name of protection and security. However, through the years the actual practice increased questions of individual confidentiality. The urgency to remedy terrorism and ease societal panic resulted in various protocols that would increasingly change how governments and citizens interacted online. In other words, objectify personal online privacy. One of the first insinuations included a "marketing and recruitment database to track students for military recruitment" (Privacy Paradox). The accessibility for militant recruits in obvious, however when individual information on ethnicity, phone numbers, and email addresses are accessed without public notability, a

resultant privacy issue arises. Nonetheless, governmental surveillance was not purposefully manipulative at the expense of democratic values, but eventually did become a concern from a personal privacy perspective.

Corporate Digital Practices

Corporate companies began picking up on this practice of obtaining user data as well as other company data information for business practices and profits. In that sense, data became less of an individual attribute and more of a contributing factor to an information system where "personal data was treated as a commodity and tradable personal asset" (Rauhofer). To understand the integrity of data collection, most companies do have the rights to collect information based on contracts in which their users digitally sign. However, sometimes it is done unethically, which is the main concern of an issue of fairness. With that being said, there is a specific term for this illegal complication called a data breach. A data breach, by definition, is "the unlawful and unauthorized acquisition of personal information compromising the security, confidentiality, and integrity of personal information" (BakerHostetler). Individual rights of privacy should be taken into account with the rise and prominence of data collection and analysis. Although considerably advantageous for individuals, Internet operations since 9/11 has challenged the issue of protecting personal information at the expense of involuntary control in America. It will continue to question the culture of surrendering personal privacy in exchange for online services which are often "free".

New Normalcy

The Internet is an all-encompassing way of life in today's society, so it is inevitable that those who constantly use it adapt to any changes in order to continue using it. However, these

consumers are not aware of the extent to which their personal data is collected, but have nevertheless voluntarily submitted their personal information time after time. Therefore, the extent to which consumers care about where their data is going is dependent on specific generations and their attitudes.

Generation Gap

In general, older participants tend to be more concerned about data privacy compared to the Millennial generation. A study conducted in 2004 showed that 64% of students who use MySpace and or Facebook had neutral attitude results about their privacy settings (Barnes). However, they "didn't seem to realize that Facebook is a public space" where virtually anyone could access their information. Therefore, a strong disagreement was displaced with "everybody should know everything about everyone else" (Barnes). In that sense, the ambiguous concern with privacy is that it is currently difficult to measure who can access or see individuals' specific data. Another study was conducted in 2014 measuring consumers' attitudes towards the same concerns regarding privacy protection. And like the 2004 study, the Millennial generation was the most relaxed sector in terms of attitudes toward data collection (Humphries). However, when educated about the extent to which companies may reuse their content, there was a clear consensus between both older and Millennial respondents that current corporate practices were "completely unacceptable" (Humphries).

Complacency with the Internet

Despite the growing normalcy of carelessly surrendering personal information, the specifics of how that data is used is articulated in the Terms and Conditions contract. But because it is simply easier to release information in exchange for Internet services, taking the time to read through this contract is not something ordinarily done. In fact, lower than "8% of the

population read the Terms and Service contracts", and that means roughly "83% do not know what they are agreeing to" (Humphries). So it is safe to say that there is a "disconnect between the way users say they feel about the privacy settings and how they react once they experience unanticipated consequences from a privacy breach" (Barnes). Consumers are not being effectively educated in the most efficient way to understand what they are agreeing to and where and how their data could potentially be accessed. The lack of control, nonetheless, is either obsolete or ambiguous by consumer usage. Therefore, it is necessary for consumers to not only be aware of where their content is going, but also for them to harness their information and take control of it - lest they learn to surrender it to the exponentially-developing online world.

Unfolding Consequences

But this accessibility is included in virtually anything where personal information is included, such as social media, a financial system, or healthcare. Although some action has been taken to regulate the concerns, they may not be explicit or cohesive across other regions. In terms of healthcare, for instance, electronic patient records can be accessed by not only the beholder, but also insurance companies, physicians, and nurses. And like personal data in general, EPRs act as a kind of commodity. The disadvantages of electronic records include hacking and hostile attacks, but most importantly, data mining. Through these records, either physicians or insurance companies can "profile certain patients based on age, gender, and disease which fall into discrimination and exclusionary effects" (Health Care Info Technology). Therefore, personal data is used in a way to target certain demographics in understanding medical history. This privacy violation is an example of how easily data is traded. Although HIPAA (Health Insurance Portability and Accountability Act) is established, the need for "cohesive policies against varying state codes" must be enacted not just in the healthcare industry, but on a national scale.

The Crux of the Problem

Through a new normalcy and culture that Internet users have adapted to, regulatory concerns arise with their involvement. It is becoming less common for people to live a private life online because of the culture they live in through social media, but also through the increasing ease of accessibility governments and companies have over their data. A myriad of knowledge is spread throughout various generations, but in general there is no doubt that consumers feel like they are constantly being watched and monitored. This Internet practice is a physical metaphor of a panopticon where "consumers are less likely to break rules as they believed they were being watched even though they were not" (Rauhofer). It is impossible to accept the fact that privacy is an utopian ideal in the Internet society because it would not reflect American democratic values and intentions. Therefore, there is a need, at the very least, for citizens to know about where their data is going and how it is being treated. More importantly, the decisions they make from here on out should not be measured by risk, but by the ease with which they can harness their data, bringing it back under their own control. In order to achieve this, an appropriate and comprehensive legal framework needs to exist.

Current Legislation

While there currently exists no national standard for data security, some laws are already in place for the protection of privacies in relation to data security. In many businesses and government entities, there already exists a standard for data privacy that varies from organization to organization. This "sectorial approach" to the privacy of personal information has seen the enactment of laws affecting the public sector as well as a few laws touching private corporations including HIPAA and the Gramm-Leach-Bliley Act discussed later. What is lacking between

these bills, however, is a standard for what constitutes a data breach, how and when consumers need to be notified, and what types of actions need to be taken when a breach occurs.

Government Data Security Initiatives

All federal government agencies are affected by the Federal Information Security Management Act (FISMA). Under FISMA, program officials and the head of each agency must conduct annual reviews of information security programs so as to minimize risk of major data breach. In 2007, the Office of Management and Budget issued the recommendation for federal agencies to implement breach notification policies that would handle both digital and paper data losses and would define the procedures that must be taken when a breach occurs. Additionally, the US Department of Veterans affairs has its own security breach notification law, requiring them to provide notification in the occurrence of a data breach.

HIPAA and HITECH

Data that is used in relation to the healthcare field can already be protected under the Health Insurance Portability and Accountability Act. This act requires "the development of a health information system through the establishment of standards and requirements for the electronic transmission of health information." This act broadly covers the field of healthcare and requires entities to meet a national standard by which health-related data is stored, secured, and transmitted (The Health Insurance Portability and Accountability Act of 1996). Under HIPAA, there are very large monetary penalties for organizations that fail to comply with the national standards and regulations and makes it criminal for any person to knowingly and in violation of HIPAA disclose identifiable health information.

The HIPAA Privacy Rule was later enacted, regulating the transmission of "protected health information" that is "individually identifiable" in all forms of communication (Stevens).

The HIPAA Privacy Rule limits the situations in which a patient's protected information may be disclosed or used without patient authorization. These situations were limited to health care operations, treatment, and payment. Additionally, exceptions were made for certain exceptions pertaining to public health, judicial, or law enforcement purposes.

The HIPAA Security Rule specifically targeted the electronic storage and usage of health information. The HIPAA Security Rule requires companies to take steps to protect their system within reasonable measures from threats to the security of the personal information that they store.

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) added a few provisions and requirements to the HIPAA privacy and security rules. It puts business associates of HIPAA-related entities who misuse data subject to criminal and civil liability and additionally limits the use of identifiable information for personal health information for fundraising and marketing. Additionally, HITECH requires covered entities to notify the public and Health and Human Services in the event of data breaches. It also provided a definition for "Unsecured Protected Health Information": "if Personal Health Information is rendered unusable, unreadable, or indecipherable to unauthorized individuals … then such information is not 'unsecured'" (Johnson).

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act requires financial institutions to notify customers as to their privacy policies and to create safeguards for the personal information of the consumers. A financial institution is considered any business that is engaged in "financial activities" as described by the Bank Holding Company Act of 1956. The institutions are prevented from disclosing "nonpublic personal information" to third parties without some notification to the

consumer and some opportunity for the consumer to opt out. (Stevens) The GLBA also requires banking agencies to establish standards to provide safeguards to protect consumer data, including the recommendation of disclosure about a potential breach when "misuse of information about a consumer has occurred or is reasonably possible".

General Consumer Protection Standards

The Federal Trade Commission Act (FTC Act) gives the FTC the ability to pursue companies when they fail to follow through on promises of keeping personal information private ("About the Federal Trade Commission Act"). One notable example of this is from 2011 when the FTC charged Facebook with failing to keep privacy promises that it made to its users. This complaint was based upon Facebook arbitrarily turning data that it had initially kept as private into public data without the consent or notification to the users. This includes making the certain information including the Friend List of users public without consent, giving apps that used Facebook's system nearly all user data instead of the claimed "info needed to operate", making information of users available to the applications that their friends used, sharing personal information with advertisers when it said it would not, and not deleting certain media files associated with accounts upon account deletion, among others ("Facebook Settles"). Under the settlement, Facebook was required to ask for "affirmative express consent" before sharing user information and was prohibited from using misrepresenting their security settings.

The Payment Card Industry Data Security Standards provides a framework for the development of a security process surrounding card data. This includes prevention, detection, and reaction to security incidents (Stevens).

Legislation on the State Level

Currently, there's no consistency or standard in legislation across the United States regarding data breach notification. Each state has variances in definitions or criteria to be met. There's no consensus/standard between states in the following areas:

- Data protected
- Consumers protected
- Definition of a breach
- Covered entities
- Notice procedures
- Existence of a centralized data loss (DL) reporting entity
- Timing
- Exemptions
    - Safe Harbors
- Penalties
- Private Cause of Action

Current Definitions

As we have mentioned above, the wording and even the definitions and/or requirements vary. However, the following definitions are the most recurrent among the current state laws, according to BakerHostetler and MintzLevin.

Personal Information (PI): An individual's first name or first initial and last name plus one or more of the following data elements: (i) Social Security number, (ii) driver's license number or state- issued ID card number, (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an

account and generally applies to computerized data that includes personal information. Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media. In addition, Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Redacted: defined as altering or truncating data "such that no more than the last four digits of a social security number, driver license number, non-operating identification license number financial account number or credit or debit card number is accessible as part of the personal information

Encrypted: is defined as (1) the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key; or (2) securing data through another method that renders the personal information unreadable. AES is the first publicly accessible and open cipher approved by the National Security Agency (NSA) for top secret information (when the 192 or 256 bit key lengths are used).

Breach of Security: The unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of personal information.

Notice: Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay. Notification may be delayed if a law enforcement agency determines that notification will impede a criminal investigation. Any required notification must be made promptly after the law enforcement agency determines that it will not compromise the investigation. Substitute notice by means

prescribed in the statute allowed in the case of very large breaches. Five-day notice requirement (to state agency) in event of breach of medical/health information.

Covered Entities: Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities. Any person who maintains or otherwise possesses personal information on behalf of another person. The definition of "person" includes governmental subdivisions, agencies, or instrumentalities

Centralized Data Loss Reporting Entity: A government agency to which covered entities must report to when a breach of security has occurred. Said agency will be in charge of logging this activity.

