Abstract

Data protection legislation is an area that has become more talked about in the current times in the United States. With the advent of the secret documents leaked by former intelligence analyst Edward Snowden, and the quick-to-follow data breaches of two major corporations, potentially affecting around 160 million Americans, the time to discuss and understand this topic is now. The in-depth understanding of US data protection laws present significant issues therein. There lie holes and fissures, as a matter of speaking, the framework that results in the lack of user protection. How then can these holes be mended, and what are the proposed solutions? In order to resolve this case, this research first understands another framework by which to compare the current US framework. When compared to the US framework, which pieces appear to be missing from the US? By analyzing the results and research of law professionals, the discovery is that the US could benefit from a cohesive law, which would protect the fundamental right of citizens to have private data protection and the proper representation. Additionally, there needs to exist, in the least, one organization which holds authority over individuals who breach this right; the EU refers to these as Independent Supervisory Authorities (ISAs). The implications of these findings highlight the urgency to provide this fundamental right to US citizens. Where the right to privacy fails is to say that there is a fundamental right to have that right protected.

Introduction

Since the rise of the World Wide Web, data sharing and information travel has boomed. This has afforded the world some incredible amenities and opportunities never seen before: companies are now able to be connected world-wide instantly, education and knowledge is available at each person's fingertips, and communication has been simplified in ways we never thought possible. However, with these amenities come the evils of the internet phenomenon. The convenience of the internet and its amenities has led to the influx of personal and private data into company and corporate data stores, which are accessible through the web. Internet usage is a means for companies to collect personal information, and often that information is used for their profit by selling it to partners and third parties for profit. With the rise of computer security threats has come the awareness of data protection legislation in the United States.

One major event that spurred the discussion of this topic, and indeed the authors interest in this field, was the events that unfolded as Edward Snowden leaked the classified documents about the bulk collection of US citizens' data (BBC). In June of 2013, Snowden single-handedly shook the world by exposing incriminating evidence that the US had been and was continuing to collect bulk data under the provision of a bill passed in 2001: the very well-known Patriot Act (BBC). Moreover, this discussion

was catalyzed by two major information security breaches: in December of 2013, major US retail company Target realized that attackers had gained access to records that affected up to 70 million people (Data); similarly, in January of 2015, Anthem, United States' largest health insurance company learned that their systems had been breached, an attack that possibly affected over 78 million people (Humer).

However, this rise in awareness has yet to translate into a cohesive data protection framework that can be seen in other parts of the developed world, such as the European Union. The United States does not have in place the complete legislation that does exist for citizens of European states. This lack of cohesion provides problematic fissures in the current legislation which is intended to protect the citizens of the US. How, then, could these fissures be mended and repaired to provide the complete coverage necessary to the citizens of the United States? There must be several questions addressed in the research in order to determine the nature of the problems within the United States' framework, and to suggest the remedy for these issues. The proposed method is to study a framework in comparison to that of the US. In this writing, the European Union's Data Protection Directive, which has now been simplified to the Data Protection Regulation, will provide the necessary foundation upon which the US' framework may be reviewed and criticized. With this Directive in mind, the next area to address will be in which ways the US is currently protecting its

citizens. Lastly, with the two systems held in parallel, the last question to be addressed will revolve around which ways the US should strive to redress their current state.

In order to determine the means necessary to provide a cohesive legislative resolution to the problems that lie in the United States' current data protection laws, an example case must first be examined and studied. This paper will explore the European Union's current laws and determine the nature of its legislation. By reviewing these laws, the reader can begin to build foundation of data protection laws. The intent for this is to better understand laws that are present today. The examination of the laws of EU depicts a cohesive and complete law framework. This will serve as the benchmark by which this paper will seek to review the US laws.

Following the full review of the EU law framework, will be an overview of the currently existing framework within the United States. This overview will be followed by the review of several federal acts that seek to augment the United States' data protection law framework in each industry. These laws will highlight some of the issues that lie within the framework present in the US. Continuing to understand the US framework will allow the comparison the two reviewed frameworks.