Private Cause of Action: Private cause of action theories are divergent, but in general, a "private cause of action" can be defined as a private person's right
to invoke a federal enforcement statute against another private person in a civil suit. The suit has its jurisdictional base in the regulatory command of a particular federal command and control statute.

Examples – How States Differ (In-depth)

Delaware - H.B. 116 - Del. C., Tit. 6, Chapter 12B, §§ 101-104

- **Data and Consumers Protected:** Personal information of Delaware residents.
- **Security Breach:** An unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of PI.

- **Covered Entities:** An individual or a commercial entity that conducts business in Delaware and owns or licenses computerized data that includes personal information.
- **Notice Procedures:** Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless disclosure impedes law enforcement investigation. Substitute notice by means prescribed in the statute allowed in the case of large breaches.
    - Notice not required if the entity responsible for the data concludes that the breach will not likely result in harms to consumers.
- **Safe Harbor:** Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted.
- **Preemption:** Entities regulated by any state or federal law that provides greater protection to personal information are exempt.
    - Exemption for good-faith acquisition by an employee or agent, so long as PI not used or subject to further willful unauthorized disclosure.
- **Penalties:** Appropriate penalties and damages may be assessed in an enforcement action brought by the Attorney General.
- **Private Cause of Action:** Yes. Plaintiff may recover treble damages and reasonable attorney fees.
- **Definitions:** "Personal information" means a Delaware resident's first name or first initial and last name in combination with any 1 or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted:
    - a. Social Security number;
    - b. Driver's license number or Delaware Identification Card number; or

- c. Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.

The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Kansas - S.B. 196 - K.S.A. 50-7a01 et seq.

- **Data and Consumers Protected:** Personal information of Kansas residents, including account number or credit card/debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account.
- **Security Breach:** Any unauthorized access to and acquisition of unencrypted or redacted computerized data that compromises the security, confidentiality, or integrity of PI and that causes, or entity reasonably believes has caused or will cause, identity theft to any consumer.
- **Covered Entities:** A person that conducts business in Kansas, or a government, governmental subdivision or agency that owns or licenses computerized data that includes personal information.
- **Notice Procedures:** Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless disclosure impedes a criminal investigation.

Substitute notice by means prescribed in the statute allowed in the case of large breaches. An entity that must notify more than 1,000 consumers at one time of a security breach is required to also promptly notify all consumer reporting agencies of the breach.

  - Notification not required if after a good-faith, reasonable and prompt investigation the entity determines that the PI has not been and will not be misused.

- **Safe Harbor:** Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted or redacted.
- **Preemption:** Entities regulated by state or federal law that maintain procedures for addressing security breaches pursuant to those laws are exempt.
- **Penalties:** Appropriate penalties and damages may be assessed in an enforcement action brought by the Attorney General.
- **Private Cause of Action:** No.

Following is an expanded table to highlight the definitions in a wider scope, highlighting the existence of centralized data reporting agencies.

Analysis of State Legislation Comparing Data Loss Reporting Capabilities

Table 1: States With Data Breach Report Law and Centralized Data Loss Reporting (MintzLevin)

State	Centralized DL Reporting	Data Loss Law	Encryption Safe Harbor	Private Cause of Action
Hawaii S.B. 2290	Yes	Yes	Encrypted	No
Maine L.D. 1671	Yes	Yes	Encrypted (Defined)	No

Maryland S.B. 486	Yes	Yes	Encrypted (Defined)	Yes
Massachusetts Mass. Gen. Laws § 93H-1 et seq.	Yes	Yes	Encrypted (Unless key has been compromised)	Potentially
Missouri Mo. Rev. State § 407.1500	Yes	Yes	Encrypted	No
New Hampshire H.B. 1660	Yes	Yes	Encrypted (Unless key has been compromised)	Potentially
New Jersey N.J. Stat. 56:8-163	Yes	Yes	Encrypted	No
New York N.Y. Gen. Bus. Law § 899-aa	Yes	Yes	Encrypted (Unless key has been compromised)	No (Attorney General only)
New York City N.Y. City Admin. Code §20-117	Yes	Yes	No	No
North Carolina S.B. 1048	Yes	Yes	Encrypted	Potentially
Vermont S.B. 284	Yes	Yes	Secured	No (Attorney General only)
Virginia S.B. 307.2	Yes	Yes	Encrypted or Redacted (Defined)	Yes

Table 2: States with Data Loss Law but No Centralized Reporting

State	**Centralized DL Reporting**	**Data Loss Law**	**Encryption Safe Harbor**	**Private Cause of Action**
Alaska H.B. 65	No	Yes	Encrypted or Redacted	Yes (Excluding Government)
Arizona S.B. 1338	No	Yes	Encrypted or Redacted (Defined)	No (Attorney General Only)
Arkansas S.B. 1167	No	Yes	Encrypted	No
California S.B. 1386	No	Yes	Encrypted	Yes
Colorado H.B.1119	No	Yes	Encrypted, Redacted, or Secured	No (Attorney General Only)
Connecticut Conn. Gen Stat. 36a-701(b)	No	Yes	Encrypted or Secured	No (Attorney General Only)
Delaware H.B. 116	No	Yes	Encrypted	Yes
District of Columbia	No	Yes	-	Yes
Florida S.B. 1524	No	Yes	Encrypted or Secured	No
Georgia S.B. 230	No	Yes	Encrypted	No
Idaho H.B. 566	No	Yes	Encrypted	No
Illinois H.B. 1633	No	Yes	Encrypted	No
Indiana S.B. 503	No	Yes	Encrypted	No
Iowa H.B. 1101	No	Yes	Encrypted or Redacted (Def.)	No

Kansas S.B. 196	No	Yes	Encrypted or Redacted (Defined)	No
Kentucky H.B. 232	No	No	Yes	No
Louisiana S.B. 205	No	Yes	Encrypted or Redacted	Yes
Michigan S.B. 309	No	Yes	Encrypted	Yes
Minnesota H.F. 225, 2121	No	Yes	Encrypted	Yes
Mississippi H.B. 585 Req. Sess. (MI 2010)	No	Yes	Encrypted (Unless key has been compromised)	No
Montana H. B. 732	No	Yes	Encrypted	No
Nebraska Neb. Rev. Stat. §§ 87-801--807	No	Yes	Encrypted or Redacted (Defined)	No
Nevada A.B. 334	No	Yes	Encrypted	No
North Dakota S.B. 2251	No	Yes	Encrypted or Secured	No (Attorney General Only)
Ohio H.B. 104	No	Yes	Encrypted or Redacted (Defined)	No (Attorney General Only)
Oklahoma H.B. 2357	No	Yes	Encrypted or Redacted (Defined)	No (Attorney General Only)
Oregon Oregon Rev. Stat. § 646A.600 et seq.	No	Yes	Encrypted (Unless key has been compromised)	No (Compensation can be Ordered)
Pennsylvania	No	Yes	Encrypted or	No (Attorney

S.B. 712			Redacted (Defined)	General Only)
Rhode Island H. 6191	No	Yes	Encrypted	Yes
Tennessee S.B. 2220	No	Yes	Encrypted	Yes
Texas S.B. 122	No	Yes	Encrypted (Unless key has been compromised)	No (Attorney General Only)
Utah S.B. 69	No	Yes	Encrypted or Secured	No (Attorney General Only)
Washington S.B. 6043	No	Yes	Encrypted	Yes
West Virginia S.B. 340	No	Yes	Encrypted or Redacted (Defined)	No
Wisconsin S.B. 164	No	Yes	Encrypted, Redacted, or Secured	---
Wyoming H.B. 208	No	Yes	None	Potentially

States with No Data Breach Report Legislation

- Alabama
- New Mexico
- South Dakota

Expanded definitions for Table 1 and 2:

Centralized DL Reporting: The existence of a government entity to which other entities can report breaches.

Data Loss Law: The existence of a set of rules that govern data breaches and their respective reports.

Encryption Safe Harbor:

- Encrypted: States are exempt from reporting data breaches if the data is encrypted. *
- Redacted: States are exempt from reporting data breaches if the data is redacted. *
- Secured: States are exempt from reporting data breaches if the data is secured or rendered unusable or unreadable through any method or technology.
- Some states have specified that in the case that the key that was used to encrypt the data is compromised, the entity is required to report the breach.
- Some states have defined the terms “encrypted” or “redacted”.
- Private Cause of Action: Allows private parties to bring a lawsuit.

(*): The term “encrypted data” is defined mainly as data that can’t be read or used. However, the laws do not specify particular encryption technologies to be used by companies (i.e. AES-256bit, 512bit, 2048bit, etc.).

Prior Attempts at National Law and Implementation Problems

There have been many previous attempts at national data breach notification standards. One problem that was initially faced when trying to enact national law was the concept of preemption, or the invalidation of a state law that conflicts with a national law. Some of these

standards received staunch opposition because they were actually weaker than the laws already enacted in many states. In the worst case, this could leave some citizens worse off than they had been under their state legislations, and in the best case it would leave a patchwork of state laws whose extra restrictions would still need to be followed by the companies that operated in those states.

The debate about whether a national law for data breach notification should preempt state laws or whether it should create a national minimum for state laws caused a number of previous notification bills to be left in subcommittees of congress. This type of debate occurred in 2013 when six witnesses testified at the US House of Representatives to weigh in on either side of the issue (Gross). That act, like many others before it, died in congress. In order to try to avoid these concerns, it will be necessary to craft a law that gives the most comprehensive protection feasibly available.

Additionally, there were many arguments over definitions and specific terms. One example of this is the Data Breach Notification Act of 2009, which sought to require "business or Government entity that experiences a data breach promptly notify any consumer whose sensitive personally identifiable information has been exposed", which was one of the many data breach notification acts proposed by Senator Dianne Feinstein from California (Data Breach Notification Act of 2009).

Detractors of this bill cited that the Data Breach Notification Act was too broad in terms of the scope of protected personal information, as some of the information protected by the act (name, address, etc.) was already under public record, and of security breach (when unauthorized "access" is taken, but not the acquisition of any data. Additionally, the detractors cited that the standard for "harm" is too vague in order to be useful. Finally, the bill did not make clear the

timing in which entities that experienced a security breach must act and how they must communicate the breach. The bill specifically said “without reasonable delay”, and it forced a widespread announcement about the breach (“Senate Report”).

Senator Feinstein modified the previous bill when she re-submitted another proposal in the form of the Data Breach Notification Act of 2011. This bill included stringent definitions for the terms “public records” and “security breaches”. Except in national security incidents, all breaches would have needed to be reported by 45 days afterwards. The bill made exceptions to the data that was heavily encrypted and to data that has been rendered unusable. This bill, like those that came before it, died in congress (Data Breach Notification Act of 2011).

From examining previous legislative failures, we have determined that it is necessary for at national notification law to be at least as strong as the state laws that are already in place and to provide strict definitions of all relevant technical terminology.

Effects of Data Breach Notification Laws

By using econometric approaches, it was determined that adoption of Data Breach Notification Laws in some states was able to reduce cases of identity theft due to data breaches by 6.1 % (Romanosky, Telang, Acquisti). This is because users, when equipped with greater knowledge of what was happening to their data, were able protect themselves more quickly and prevent potential cases of fraud and identity theft. The adoption of Data Breach Notification Laws also prompted an immediate increase in security by companies due to a rise in concern over a potential breach.

It was found that the number of identity theft cases due to data breaches decreased most over the first year after the enactment of data breach notification laws, most likely due to heightened awareness of the issue, but it was found that this effect was lessened slightly over

time. This is because some consumers became desensitized to the warnings that they had been receiving and once again followed less secure data practices. Additionally, it seemed as though managers, after making initial security upgrades in compliance with the data security laws, also became complacent with their security standards. That being said, it has been found that information security was generally improved after some form of data breach notification law was enacted (Romanosky, Telang, Acquisti).

The passage of a national standard for data breach notification and protection would allow this process to become more transparent and streamlined while still affording individuals the protections that they need. The passage of a national law would make it easier for consumers to understand their rights in the event of a breach, which will allow individuals to become better stewards of their own data. Additionally, it is believed that a national standard for data breach notification will make it easier for businesses to comply with the bill. In the current situation, companies are forced to send teams of lawyers to handle the nearly fifty different state notification laws required, which is costly and difficult, especially for smaller businesses. Because it would be easier for companies to be in compliance with the national standards, companies would be free to put their efforts toward strengthening their networks and minimizing the threat of future attacks.

Our Solution - and Why it Matters

We see a bill being passed by Congress as the most effective means of creating long-lasting reform on this issue. If crafted intelligently and carefully, it will be able to balance the right individuals have to their data's privacy with the need of companies to operate in a cost effective manner, as mentioned earlier.

As with any bill, it needs to stem from a solid foundation. For our purposes, we chose the seven principles that were central to the European Directive on Data Privacy, officially known as Directive 95/46/ec of the European Parliament and the Council. Approved in 1995 and brought into effect three years later, this is one of the strongest and longest standing laws on data protection in the world today, especially when one takes into account the fact that the European Union covers a population double that of the United States. These principles, officially, are known as Notice, Choice, Onward Transfer, Security, Data Integrity, Access, and Enforcement. Combined, they work together to ensure that businesses and other corporations don't infringe on the right of the individual to the privacy of their data and personal information. This right is explicitly stated in the Directive itself, and not just once but at multiple points throughout the document as the raison d'etre for this law's existence. Since the same logic lies behind our own desire for greater awareness among the general public as to how companies handle and protect the data of their customers, it seemed prudent to include these principles within the introductory text of our bill.

Before the main title begins, there is a section that details the arguments already made in this paper as to why this proposed bill is necessary, but in a more concise format. It logically argues that since personal data is becoming a prime target for hackers, and hacking/data breaches disrupt the economy and society disproportionately compared to the number of individuals needed to carry out the act itself, it allows for the operations of businesses and governments to be tripped up and the privacy rights of American citizens to be trespassed. Because of this possibility, businesses must be responsible stewards of the data they collect from their customers, and in order to do that, must therefore also provide prompt notification - within

reason - of all breaches of personal customer data that occurs so as to minimize the inherent risks to the consumer associated with such an occurrence.

Title I: National Data Breach Notification Standard - Section 101

The main Title of the bill is straightforward in name. To begin with, the first section of this title deals with the core of the law. One of the key components of this bill that is introduced here is to whom this law generally applies. Any business that uses, collects, stores, transmits, accesses, disposes of, or otherwise interacts with personal data in the course of carrying out interstate commerce within the 12 months immediately preceding the date on which the data breach is discovered falls under the purview of this bill, so long as it was the data of more than 1,000 different individuals. Under the House Bill (H.R. 1704), this threshold had previously been set at 5,000. However, moving the threshold lower allows for more companies to be held accountable, while still protecting boutique small businesses that aren't handling enough data to be significant at a federal level. Plus, most companies that are targets for electronic data breaches (as opposed to just breaking in and stealing cash out of the register or more conventional forms of criminal activity) are operating well above either threshold, so it realistically serves to cover smaller businesses with sensitive information as a part of their business, such as community hospitals and private investments firms. Smaller firms are much less likely to be targets of data breaches on a large scale than major retailers, hospitals, and financial institutions. For the sake of legality, this bill refers to the data of users as "sensitive personally identifiable information that the business entity does not own or license." This slightly broader definition is a more conventional legal way of phrasing to achieve the end goal of requiring companies to notify their customers when they've detected that their data has been breached. This definition also allows for a third party to do the notifying for the business entity, which mainly applies when a business

contracts out its IT services to another firm, uses a web service to host their website, or otherwise interacts with another business entity who is the direct target of the data breach in which their company's clients' data were involved. Furthermore, it makes sure that any service provider or "middle man" in the transport and relaying of data who detects a data breach notifies the company whose data was intercepted or breached. This is all in an effort to cover all of the bases with regards to ensuring that the overall goal of the bill is brought to fruition.

The next subsection deals with the timeliness of the notification. It states that as of now, the full process of notifying all individuals affected must be carried out "without unreasonable delay", which in this bill is defined as within 60 days of the company being made aware of or otherwise discovering the breach in question. The main exception to this rule is if the Federal Trade Commission finds that more time is needed for reasons such as figuring out what exactly happened or otherwise delaying the announcement of a data breach in order to better prevent such a breach from occurring again, after the breach in question was announced to the public. Under the current draft of the bill, notification system is also established as two-tiered. This means that within 72 hours of notifying the breach notification entity in the Federal Government (as required in subsection 106(d) of the bill), the company has to put out a generic news blast saying that they were breached and are working to determine exactly what was put at risk. The full, more often personal, notification of what data was actually put at risk is then released to the general public and/or those people who were specifically affected before the 60-day window to do so closes. In discussion with Mr. Leiserson, a legislative aide to Rep. Langevin (D-RI) who wrote the bulk of H.R. 1704 for the congressman, he felt that this two-tiered approach, which was a modification of his own bill, would pose a risk of having too many companies be required to falsely report a data breach, only to later determine that no such breach occurred, or that it was

minor enough that it didn't have to be reported, and thus suffer bad press as a result. As this bill is worked towards implementation across the country, this is one concept that, while good in theory, may need to be modified, or other parts of the bill strengthened to better support it, in order for the clause in question to be effective.

This notification can be delayed for a number of reasons, which are also detailed in section 101 of the bill, and later elaborated upon in later sections of Title I as needed. With the exception of ongoing criminal or national defense issues or investigations, all delays to when a company must notify users that their data has been breached must be approved by the FTC, and each extension can be no longer than 30 days in length. For matters of national security or legal proceedings, the FBI, Secret Service, Secretary of Homeland Security, or U.S. Attorney General can also intervene and extend the period until which the public must be notified by 30 day increments at a time, and this may continue indefinitely as long as it is reaffirmed that such a disclosure of information about a data breach would be more dangerous to national security than the threats caused by a lack of notification. Currently, the FBI and Secret Service would have the greatest individual power in this process. The Secretary of Homeland Security and the U.S. Attorney General would act as overseers who process and approve a request by any other national security or law enforcement agency to delay the notification report of a data breach. At present, the roles of DHS and the U.S. Attorney General were questioned by Mr. Leiserson due to the way that these responsibilities are currently handled at the federal level, with the FBI overseeing most prosecution cases. However, this doesn't mean that change can't occur. Until more opinions are gathered - besides the author of H.R. 1704 - on this point, the current division of reporting between federal agencies will be the most efficient over the long term, if slightly more involved at the onset due to the minor bureaucratic restructuring that would need to occur

should this bill be passed into law. In addition, this section includes an additional statement that, as it relates to 28 U.S. Code 1346(b) in terms of jurisdiction, protects these Federal agencies from being sued by corporations or individuals for preventing them from being notified of a data breach in a "timely manner" as a result doing their job to protect national security or execute the laws of the nation in the nation's courts.

The last two subsections of section 101 explain how reports of data breaches will be tracked by the federal government and how pre-existing laws will be permitted as substitutes for this act. The former warrants almost no further explanation as it simply states that within 60 days of the bill being passed, the Secretary of Homeland Security shall designate or choose which government agency shall be the official recipient of data breach notification reports filed with the government (pursuant to subsection 106(b) of the bill), and shall help keep the Federal Trade Commission informed on issues pertaining to the implementation and enforcement of the bill. Under the subsection that deals with laws that can be substituted for the one we've crafted, we initially looked at a set of several laws currently in existence that regulate specific industries. Healthcare and financial services were the primary industries for which data-based laws already exist, with HIPAA and the Gramm-Leach-Bliley Act respectively. These were based off of limitations that had been listed within Senator Patrick Leahy's (D-VT) S. 1158 bill. However, after a conversation with Mr. Leiserson, we determined that the Gramm-Leach-Bliley exclusion should not make it into the final bill due to the relaxed nature of the requirements outlined within the Act. In essence, the language of Gramm-Leach-Bliley permits banks too much leeway to determine how much is reasonable when it comes to protecting data and notifying the "owners or licensees" of the data that a breach occurred. On the other hand, HIPAA and the HITECH laws passed in recent years have much more specific standards on data protection in place, and are

thus more likely to effectively lead the companies to which these laws apply towards achieving the same goals of our own bill, without officially being under the legal authority of it directly. These limitations also tie back to the notion of saving companies legal fees. While our proposed legislation needs to be strong enough that it can preempt the various state laws that are currently in existence in order to simplify compliance across state borders, it also is critical that companies are able to reduce their legal expenses as a result of this bill, and these exclusions for companies complying with certain other laws helps to achieve that goal.

Title I: Sections 102 - Exceptions

The other sections under Title I all serve to clarify, expound upon, and explain that which was initially laid out in section 101. Section 102 clarifies and explains in greater detail how extensions and delays to the notification process outlined in section 101 can be brought about, detailing the steps to be followed by both the business entities and the federal agencies involved with any particular case relating to this bill. One key change we made from H.R. 1704's version of section 102 is in 102(b)(1)(C). Originally, this subparagraph stated that if the Federal Trade Commission didn't provide an explicit written request that a company notify the public of a breach within 10 days of the company submitting the request, that the business entity would no longer be obligated under the law to notify the consumers affected by the data breach. This essentially created a pocket veto situation where the FTC could avoid ruling on a case while letting it slip through the cracks and not notify anyone through this effective loophole, had the House bill ever been put into law. Instead, the new language requires a positive affirmation from the FTC in order for a company to be permitted to not notify, whereas a lack of response from the FTC results in the company still being expected to release a data breach notification report as outlined under Title I of that bill.

In the paragraph immediately following the one referenced above, the bill talks about "rebuttable presumptions", or cases in which a company might rebut a charge in a court of law that they failed to comply with this bill, with specific instructions for business entities on how they might prove their innocence in a court of law. To strengthen this section of the bill, we assigned specific agencies to set the security standards which would be regularly updated to keep companies abreast of recent technological changes. The National Institute for Science and Technology, in collaboration with the National Security Agency in terms of encryption, has the best chance of mediating the capabilities and technologies companies need to keep their data safe with finding reasonable methods of implementing it. NIST has already partially achieved this with their Cybersecurity Framework (National Institute for Standards and Technology, "Overview"), which provides a solid foundational baseline off of which these new standards mandated to be set by NIST can be formed. Their involvement in the process will also help to mediate any tendencies the NSA might have to recommend prohibitively cost-heavy security solutions due to their role in protecting the data of the federal government and the associated selection biases that go along with that.

The final subsection of section 102 waives the notification requirement for business entities if the data breach involved only one piece of information per user that would normally permit the hacker(s) to carry out financial transactions, either through that company's interface (Amazon) or in the greater online market (PayPal or Venmo). The notification requirement is only waived if the company is able to definitively stop the use of the breached data to execute any future financial transactions, and it must also notify the affected individuals and provide them with free credit monitoring for a year following the date of the incident in question. Again, exemption only occurs if only one piece of user data was collected per user from a company,

through one means or another, and the second another piece of data was gathered on each user in the course of a data breach, this exemption disappears.