The last step in determining how the fissures which are present in the US data protection framework is to provide expert opinion on the ways in which the US should modernize its current system. This section will review the writings of one professional

law practitioner on his suggestions for redress. Specifically, author Joel Reidenberg addresses the current state of the US patchwork in terms of the current European Union's framework. Therefore, the information provided in the previous sections will allow the reader to understand why the necessary changes should be implemented to fill the problematic holes within the United States' data protection framework.

European Union Data Protection Laws

The first area to review and understand is the European Union's (EU) view of data protection and privacy. The EU provides a blanket law that covers all of its citizens in a unified manner. Moreover, the EU provides a defense for the data subject against the controller, or the entity which is collecting data. As will be later shown, this is not the case in the United States. The US has a patchwork and piecemeal approach, with attempts to encourage self-regulation. The EU provides data protection and privacy as a fundamental right to its citizens, and goes even further to require that even other countries who may be processing their citizens' data must follow these laws, this is what is commonly referred to as Safe Harbor in the US. Exploring these laws will provide a clear example by which to contract the US laws that are currently in place. This will also provide a means by which to suggest improvements to the current patchwork of US laws.

European data protection laws seek to unify the protection of its citizens' data while also allowing the free flow of data according to the groundwork laid by the EU Data Protection Directive, or the Directive for short. While it seeks that data may flow freely, it is first concerned with the unity in protecting its citizens' privacy. All members of the Directive must make the laws complete. They have very little ability to maneuver within the implementation of the Directive (Luxembourg 18). Additionally, the Directive provides the data subject, or the person whose data is being collected, with explicit rights. Those rights serve to be protected and they serve to maintain the correct use and general correctness of the user's data. Key rights of the data subject include: the right to access; the right to have the data rectified; and the right to have any data blocked or deleted if the controller, or the entity that has acquired and now holds the data, gathered the data illegally, or it is incorrect (Luxembourg 105).

Right to Access

Data subjects have the right to access what is being processed by the controller within limitations (Luxembourg 107). Those items that have been deemed appropriate for the data subject to know will allow him or her to determine, whether the data is accurate. The EU law handbook lists the following as what the subject may obtain from the controller:

- Purpose of the data processing by the data controller

- Categories of data that the controller will be processing
- What data is undergoing processing
- Recipients or categories of recipients of processed data to whom the private data is disclosed
- Any available information about the source of the data being processed
- Logic involved in any of the automatic processing

Additionally, the individual states within the EU have the ability to increase what the controllers are responsible for to their citizens. An example of this is that the states may require that the controller add necessary information so the data subject can assure that the information is accurate. Simply providing that "name, address, and birth date" information was collected may not be enough. The controller may also need to provide what the content of that information is so that the data subject can check the validity of that information (Luxembourg 107-108)

Right to Rectification, Erasure and Blocking of Data

Following the right of access is the right of rectification. The right to rectification is the result of the necessity that data must be accurate, as in the data subject has the right to have correct information available, per the example mentioned above. Complementing the data subject's right to rectification is the protection of the subject's burden of proof. The case presented by the EU sows that the collector may be in

violation of Article 8 if the proof for which they ask presents "an insurmountable barrier" to the subject. Data subjects also have the right to request contested inaccuracies be blocked or annotated during disputes or in the even that data may be of some harm during the litigation (Luxembourg 113). This right serves to protect the data subject from inaccurate data and the burden of proving those inaccuracies.

Independent Supervision

Under the Additional Protocol to Convention 108, independent supervisory authorities (ISAs) are mandatory in Europe. The ISAs are in place with specific tasks and are guaranteed the authority to uphold them. The authorities must act with complete independence. Authorities, according to the EU handbook must:

- Monitor and promote data protection
- Advise data subjects
- Hear complaints
- Supervise Controllers and Processors
- Intervene if necessary
- Refer matters to court

And there are additional responsibilities of the ISAs in addition to these mentioned (Luxembourg 113-118).

The overview of the EU data protection laws allows the reader to view into the workings of the EU laws that protect the data of EU citizen. EU laws seek to hold controllers and processors accountable for the use of the data subject's data, and it seeks to make them responsible for the removal and accuracy of the data collected. By implementing several rights and procedures, the EU uses the ISAs to police the controllers and represent the data subjects. The rights of the data subject reach further than even the ones addressed here, as they are out of the scope of this material, but it is noteworthy that the fundamental right of data protection leads to several rights to the data subject. It is also important to mention and realize that the laws present in the EU do not seek to stop the flow of data and information; indeed, the desire to allow free flow of data is stated clearly in its guidelines; however the main goal of the Directive is to protect the data subject before protecting the flow of data. After reviewing the US privacy laws, there will be a review of the missing components as compared to the EU laws.