Title I: Sections 103 & 104 – Notifications

Section 103 discusses at length the different method through which a company might stay in contact with their customers and users in order to notify them of a data breach. This section was modified from the original version as found in H.R. 1704 in order to better reflect the technological realities of the modern era. One way this was done was through detailing the exact type of email notification that would be permitted as an alternative for written or phone notification of a breach, which often lags weeks to months behind the actual news about an issue. Furthermore, this section now also details how a website can be implemented alongside other means of mass media when issuing a "mass notification" at any given time as a part of compliance with this bill.

Section 104 is intricately connected to section 103, as it deals with the content of the notifications that are sent out through the means described in section 103. Again similar to the preceding section, this one saw few alterations from its original House draft version, but they are significant changes nonetheless. First of all, the wording in paragraph 104(a)(6) was expanded. In this way, it could be clarified that, while legally a state law that was stronger than this bill would still have to be complied with by a business entity, the same business entity could delay compliance with that portion of their notifications almost indefinitely - with FTC approval - so long as they complied with all standards required under the national notification act that this bill would become. Furthermore, an additional subsection was added to create an exemption to paragraph 104(a)(2) regarding the provision of a toll-free number for people to call. Toll-free numbers inevitably cost a company money, and also people to man the phones, no matter how

many automated menus are incorporated into the number's answering programming. With this exemption, companies may choose to instead provide all of the same information through a web portal, most likely just an extension of their own existing company website. Naturally, a prerequisite of using this option is that the website in question be entirely secure and safe from being further compromised in a hack or other type of data breach similar to what was experienced by the business entity to cause the need for a reporting and notification website in the first place. This standard of security is determined based on the National Institute of Standards and Technology's expanded Cybersecurity Framework, created in consultation with the National Security Administration with regards to encryption issues.

Title I: Sections 105 & 106: Credit Monitoring and Federal Hierarchies

Section 105 defines and declares the point at which the major credit-rating notification agencies are notified that there was a breach. Originally, this section set a minimum requirement of 5,000 individuals affected and a reasonable delay of 30 days between the discovery and reporting on a security breach to the impacted parties. As seen at various spots, this definition of "reasonable delay" has been 60 days consistently throughout the draft bill. When we spoke with Mr. David Dulabon, Penn State's General Counsel, in early December of 2015, one of the few things he definitively suggested we alter was the amount of time that constituted a "reasonable delay", seeing 45-60 days as much more likely to be welcomed by businesses than the 30 day timetable that would've existed had Langevin's House bill gone unaltered. When pressed, Mr. Leiserson admitted that "30 days was the shortest amount of time that we could get that left corporations the least upset with us and saying, for the most part, that they would be able to comply within that timeframe." However, while that initial reasonable delay is still the 60 days

figure, all extensions pushing back the notification required release date must still be issued every hour in order to be the most effective.

Section 106 lays out a plan for federal employees as to how and when the different government agencies would all get notified each time there's a data breach that falls under the purview of this bill's authority. It once again divides itself between law enforcement and national security. Law enforcement includes the U.S. Secret Service, the FBI, the U.S. Attorney General, and the Federal Trade Commission as appropriate. On the national security side, the only named entity is the Department of Homeland Security, which is notified only in the event that more than 5,000 individuals are impacted, a database which includes sensitive personally identifiable information on over 500,000 individuals nationwide may have been put at risk, or it somehow relates to a federal agency or federal employees. While left unchanged from H.R. 1704, it should be noted that under this section, business entities have a maximum of 10 days in which to comply with the federal agency notification requirements outlined in this section, which is a much shorter timetable than is given for notifying any of the other parties as required under this bill for the business entity that had a data breach occur to them.

Title I: Sections 107 & 108 - The Long Arm of the Law

Sections 107 and 108 are fairly similar in that they both look at how government bodies and agencies can enforce the regulations outlined within the bill itself. In essence, the U.S. Attorney General and the Federal Trade Commission hold the sole power to bring civil lawsuits against business entities that violate the regulations of this proposed legislation. In both cases, any financial penalties assessed against a business entity that failed to comply may not exceed, "the product of the number of violations of this title and $16,500". It should be noted that, in order for the Federal government to actually act against a company, at least 1,000 or more people

would have had to have never received a notification, putting the financial penalty upwards of $16,500,000 instantaneously, despite a fine per violation that's less than $20,000. This is because it counts "each failure to provide notification to an individual as required...as a separate violation." (H.R. 2017). The only reprieve that exists, which is mainly designed to protect smaller businesses, is that so long as they can prove that there was no "willful or intentional" violation of the law, most likely due to an inability to detect that a certain individual or group of individuals' data had been compromised in the data breach, only for that person or group of people to later make such a realization on their own and bring suit against the company through the FTC or the U.S. Attorney General. Likewise, Section 108 stipulates that the Attorney Generals of each State within the United States may bring suit against a business entity if they believe that the regulations of the proposed law were violated, thus serving a *parens patriae* lawsuit, where the state's Attorney General is suing the business entity in order to protect and otherwise sue on behalf of their state's citizenry, akin to a class-action lawsuit in some small sense (West's Encyclopedia of American Law). While harder to bring a suit en parens patriae as a state Attorney General than it is for the FTC or U.S. Attorney General to bring a lawsuit against a business entity, it can nevertheless be done provided they comply with the regulations outlined within section 108. Possibly the most important of the limitations placed on the state Attorney Generals are that the U.S. Attorney General and the Federal Trade Commission can bring their own suit against the same entity if they see multiple state Attorney Generals bringing suit against the same business entity, in which case they are then also able to consolidate all of the disparate lawsuits into one legal action against the business entity, saving the federal court system time and money. Furthermore, the FTC and the U.S. Attorney General initiating a legal action against a business entity prevents any state Attorney General from bringing the same legal

action against that business entity, saving the companies more time and money in the event that they are brought to court, leaving more money available to pay the fine, should they be found guilty.

Title I: Sections 109, 110, & 111: Supremacy, Reporting, and Definitions

Section 109 simply states that, with the intentionally rare exception of a state law that is stronger than the federal law, that this national bill will supercede all existing legislation on the books of any state, so far as it can be applied to the regulation of interstate commerce as outlined in the Constitution. Going off of that, Section 110 lists the different committees within the Legislative Branch that the parties involved in enforcing this bill must report to, what they must report, and how often it shall be reported to those committees. The section on Financial Fraud Protection Exemption reporting, 110(c), was added in its entirety by our group, as it was considered to be an oversight by us on the part of Rep. Langevin's team to omit such reports when portions of their bill, and this one, deal with the financial industry specifically. Additionally, Mr. Leiserson agreed with us that this was one of the better additions we had made to his draft bill (H.R. 1704). Coming from the author of the House bill that was dramatically altered to fit with both the Senate bill's language and our own research, that can be taken as a sign that this was a good addition to the bill, for sure.

In section 111, all of the various terms used throughout the paper are clarified, explained, and officially defined in terms of how they are used within the bill's language itself. While formed the same way as the rest of the bill, there were some critical alterations done to the definitions of encryption, security breaches and sensitive personally identifiable information. The definition of encryption was expanded to say that the initial standard of encryption will be established by the Director of the National Security Agency, who approves of as wide an array as

possible of encryption technologies and methodologies that are reasonable safe, secure, and cost-effective for companies to implement. These standards will be updated as needed, but at least yearly in order to be in compliance with this bill. Furthermore, the Director of the FBI or the Secret Service may request that the standards be updated at specific times as situations that those agencies are involved in develop. The H.R. 1704 version of the definition of a "Security Breach" was solid, but it could've been marginally better. Fortunately, the language to do so was found within the definition for the same phrase in S. 1158. Subparagraph 111(15)(B)(ii) is included so that when an employee accidentally sees data that they aren't supposed to, but they're the only one who does and it stays within the overall company that is holding and storing that data, then that becomes an issue of that company and not federal law, or so that part of the bill would make it if passed into law. Again, this will help cut down the legal costs accrued by business entities as they comply with this new national standard. Last but not least, two new subsections were incorporated in the definition of SPII that, apart from the existing and traditional elements that are considered, also address the evolving data collection points in existence today, such as media files, geolocation, and internet protocols.

Other Titles: Extraterritoriality and Funding

The last two Titles of the bill are shorter than the main, first Title, being around a paragraph each in length. The second title allows this law to be applied, as other countries allow, to non-U.S. Citizens perpetrating cyber crimes from outside of the United States against U.S. computers, networks, and other information systems. Essentially, so long as any one part of the criminal act takes place within the United States or is targeted against property or business entities operating under the laws of the United States, then those who are guilty of such acts can be prosecuted in the United States to the fullest extent of the law. The third and last Title looks at

how the bill will be funded. Thanks to a spending bill passed in 2010, any mandatory and annual federal spending must have a system called a scorecard system in place in order to keep track of annualized expenses for each project and department within the federal government. Since there could potentially be a small but noticeable increase in annual spending to help the offices, agencies, and departments listed within the bill implement and enforce it should it be passed, this Title is included at the end to ensure that the costs of the program, and where subsequent spending cuts or revenue increases will occur to cover those costs, are known before final voting on the bill occurs.

Conclusion

As society continues its trend of increased digitization, there is sure to be a new wave of innovation and improvement in database system technology. Increased threats due to hackers and other cyber criminals can be managed with proactive information technology management strategies, and the damage caused by the rare data breaches that do occur can be minimized through effective implementation of consumer and data protection policies. So long as business agencies are held accountable for protecting the data of their consumers and government agencies are able to enforce those protections, we will be able to forge a pathway to a better, more data-driven tomorrow.

H. R. 2017

To establish a national data breach notification standard, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 3RD, 2017

Mr. MCCOLLOM (for himself, Mr. Barczynski, Mr. Cuevas, and Ms. Kretzer) introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committee on the Judiciary, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

This Bill is based off of H.R. 1704 and S. 1158 of the 114th Congress of the United States of America.

A BILL

To establish a national data breach notification standard, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Personal Data Notification and Protection Act of 2017".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

SEC. 2. FOUNDING PRINCIPLES OF FUTURE DATA BREACH LEGISLATION.

So as to prevent the misinterpretation of this act by future generations, and to set into writing the guidelines and ideals by which this Congress finds all future data breach legislation should follow, the following "Founding Principles" are set forth:

(a) NOTICE.— Whenever data is collected, or breached, by a person, corporation, organization, group, or other entity, the individual whose data is in question shall be notified as to:

(1) The nature of the data to be collected or that was breached.

(2) How their data will be used or how it is expected the breaching entity will attempt to use their data.

(b) CHOICE.— Individuals must be able to choose to opt out of the collection of any personal data by a business entity that will be forwarded to a third party, or the option to deny the business entity in question the right to forward the user's own personal data to a third party after submitting it to the business entity.

(c) ONWARD TRANSFER.— Business entities shall only transfer individual user data, especially sensitive and personally identifiable user data, to third parties that follow adequate or superior data protection principles, as outlined in this act.

(d) SECURITY.—Reasonable efforts must be made by business entities to prevent the loss of sensitive and personally identifiable information collected by the business entity from the user.

(e) DATA INTEGRITY.— All data must have a relevant reason for being collected, and must also be reasonably reliable and accurate, to the best verifiable knowledge of the business entity.

(f) ACCESS.— Individuals must be able to access, edit, and/or delete the information held about them by a business entity from the computers and other smart devices of the company immediately and rapidly, assuming the original information was inaccurate.

(g) ENFORCEMENT.— Any such rule on data privacy, security, or policy must have strong enforcement mechanisms in place in order to deal with the ever-evolving threats of the digital world.

SEC. 3. FINDINGS.

Congress finds that—

(1) databases of sensitive personally identifiable information are increasingly prime targets of hackers, identity thieves, rogue employees, and other criminals, including organized and sophisticated criminal operations;

(2) security breaches caused by such criminal acts are a serious threat to consumer privacy, consumer confidence, homeland security, national security, e-commerce, and economic stability;

(3) misuse of sensitive personally identifiable information has the potential to cause serious or irreparable harm to an individual's livelihood, privacy, and liberty and undermine efficient and effective business and government operations;

(4) identity theft is a serious threat to the Nation's economic stability, national security, homeland security, cybersecurity, the development of e-commerce, and the inherent privacy rights of Americans;

(5) it is important for business entities that own, use, store, or license sensitive personally identifiable information to adopt reasonable policies and procedures to help ensure the security and privacy of sensitive personally identifiable information; and

(6) individuals whose personal information has been compromised or who have been victims of identity theft should receive the necessary information and assistance to mitigate any potential damage and protect their inherent right to privacy and control of their personal information.

TITLE I—NATIONAL DATA BREACH NOTIFICATION STANDARD

SEC. 101. NOTIFICATION TO INDIVIDUALS.

(a) IN GENERAL.—Except as provided for in section 102, any business entity engaged in or affecting interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information about more than 1,000 individuals during any 12-month period shall, following the discovery of a security breach of such information, notify, in accordance with sections 103 and 104, any individual whose sensitive personally identifiable information has been, or is reasonably believed to have been, *illegally* accessed or acquired.

(b) OBLIGATIONS OF AND TO OWNER OR LICENSEE.—

(1) NOTIFICATION TO OWNER OR LICENSEE.—Any business entity engaged in or affecting interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information that the business entity does not own or license shall notify the owner or licensee of the information following the discovery of a security breach involving such information, unless there is no reasonable risk of harm or fraud to such owner or licensee.

(2) NOTIFICATION BY OWNER, LICENSEE, OR OTHER DESIGNATED THIRD PARTY.—Nothing in this title shall prevent or abrogate an agreement between a business entity required to provide notification under this section and a designated third party, including an owner or licensee of the sensitive personally identifiable information subject to the security breach, to provide the notifications required under subsection (a).

(3) SERVICE PROVIDERS.—If a service provider becomes aware of a security breach containing sensitive personally identifiable information that is owned or possessed by a covered entity that connects to or uses a system or network provided by the service provider for the purpose of transmitting, routing, or providing intermediate or transient storage of such data, the service provider shall be required to promptly notify the covered entity who initiated such connection, transmission, routing, or storage of the security breach if the covered entity can be reasonably identified. Upon receiving such notification from a service provider, the covered entity shall be required to provide the notification required under subsection (a).

(4) BUSINESS ENTITY RELIEVED FROM GIVING NOTIFICATION.—A business entity required to provide notification under subsection (a) shall not be required to provide such notification if an owner or licensee of the sensitive personally identifiable information subject to the security breach, or other designated third party, provides such notification.

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—All notifications required under this section shall be made without unreasonable delay following the discovery by the business entity of a security breach. A business entity shall, upon the request of the Commission or the U.S. Attorney General, provide records or other evidence of the notifications required under this section.

(A) INITIAL NOTIFICATION.—Following the discovery of a security breach, a business entity shall issue an initial notification declaring that a security breach has occurred and that a more detailed notification defining the size, scope, and nature of the security breach shall be issued on or before a time 60 days following the initial

discovery of a security breach as verified by records or other evidence as required under paragraph (1).

(B) FULL NOTIFICATION.—Upon determining the size, scope, and nature of the security breach, a business entity shall notify all affected parties of the size, scope, and nature of the security breach, unless prevented under subsection (d) of this section from doing so.

(2) REASONABLE DELAY.—

(A) IN GENERAL.—Except as provided in subsection (d), reasonable delay under this subsection shall not exceed 60 days, unless the business entity seeking additional time requests an extension of time and the Commission determines that additional time is reasonably necessary to determine the size, scope or nature of the security breach, prevent further disclosures, conduct the risk assessment, restore the reasonable integrity of the data system, or provide notice to the breach notification entity.

(B) EXTENSION.—If the Commission determines that additional time is reasonably necessary as described in subparagraph (A), the Commission may extend the time period for notification for additional periods of up to 30 days each. Any such extension shall be provided in writing by the Commission.

(3) BURDEN OF PRODUCTION.—If a business entity requires additional time under paragraph (2), the business entity shall provide the Commission with records or other evidence of the reasons necessitating delay of notification.

(d) DELAY OF NOTIFICATION FOR LAW ENFORCEMENT OR NATIONAL SECURITY.—

(1) IN GENERAL.—If the Director of the United States Secret Service, Secretary of Homeland Security, U.S. Attorney General or the Director of the Federal Bureau of Investigation determines that the notification required under this section would impede a criminal investigation or national security activity, the time period for notification shall be extended 30 days upon written notice from such Director, Secretary, or U.S. Attorney General to the business entity that experienced the breach and to the Commission.

(2) EXTENDED DELAY OF NOTIFICATION.—If the time period for notification required under subsection (a) is extended pursuant to paragraph (1), a business entity shall provide the notification within such time period unless the Director of the United States Secret Service, Secretary of Homeland Security, U.S. Attorney General or the Director of the Federal Bureau of Investigation provides written notification that further extension of the time period is necessary. The Director of the United States Secret Service, Secretary of Homeland Security, U.S. Attorney General or the Director of the Federal Bureau of Investigation may extend the time period for additional periods of up to 30 days each.

(3) ISSUING OR EXTENDING A DELAY OF NOTIFICATION.—With the exception of the Federal Bureau of Investigation and the United States Secret Service, any other Federal law enforcement agency's request for a delay of notification or an extension on such a previously issued request must be approved and administered by the acting U.S. Attorney General. With the exception of the Federal Bureau of Investigation and the United States Secret Service, any other federal intelligence agency, military or civilian, must have their request for a delay of notification or an extension on such a previously issued request approved and served by the Secretary of Homeland Security.

(4) IMMUNITY.—No cause of action for which jurisdiction is based under section 1346(b) of title 28, United States Code, shall lie against any Federal agency for acts relating to the extension of the deadline for notification for law enforcement or national security purposes under this section.

(e) DESIGNATION OF BREACH NOTIFICATION ENTITY.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security shall designate a Federal Government entity to receive notices, reports, and information about information security incidents, threats, and vulnerabilities under this title. Unless prevented under subsection (d), this information shall be shared openly with the Commission to monitor and keep record of compliance with this act.

(f) LIMITATIONS.—Notwithstanding any other obligation under this title, this title does not apply to the following, unless the below-listed acts do not have sufficient legal requirements to meet the standards for data breach notification, as outlined in this act:

(1) FINANCIAL INSTITUTIONS.—Financial institutions—

(A) subject to and in compliance with the data security requirements and standards under section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)); and

(B) subject to the jurisdiction of an agency or authority described in section 505(a) of the Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)).

(2) HIPAA AND HITECH REGULATED ENTITIES.—An entity that is subject to and in compliance with the data breach notification of the following, with respect to data that is subject to such requirements:

(A) Section 13401 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931).

(B) Part 160 or 164 of title 45, Code of Federal Regulations (or any successor regulations).

(C) The regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note).

(D) In the case of a business entity, the applicable data breach notification requirements of part 1 of subtitle D of title XIII of division A of the American Reinvestment and Recovery Act of 2009 (42 U.S.C. 17931 et seq.), if such business entity is acting as a covered entity, a business associate, or a vendor of personal health records, as those terms are defined in section 13400 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17921).

(E) In the case of a third party service provider, section 13407 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17937).

SEC. 102. EXEMPTIONS FROM NOTIFICATION TO INDIVIDUALS.

(a) EXEMPTION FOR NATIONAL SECURITY AND LAW ENFORCEMENT.—

(1) IN GENERAL.—Notwithstanding section 101, if the Director of the United States Secret Service, Secretary of Homeland Security, U.S. Attorney General or the Director of

the Federal Bureau of Investigation determines that notification of the security breach required by section 101 could be expected to reveal sensitive sources and methods or similarly impede the ability of a Federal, State, or local law enforcement agency to conduct law enforcement investigations, or if the Director of the Federal Bureau of Investigation or the Secretary of Homeland Security determines that notification of the security breach could be expected to cause damage to national security, such notification is not required.

(2) IMMUNITY.—No cause of action for which jurisdiction is based under section 1346(b) of title 28, United States Code, shall lie against any Federal agency for acts relating to the extension of the deadline for notification for law enforcement or national security purposes under this section.

(b) SAFE HARBOR.—

(1) IN GENERAL.—A business entity is exempt from the notification requirement under section 101, if the following requirements are met:

(A) RISK ASSESSMENT.—A risk assessment, in accordance with paragraph (3), is conducted by or on behalf of the business entity that concludes that there is no reasonable risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach.

(B) NOTICE TO COMMISSION.—Without unreasonable delay as defined in subparagraph 101(c)(2)(A) of this act and not later than 60 days after the discovery of a security breach, unless extended by the Commission, the Director of the United States Secret Service, Secretary of Homeland Security, U.S. Attorney General or the Director of the Federal Bureau of Investigation under section 101 (in which case, before the extended deadline), the business entity notifies the Commission, in writing, of—

(i) the results of the risk assessment; and

(ii) the decision by the business entity to invoke the risk assessment exemption described under subparagraph (A).

(C) DETERMINATION BY COMMISSION.—During the period beginning on the date on which the notification described in subparagraph (B) is submitted and ending 10 days after such date, the Commission has issued a determination in writing that a notification should not be provided under section 101.

(2) REBUTTABLE PRESUMPTION.—For purposes of paragraph (1)—

(A) the rendering of sensitive personally identifiable information at issue unusable, unreadable, or indecipherable through a security technology generally accepted by experts in the field of information security as set by the National Institute of Standards and Technology in their Cybersecurity Framework or the Director of the National Security Agency as applicable shall establish a rebuttable presumption that such reasonable risk does not exist; and

(B) any such presumption shall be rebuttable by facts demonstrating that the security technologies or methodologies in a specific case have been, or are reasonably likely to have been, compromised.

(3) RISK ASSESSMENT REQUIREMENTS.—A risk assessment is in accordance with this paragraph if the following requirements are met:

(A) PROPERLY CONDUCTED.—The risk assessment is conducted in a reasonable manner or according to standards generally accepted by experts in the field of information security and in line with the National Institute of Standards and Technology's Cybersecurity Framework.

(B) LOGGING DATA REQUIRED.—The risk assessment includes logging data, as applicable and to the extent available, for a period of at least six months before the discovery of a security breach described in section 101(a)—

(i) for each communication or attempted communication with a database or data system containing sensitive personally identifiable information, the data system communication information for the communication or attempted communication, including any Internet addresses, and the date and time associated with the communication or attempted communication; and

(ii) all log-in information associated with databases or data systems containing sensitive personally identifiable information, including both administrator and user log-in information.

(C) FRAUDULENT OR MISLEADING INFORMATION.—The risk assessment does not contain fraudulent or deliberately misleading information.

(c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

(1) IN GENERAL.—A business entity is exempt from the notification requirement under section 101 if the business entity uses or participates in a security program that—

(A) effectively blocks the use of the sensitive personally identifiable information to initiate unauthorized financial transactions before they are charged to the account of the individual; and

(B) provides notification and one year of free credit monitoring to affected individuals after a security breach that has resulted in fraud or unauthorized transactions.

(2) LIMITATION.—The exemption in paragraph (1) does not apply if the information subject to the security breach includes any other type of sensitive personally identifiable information as defined in section 111 of this title.

SEC. 103. METHODS OF NOTIFICATION.

A business entity shall be in compliance with the requirements of this section if, with respect to the method of notification as required under section 101, the following requirements are met:

(1) INDIVIDUAL NOTIFICATION.—Notification to an individual is by one of the following means:

(A) Written notification to the last known home mailing address of the individual in the records of the business entity.

(B) Telephone notification to the individual personally.

(C) E-mail notification, if—

(i) (I) the covered entity's primary method of communication with the individual is by e-mail; or

(II) the individual has consented to receive such notice and the notice is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001); and

(ii) the e-mail notice does not request, or contain a hypertext link to a request, that the consumer provide personal information in response to the notice.

(2) MEDIA NOTIFICATION.—If the number of residents of a State whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person exceeds 5,000 individuals in a State and individual notice is not feasible due to lack of sufficient contact information for the individuals required to be notified, a business entity shall:

(A) Provide notification to media reasonably calculated to reach such individuals, such as major media outlets serving a State or jurisdiction. Such a mass notification must still conform to content requirements as outlined in section 104.

(B) Place notice in a clear and conspicuous place on their website and the websites of any third-party entities which have any direct contact with end users, provided the business entity and any third-parties meeting the above requirement operate a website and they conform to the content requirements outlined for them in section 104.

SEC. 104. CONTENT OF NOTIFICATION.

(a) IN GENERAL.—The notification provided to individuals required by section 101 shall include, to the extent possible, the following:

(1) A description of the categories of sensitive personally identifiable information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, group, entity, or other organization of individuals.

(2) A toll-free number—

(A) that the individual may use to contact the business entity, or the agent of the business entity; and

(B) from which the individual may learn what types of sensitive personally identifiable information the business entity maintained about that individual, including information on which, if any, categories of sensitive personally identifiable information may have been breached or otherwise put at risk:

(3) The toll-free contact telephone numbers and addresses for the major credit reporting agencies if the sensitive personally identifiable information that was breached could be used to commit financial fraud or identity theft, as well as the corresponding toll-free contact telephone number and address of the Commission:

(4) The acts the covered entity, or the agent of the covered entity, has taken to protect sensitive personally identifiable information from further security breach;

(5) The name of the business entity that has the most direct business relationship with the individual:

(6) Notwithstanding section 109, any additional information regarding victim protection assistance required by the State in which the individual resides, unless adherence to this paragraph of section 104(a) is the sole cause of a business entity's request for a delay of notification under section 101(c)(2) of this act, in which case the Commission shall issue the extension for compliance with state law while mandating the timeliness of a notification that complies with the national standard for notification, as outlined in this act:

(b) EXCEPTION.—The toll-free number in paragraph (2) of subsection (a) above may be substituted with an online platform - in most cases, the website of the business entity in question

- provided that the conditions outlined in the same paragraph and subsection are met, as well as the following conditions:

(1) The online platform is accessible within reason by anyone via the internet through any of the major Internet browser applications, mobile or otherwise, as of the day the notification is published or otherwise brought online.

(2) The online platform maintains clear links to the major credit agencies' websites.

(3) The online platform is hosted by an Internet address deemed reasonably secure by the standards outlined in the most recent version of the National Institute of Standards and Technology's Cybersecurity Framework as of the day preceding the day the breach was discovered by the business entity or relevant third-party of the business entity by 30 days.

SEC. 105. COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.

(a) REQUIREMENT TO NOTIFY CREDIT REPORTING AGENCIES.—If a business entity is required to notify more than 1,000 individuals under section 101, the business entity shall also notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis (as defined in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p))) of the timing and distribution of the notifications. Such notification shall be given to the consumer credit reporting agencies without unreasonable delay and, if it will not delay notification to the affected individuals, prior to the distribution of notifications to the affected individuals.

(b) REASONABLE DELAY.—Reasonable delay under subsection (a) shall not exceed 60 days following the discovery of a security breach, except as provided in subsection (c) or (d) of section 101 (in which case, before the extended deadline), or unless the business entity providing notification can demonstrate to the Commission that additional time is reasonably necessary to determine the size, scope, and nature of the security breach, prevent further disclosures, conduct the risk assessment, restore the reasonable integrity of the data system, and provide notice to the breach notification entity. If the Commission determines that additional time is necessary, the Commission may extend the time period for notification for additional periods of up to 30 days each. Any such extension shall be provided in writing.

SEC. 106. NOTIFICATION FOR LAW ENFORCEMENT AND OTHER PURPOSES.

(a) DESIGNATION OF GOVERNMENT ENTITY TO RECEIVE NOTICE.—

(1) IN GENERAL.—Not later than 60 days after the date of enactment of this Act, the Secretary of Homeland Security, in consultation with the Attorney General, shall designate a breach notification entity to receive the notices required under section 101 and this section.

(b) NOTIFICATION TO LAW ENFORCEMENT AND NATIONAL SECURITY AUTHORITIES.—Any business entity shall notify the breach notification entity, and the breach notification entity shall promptly notify and provide that information:

(1) To the United States Secret Service, the Federal Bureau of Investigation, the U.S. Attorney General and the Commission for civil law enforcement purposes.

(2) As appropriate to the Department of Homeland Security or other Federal agencies for national security or computer security purposes, if—

(A) The number of individuals whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person exceeds 5,000;

(B) The security breach involves a database, networked or integrated databases, or other data system containing the sensitive personally identifiable information of more than 500,000 individuals nationwide;

(C) The security breach involves databases owned by the Federal Government; or

(D) The security breach involves primarily sensitive personally identifiable information of individuals known to the business entity to be employees and contractors of the Federal Government involved in national security or law enforcement.

(b) REGULATIONS.—Not later than one year after the date of enactment of this Act, the Commission shall promulgate regulations (in accordance with section 553 of title 5, United States Code) in consultation with the Attorney General and the Secretary of Homeland Security, that describe what information is required to be included in the notification under subsection (a). In addition the Commission shall promulgate regulations, as necessary, (in accordance with section 553 of title 5, United States Code) in consultation with the Attorney General, to adjust the thresholds for notification to law enforcement and national security authorities under subsection (a) and to facilitate the purposes of this section.

(c) TIMING OF NOTIFICATION.—The notification required under this section shall be provided as promptly as possible and at least 72 hours before notification of an individual pursuant to section 101 or 10 days after discovery of the breach requiring notification, whichever comes first.

SEC. 107. FEDERAL ENFORCEMENT.

(a) IN GENERAL.—The Attorney General and the Federal Trade Commission may enforce civil violations of this subtitle.

(b) CIVIL ACTIONS BY THE ATTORNEY GENERAL OF THE UNITED STATES.—

(1) IN GENERAL.—The Attorney General may bring a civil action in the appropriate United States district court against any covered entity that engages in conduct constituting a violation of this subtitle and, upon proof of such conduct by a preponderance of the evidence, the covered entity shall be subject to a civil penalty in an amount not greater than the product of the number of violations of this subtitle and $16,500. Each failure to provide notification to an individual as required under this subtitle shall be treated as a separate violation.

(2) PENALTY LIMITATION.—Notwithstanding any other provision of law, the total amount of the civil penalty assessed against a covered entity for conduct involving the same or related acts or omissions that results in a violation of this subtitle may not exceed $10,000,000, unless such conduct is found to be willful or intentional.

(3) DETERMINATIONS.—The determination of whether a violation of a provision of this subtitle has occurred, and if so, the amount of the penalty to be imposed, if any, shall be

made by the court sitting as the finder of fact. The determination of whether a violation of a provision of this subtitle was willful or intentional, and if so, the amount of the additional penalty to be imposed, if any, shall be made by the court sitting as the finder of fact.

(4) ADDITIONAL PENALTY LIMIT.—If a court determines under paragraph (3) that a violation of a provision of this subtitle was willful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $10,000,000.

(c) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—If it appears that a covered entity has engaged, or is engaged, in any act or practice constituting a violation of this subtitle, the Attorney General may petition an appropriate district court of the United States for an order—

(A) enjoining such act or practice; or

(B) enforcing compliance with this subtitle.

(2) ISSUANCE OF ORDER.—A court may issue an order under paragraph (1), if the court finds that the conduct in question constitutes a violation of this subtitle.

(d) CIVIL ACTIONS BY THE FEDERAL TRADE COMMISSION.—

(1) IN GENERAL.—Compliance with the requirements imposed under this subtitle may be enforced under the Federal Trade Commission Act (15 U.S.C. 41 et seq.) by the Federal Trade Commission with respect to business entities subject to this Act. All of the functions and powers of the Federal Trade Commission under the Federal Trade Commission Act are available to the Commission to enforce compliance by any person with the requirements imposed under this title.

(2) CIVIL PENALTIES.—

(A) IN GENERAL.—Any covered entity that violates this subtitle shall be subject to a civil penalty in the amount that is not greater than the product of the number of

violations of this subtitle and $16,500. Each failure to provide notification to an individual as required under this subtitle shall be treated as a separate violation.

(B) PENALTY LIMITATION.—Notwithstanding any other provision of law, the total sum of civil penalties assessed against a covered entity for all violations of the provisions of this subtitle resulting from the same or related acts or omissions may not exceed $10,000,000, unless such conduct is found to be willful or intentional.

(C) DETERMINATIONS.—The determination of whether a violation of a provision of this subtitle has occurred, and if so, the amount of the penalty to be imposed, if any, shall be made by the court sitting as the finder of fact. The determination of whether a violation of a provision of this subtitle was willful or intentional, and if so, the amount of the additional penalty to be imposed, if any, shall be made by the court sitting as the finder of fact.

(D) ADDITIONAL PENALTY LIMIT.—If a court determines under subparagraph (C) that a violation of a provision of this subtitle was willful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $10,000,000.

(3) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—For the purpose of the exercise by the Federal Trade Commission of its functions and powers under the Federal Trade Commission Act, a violation of any requirement or prohibition imposed under this title shall constitute an unfair or deceptive act or practice in commerce in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(I)(B)) regarding unfair or deceptive acts or practices and shall be subject to enforcement by the Federal Trade Commission under that Act with respect to any business entity, irrespective of whether that business entity is engaged in commerce or meets any other jurisdictional tests in the Federal Trade Commission Act.

(e) COORDINATION OF ENFORCEMENT.—

(1) IN GENERAL.—When opening an investigation, the Federal Trade Commission shall consult with the Attorney General.

(2) LIMITATION.—The Federal Trade Commission may initiate investigations under this subsection unless the Attorney General or the Secretary of Homeland Security determines that such an investigation would impede an ongoing criminal investigation or national security activity.

(3) COORDINATION AGREEMENT.—

(A) IN GENERAL.—In order to avoid conflicts and promote consistency regarding the enforcement and litigation of matters under this Act, not later than 90 days after the enactment of this Act, the Attorney General and the Federal Trade Commission shall enter into an agreement for coordination regarding the enforcement of this Act.

(B) REQUIREMENT.—The coordination agreement entered into under subparagraph (A) shall include provisions to ensure that parallel investigations and proceedings under this section are conducted in a manner that avoids conflicts and does not impede the ability of the Attorney General to prosecute violations of Federal criminal laws.

(f) RULEMAKING.—The Federal Trade Commission may, in consultation with the Attorney General, issue such other regulations as it determines to be necessary to carry out this subtitle. All regulations promulgated under this Act shall be issued in accordance with section 553 of title 5, United States Code.

(g) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this subtitle are cumulative and shall not affect any other rights and remedies available under law.

(h) FRAUD ALERT.—Section 605A(b)(1) of the Fair Credit Reporting Act (15 U.S.C. 1681c–1(b)(1)) is amended by inserting ", or evidence that the consumer has received notice that the consumer's financial information has or may have been compromised," after "identity theft report".

SEC. 108. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) IN GENERAL.—

(1) CIVIL ACTIONS.—

(A) IN GENERAL.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that a covered entity has violated this subtitle, the State, as parens patriae, may bring a civil action on behalf of the residents of the State to—

(i) enjoin that practice;

(ii) enforce compliance with this subtitle; or

(iii) impose a civil penalty in an amount not greater than the product of the number of violations of this subtitle and $16,500.

(B) FAILURE TO PROVIDE NOTIFICATION.—For purposes of subparagraph (A)(iii), each failure to provide notification to an individual as required under this subtitle shall be treated as a separate violation.

(2) PENALTY LIMITATION.—

(A) IN GENERAL.—Notwithstanding any other provision of law, the total sum of civil penalties assessed against a covered entity for all violations of the provisions of this subtitle resulting from the same or related acts or omissions may not exceed $10,000,000, unless such conduct is found to be willful or intentional.

(B) DETERMINATIONS.—The determination of whether a violation of a provision of this subtitle has occurred, and if so, the amount of the penalty to be imposed, if any, shall be made by the court sitting as the finder of fact. The determination of whether a violation of a provision of this subtitle was willful or intentional, and if so, the amount of the additional penalty to be imposed, if any, shall be made by the court sitting as the finder of fact.

(C) ADDITIONAL PENALTY LIMIT.—If a court determines under subparagraph (B) that a violation of a provision of this subtitle was willful or

intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $10,000,000.

(3) NOTICE.—

(A) IN GENERAL.—Before filing an action under paragraph (1), the attorney general of the State involved shall provide to the Attorney General of the United States and the Federal Trade Commission—

(i) written notice of the action; and

(ii) a copy of the complaint for the action.

(B) EXEMPTION.—

(i) IN GENERAL.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subtitle, if the State attorney general determines that it is not feasible to provide the notice described in such subparagraph before the filing of the action.

(ii) NOTIFICATION.—In an action described in clause (i), the attorney general of a State shall provide notice and a copy of the complaint to the Attorney General of the United States and the Federal Trade Commission at the time the State attorney general files the action.

(b) FEDERAL PROCEEDINGS.—Upon receiving notice under section 106(b)(1) from the breach notification entity, the Attorney General and the Federal Trade Commission shall have the right to—

(1) move to stay the action, pending the final disposition of a pending Federal proceeding or action;

(2) initiate an action in the appropriate United States district court under section 107 and move to consolidate all pending actions, including State actions, in such court;

(3) intervene in an action brought under subsection (a)(2); and

(4) file petitions for appeal.

(c) PENDING PROCEEDINGS.—If the Attorney General or the Federal Trade Commission initiates a criminal proceeding or civil action for a violation of a provision of this title, or any regulations thereunder, no attorney general of a State may bring an action for a violation of a provision of this subtitle against a defendant named in the Federal criminal proceeding or civil action.

(d) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this subtitle regarding notification shall be construed to prevent an attorney general of a State from exercising the powers conferred on such attorney general by the laws of that State to—

(1) conduct investigations;

(2) administer oaths or affirmations; or

(3) compel the attendance of witnesses or the production of documentary and other evidence.

(e) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in—

(A) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(B) another court of competent jurisdiction.

(2) SERVICE OF PROCESS.—In an action brought under subsection (a), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

(f) NO PRIVATE CAUSE OF ACTION.—Nothing in this subtitle establishes a private cause of action against a business entity for violation of any provision of this subtitle.

SEC. 109. EFFECT ON STATE LAW.

The provisions of this title shall supersede any provision of the law of any State, or a political subdivision thereof, relating to notification by a business entity engaged in interstate commerce of a security breach, except as provided in section 104(6).

SEC. 110. REPORTING ON SECURITY BREACHES.

(a) REPORT REQUIRED ON NATIONAL SECURITY AND LAW ENFORCEMENT EXEMPTIONS.—Not later than 6 months after the date of enactment of this title, and annually thereafter, the Director of the United States Secret Service, Secretary of Homeland Security, U.S. Attorney General and the Director of the Federal Bureau of Investigation shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate on a report on the number and nature of security breaches subject to the national security and law enforcement exemptions under section 102(a).

(b) REPORT REQUIRED ON SAFE HARBOR EXEMPTIONS.—Not later than 6 months after the date of enactment of this title, and annually thereafter, the Commission shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on the number and size, scope, and nature of the security breaches described in the notices filed by business entities invoking the risk assessment exemption under section 102(b) and the response of the Commission to such notices.

(c)REPORT REQUIRED ON FINANCIAL FRAUD PROTECTION EXEMPTIONS.—Not later than 6 months after the date of enactment of this title, and annually thereafter, the Commission shall submit to the Committee on Energy and Commerce and the Financials Services Committee of the House of Representatives and the Committee on Commerce, Science, and Transportation and Finance Committee of the Senate a report on the number and size, scope, and nature of the

security breaches described in the notices filed by business entities invoking the financial fraud protection exemption under section 102(c) and the response of the Commission to such notices.

SEC. 111. DEFINITIONS.

In this title:

(1) AFFILIATE.—The term "affiliate" means persons related by common ownership or by corporate control.

(2) AGENCY.—The term "agency" has the same meaning given such term in section 551 of title 5, United States Code.

(3) BREACH NOTIFICATION ENTITY.—The term "breach notification entity" means the Federal Government entity designated pursuant to section 101(e).

(4) BUSINESS ENTITY.—The term "business entity" means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture, whether or not established to make a profit.

(5) COMMISSION.—The term "Commission" means the Federal Trade Commission.

(6) CONSUMER FINANCIAL PRODUCT OR SERVICE.—The term "consumer financial product or service" has the meaning given that term in section 1002 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (12 U.S.C. 5481).

(7) COVERED ENTITY.—The term "covered entity" means any business entity, other than a service provider, that collects, uses, accesses, transmits, stores, or disposes of sensitive personally identifiable information.

(8) DATA SYSTEM COMMUNICATION INFORMATION.—The term "data system communication information" means dialing, routing, addressing, or signaling information that identifies the origin, direction, destination, processing, transmission, or termination of each communication initiated, attempted, or received.

(9) DATE AND TIME.—The term "date and time" includes the date, time, and specification of the time zone offset from Coordinated Universal Time.

(10) ENCRYPTION.—The term "encryption"—

(A) means the protection of data in electronic form, in storage or in transit, using an encryption technology that renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and

(B) includes appropriate management and safeguards of such cryptographic keys so as to protect the integrity of the encryption; and

(C) its validity will be determined based upon the validity of the encryption technology utilized as established by the Director of the National Security Agency; who will approve a list encryption technologies that meet the current standards and demands of the information security field. This list —

(i) will be reviewed and updated accordingly at a minimum of once every year.

(ii) can be amended or updated upon a request presented by the Director of the Federal Bureau of Investigation or the Director of the Secret Service.

(iii) will be created upon enactment of this Act and by no later than 90 days.

(11) FEDERAL AGENCY.—The term "Federal agency" has the meaning given the term "agency" in section 3502 of title 44, United States Code.

(12) IDENTITY THEFT.—The term "identity theft" means a violation of section 1028(a)(7) of title 18, United States Code.

(13) INTELLIGENCE COMMUNITY.—The term "intelligence community" has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(14) INTERNET ADDRESS.—The term "Internet address" means an Internet Protocol address as specified by the Internet Protocol version 4 or 6 protocol, or any successor protocol or any unique number for a specific host on the Internet.

(15) SECURITY BREACH.—

(A) IN GENERAL.—The term "security breach" means a compromise of the security, confidentiality, or integrity of, or the loss of, computerized data that results in, or there is a reasonable basis to conclude has resulted in—

(i) the unauthorized acquisition of sensitive personally identifiable information; or

(ii) access to sensitive personally identifiable information that is for an unauthorized purpose, or in excess of authorization.

(B) EXCLUSION.—The term "security breach" does not include—

(i) any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an element of the intelligence community.

(ii) a good faith access or acquisition of sensitive personally identifiable information by a business entity, or an employee or agent of a business entity, if the sensitive personally identifiable information is not subject to further unauthorized disclosure;

(16) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term "sensitive personally identifiable information" means any information or compilation of information, in electronic or digital form that includes one or more of the following:

(A) An individual's first and last name or first initial and last name in combination with any two of the following data elements:

(i) Home address or telephone number.

(ii) Mother's maiden name.

(iii) Month, day, and year of birth.

(B) A social security number (but not including only the last four digits of a social security number), driver's license number, passport number, or alien registration number or other government-issued unique identification number.

(C) Unique biometric data such as a fingerprint, voice print, a retina or iris image, or any other unique physical representation.

(D) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code.

(E) A username or electronic mail address, in combination with a password or security question and answer that would permit access to an online account.

(F) Any combination of the following data elements:

(i) An individual's first and last name or first initial and last name, user name, or email address

(ii) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code.

(iii) Any security code, access code, or password, or source code that could be used to generate such codes or passwords.

Any security code, access code, password, security question and answer, or source code that could be used to generate such codes or passwords required for an individual to obtain money, goods, services, access to digital photographs, digital videos or electronic communications, or any other thing of value.

(G) Information about an individual's geographic location generated by or derived from the operation or use of an electronic communications device that is sufficient to identify the street and name of the city or town in which the device is located, excluding telephone numbers or network or Internet protocol addresses.

(H) Password-protected digital photographs and digital videos not otherwise available to the public.

(17) SERVICE PROVIDER.—The term "service provider" means a business entity that provides electronic data transmission, routing, intermediate and transient storage, or connections to its system or network, where the business entity providing such services does not select or modify the content of the electronic data, is not the sender or the intended recipient of the data, and the business entity transmits, routes, or provides connections for sensitive personally identifiable information in a manner that sensitive personally identifiable information is undifferentiated from other types of data that such business entity transmits, routes, or provides connections. Any such business entity shall be treated as a service provider under this act only to the extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage or connections.

(18) MODIFIED DEFINITION BY RULEMAKING.—The Commission may, by rule promulgated under section 553 of title 5, United States Code, amend the definition of "sensitive personally identifiable information" to the extent that such amendment will accomplish the purposes of this title. In amending the definition, the Commission may determine—

(A) that any particular combinations of information are sensitive personally identifiable information; or

(B) that any particular piece of information, on its own, is sensitive personally identifiable information.

SEC. 112. EFFECTIVE DATE.

This title shall take effect 90 days after the date of enactment of this Act.

TITLE II—EXTRATERRITORIAL APPLICATION OF CYBER CRIME LAW

SEC. 201. EXTRATERRITORIAL JURISDICTION.

Subsection (h) of section 1029 of title 18, United States Code, is amended to read as follows:

"(h) Any person who, outside the jurisdiction of the United States, engages in any act that, if committed within the jurisdiction of the United States, would constitute an offense under subsection (a) or (b), shall be subject to the fines, penalties, imprisonment, and forfeiture provided in this title if the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity organized under the laws of the United States, or any State, the District of Columbia, or other territory of the United States.".

TITLE III—COMPLIANCE WITH STATUTORY PAY-AS-YOU-GO ACT

SEC. 301. BUDGET COMPLIANCE.

The budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined by reference to the latest statement titled "Budgetary Effects of PAYGO Legislation" for this Act, submitted for printing in the Congressional Record by the Chairman of the Senate Budget Committee, provided that such statement has been submitted prior to the vote on passage.

Works Cited

28, §§ 1346-B-B. Print.

7,500 Online Shoppers Unknowingly Sold Their Souls. (2010, April 15). Retrieved December 3, 2015, from http://www.foxnews.com/tech/2010/04/15/online-shoppers-unknowingly-sold-souls.html

About - Project Moore. (n.d.). Retrieved December 3, 2015, from http://www.projectmoore.com/en/lawyers

"About the Federal Trade Commission Act." *Federal Trade Commission Act*. Federal Trade Commission, n.d. Web. 16 Oct. 2015.

BakerHostetler. *Data Breach Charts*. Rep. BakerHostetler LLP, 2015. Web. 17 Dec. 2015.

Barnes, Susan B. "A Privacy Paradox: Social Networking in the United States." *First Monday* 11.9 (2006). Print.

Connolly, Chris. "The US Safe Harbor - Fact or Fiction? (2008)." *The US Safe Harbor - Fact or Fiction? (2008)*. Galexia, 2008. Web. 17 Dec. 2015.

Consumer Privacy Protection Act of 2015, S. 1158, 114th Cong. (2015). Print.

Cotton, Hamish, and Christopher Bolan. "User Perceptions of End User License Agreements in the Smartphone Environment." *Edith Cowan University Research Online*. Research Online, 5 Dec. 2011. Web. 17 Dec. 2015.

Data Breach Notification Act of 2009, S. 139, 111th Cong. (2009). Print.

Data Breach Notification Act of 2011, S. 1048, 112th Cong. (2011). Print.

Denvil, James. "Insights on the Consumer Privacy Bill of Rights Act of 2015." *HL Chronicle of Data Protection*. Hogan Lovells, 3 Mar. 2015. Web. 17 Dec. 2015.

Directive 95/46/EC of the European Parliament and of the Council. (1995). Official Journal, L(281), 31-50. Retrieved December 3, 2015, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Dulabon, David W. "Interview with Mr. Dulabon." Personal interview. 4 Dec. 2015.

"Energy & Commerce Committee." *Energy & Commerce Committee*. U.S. House of Representatives, 2015. Web. 17 Dec. 2015.

European Parliament. "Directive 95/46/ec of the European Parliament and of the Council." *Official Journal* (1995): 31-50. Print.

"Fair EULAs." *The Simple EULA Project*. 2015. Web. 17 Dec. 2015.

Federal Trade Commission. *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*. *Federal Trade Commission*. Federal Trade Commission, 29 Nov. 2011. Web. 30 Oct. 2015.

FileCatalyst. "Today's Media File Sizes - What's Average? - FileCatalyst." *FileCatalyst*. N.p., 06 Mar. 2013. Web. 16 Dec. 2015.

"Flesch Kincaid, Gunning Fog and More ..." *Free Online Readability Calculator*. Readability-Score.com, 2015. Web. 17 Dec. 2015.

Floresca, Lauri. "Data Breach Settlements: A New Cost in Cyber Risk." *News & Events Blogs*. Woodruff-Sawyer & Co, 2015. Web. 17 Dec. 2015.

Fox News Network. "7,500 Online Shoppers Unknowingly Sold Their Souls." *Fox News*. FOX News Network, LLC, 15 Apr. 2010. Web. 17 Dec. 2015.

Free Online Readability Calculator - Flesch Kincaid, Gunning Fog and more ... (2015). Retrieved December 3, 2015, from https://readability-score.com/

Gross, Grant. "Lawmakers Push for Federal Data Breach Notification Law." *PCWorld*. N.p., 18 July 2013. Web. 12 Dec. 2015.

The Health Insurance Portability and Accountability Act of 1996. Pub. L. 104-191. Stat. 1936. Web. 21 Sept 2015.

Humphries, Daniel. "Public Attitudes Towards Data Collection and Privacy." *Public Attitudes Towards Data Collection and Privacy*. Software Advice, 11 Nov. 2014. Web. 14 Dec. 2015.

Insurance Information Institute. "Identity Theft and Cybercrime." *Insurance Information Institute*. Insurance Information Institute, n.d. Web. 16 Dec. 2015.

Johnson, Kara J. "HITECH 101." *ABA Young Lawyers Division*. American Bar Association, n.d. Web. 16 Dec. 2015.

Kharpal, Arjun. "US and EU in Data Privacy Clash: What You Need to Know." *CNBC*. CNBC LLC., 7 Oct. 2015. Web. 17 Dec. 2015.

Kitten, Tracy. "Is Neiman Marcus Case a Game-Changer?" *DataBreach Today*. Information Security Media Group, Corp., 10 Aug. 2015. Web. 17 Dec. 2015.

Koëter, Jeroen. "About - Project Moore." *Project Moore*. Project Moore Advocaten B.V., 2015. Web. 17 Dec. 2015.

Krantz, Peter. "Methods for Measuring Text Readability." *Standards Schmandards*. 9 Sept. 2005. Web. 17 Dec. 2015.

Leiserson, Nicholas. "Interview with Mr. Leiserson." Telephone interview. 14 Dec. 2015.

Lesk, Michael. "How Much Information Is There In the World?" Michael Lesk, 1997. Web. 16 Dec. 2015.

Lomas, Natasha. "Europe's Top Court Strikes Down 'Safe Harbor' Data-Transfer Agreement With U.S." *TechCrunch*. AOL Inc., 6 Oct. 2015. Web. 17 Dec. 2015.

"Maastricht Treaty." *Maastricht Treaty*. Eurodollarcurrency.com, 2012. Web. 17 Dec. 2015.

Masnick, Mike. "To Read All Of The Privacy Policies You Encounter, You'd Need To Take A Month Off From Work Each Year." *Techdirt*. Techdirt, 23 Apr. 2012. Web. 17 Dec. 2015.

McDonald, Aleecia, and Lorrie Cranor. "The Cost of Reading Privacy Policies." *I/S: A Journal of Law and Policy for the Information Society* 4.3 (2008). *I/S*. Moritz College of Law. Web. 17 Dec. 2015.

Matteson, Scott. "How Does Google Search Really Work? - TechRepublic." *TechRepublic*. N.p., 11 Dec. 2013. Web. 16 Dec. 2015.

Mearian, Lucas. "Scientists Calculate Total Data Stored to Date: 295+ Exabytes." *Computerworld*. N.p., 14 Feb. 2011. Web. 16 Dec. 2015.

Mullins, Brody. "Google Makes Most of Close Ties to White House." *WSJ*. The Wall Street Journal, 24 Mar. 2015. Web. 17 Dec. 2015.

MintzLevin. *State Data Security Breach Notification Laws*. Rep. Mintz, Levin, Cohn, Ferris, Glovsky, and Popeo PC, 2015. Web. 17 Dec. 2015.

Morooney, Kevin M. "Interview with Mr. Morooney." Personal interview. 18 Nov. 2015.

National Institute for Standards and Technology. "Overview." *Cybersecurity Framework*. U.S. Department of Commerce, 12 Nov. 2013. Web. 17 Dec. 2015.

Obama, Barack. "Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015." *Whitehouse.gov*. The White House, 2015. Web. 17 Dec. 2015.

"Parens Patriae." West's Encyclopedia of American Law, edition 2. 2008. The Gale Group 17 Dec. 2015 http://legal-dictionary.thefreedictionary.com/Parens+Patriae

Personal Data Notification and Protection Act of 2015, H.R. 1704, 114th Cong. (2015). Print.

Personal Data Notification and Protection Act of 2017, H.R. 2017, 115th Cong. Print.

"Press Release No 117/15." *Curia.europa.eu*. Court of Justice of the European Union, 6 Oct. 2015. Web. 17 Dec. 2015.

Rauhofer, Judith(2008) 'Privacy is dead, get over it! Information privacy and the dream of a risk-free society', Information & Communications Technology Law, 0: 0, 185 — 197.

Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti. *Do Data Breach Disclosure Laws Reduce Identity Theft?* Rep. N.p.: n.p., n.d. Print.

Scott, Mark. "Data Transfer Pact Between U.S. and Europe Is Ruled Invalid." *The New York Times*. The New York Times, 6 Oct. 2015. Web. 17 Dec. 2015.

Segalis, Boris, Marcus Evans, and Jay Modrall. "Day-after-Safe Harbor Action Plan: Anticipating ECJ Schrems Decision." *Data Protection Report*. Norton Rose Fulbright LLP, 5 Oct. 2015. Web. 17 Dec. 2015.

Shoemaker, Natalie. "Don't Click "Agree": Demand More Readable Terms of Service Agreements." *Big Think*. The Big Think, Inc., 17 Nov. 2014. Web. 17 Dec. 2015.

Snyder, Benjamin. "Google Averages One White House Visit Every Week." *Fortune*. Time Inc., 25 Mar. 2015. Web. 17 Dec. 2015.

Stevens, Gina. *Data Security Breach Notification Laws*. Rep. Washington DC: Congressional Research Service, 2011. Print.

Stray, Jonathan. "Iceland Aims to Become an Offshore Haven for Journalists and Leakers." *Niemanlab*. Walter Lippmann House, 11 Feb. 2011. Web. 17 Dec. 2015.

"The Bill of Rights: A Transcription." *The Charters of Freedom*. National Archives and Records Administration, 1791. Web. 17 Dec. 2015.

"The U.S.-EU Safe Harbor Guide to Self-Certification." *U.S. - EU Safe Harbor Framework*. U.S. Department of Commerce, 1 Mar. 2013. Web. 17 Dec. 2015.

"U.S. Senate Select Committee on Intelligence." *U.S. Senate Select Committee on Intelligence*. U.S. Senate, 2015. Web. 17 Dec. 2015.

"U.S.-EU Safe Harbor." *Export.gov*. U.S. Department of Commerce, 18 Dec. 2013. Web. 17 Dec. 2015.

UN General Assembly. "The Universal Declaration of Human Rights." *UN News Center*. The United Nations, 10 Dec. 1948. Web. 17 Dec. 2015.

United States. Cong. Committee on the Judiciary. *Data Breach Notification Act, September 15, 2010, 111-2 Senate Report 111-290*. By Patrick Leahy. 111th Cong., 2nd sess. Cong. Rept. 111-290. N.p.: n.p., 2010. Print.

Weil. *Security Breach Notification Laws - Data Privacy Survey 2014*. Rep. Weil, Gotshal, & Manges, 2014. Web. 17 Dec. 2015.x

Zukerman, Erez. "4 Ways To Read & Understand An End User License Agreement (EULA) More Easily." *MakeUseOf*. MakeUseOf, 13 Oct. 2011. Web. 17 Dec. 2015.