United States Data Protection Laws

The United States' data protection laws that exist for its citizens are certainly more piecemeal than the laws protecting the EU citizens (Jolly). This review of the laws in place in the US serves to provide the reader with the necessary background of current laws and their extent for the purpose of understanding the forthcoming

comparative analysis to the aforementioned EU laws. This overview is a summary of several of the pieces that comprise US data protection.

Overview

It is wise to understand that there is no comparable law in the US to that of the EU's Directive. As practicing lawyer Ieuen Jolly states, the US data protection laws consist of a "patchwork" of state and federal laws by which the US encourages "best practices" in an effort for self-regulation (Jolly). Often, these laws will overlap, but they can even contradict one another. To understand the direction for the following section is crucial to understand that fact. Here the "patchwork" will be examined by reviewing several of the major laws within US data protection. Once this section provides the necessary background, the two systems, EU and US will be compared with the attempt to clarify some areas of need within US data protection.

Federal Trade Commission (FTC) Act

This act is a general provision for most of the companies which do business in the US; however, there are certain industries to which this does not apply as there exist other entities with the assigned authority for their regulation (Jolly). The Federal Trade Commission Act exists to protect consumers from unfair or deceptive practices (Jolly). This act empowers the FC with authority to perform several clearly defined roles. First, the FTC is empowered to investigate persons partnerships, or corporations except those

outside the jurisdiction of the FTC (Dictionary). Next, the FTC may then compile reports of the aforementioned entities (Dictionary). The FTC must investigate the compliance with antitrust decrees, as defined in the FTC Act (Dictionary). Lastly, the FTC must make and advise the readjustment of the entities mentioned prior (Dictionary).

The small overview of this act reveals its focus inward on the entities over which the FTC reigns as authority. This sets the precedent for the nature of the laws in the US. The laws focus not on the individual; however, they focus on the entities which would be referred to as "collectors" in the EU law framework.

Financial Services Modernization Act (Gramm-Leach-Bliley Act)

Continuing to the next piece in the US privacy law quilt is the Financial Services Modernization Act, also known as the Gramm-Leach-Bliley Act or, simply, the GLBA. This act stems from the desire to modernize the financial industry from regulations made during the Great Depression to reduce the control that banks could have over other companies, and to mitigate the ability of banks to act as holding companies for entities in other industries, creating a boundary between industries (Jolly). It is important to know the historical significance of this act in order to understand that this does not solely focus on privacy; however, it does make some regulations, and is therefore widely used for financial industry information protection guidelines (Jolly).

The GLBA regulates, therefore, information protection in the financial industry by requiring specific guidelines be followed by institutions over which it has authority. To begin, the institutions must provide notice of privacy practices to its customers and some means for the ability to opt out of data collection (Gramm). However, the customer is limited in that it can primarily only stop the trading of information to outside the corporation (Gramm). If, for example, a bank holds another type of company within its corporate family, the customer has no say about the sharing within that corporate entity (Gramm).

The review of this act furthers the example that the US data protection laws in place focus on the business entities over which they have regulatory authority. A law that's main goal is to deregulate the merging ability of banks with other industries is the main source of financial institution data protection legislation. During research of this law, there was no mention of the burden of proof for inaccurate information, or even for the right of an individual to know the exact information collected or being used.

Health Insurance Portability and Accountability Act (HIPAA)

Arguably the most well-known, and most regulated privacy and data protection act in the US is HIPAA. This act regulates, monitors, and enforces healthcare information protection in the US. It regulates the rights and responsibilities of patients and providers respectively. HIPAA seeks to provide data protection to the patient for

all Private Healthcare Information (PHI), but also allow for the proper flow of necessary PHI to the necessary healthcare professionals (Summary 2).

HIPAA guarantees several rights to the patient as specific provisions. Similar to some of the elements of the EU directive, HIPAA assures the right for patients to access and copy PHI held by the entities covered with HIPAA (Medical). Additionally, the individuals have the right to request amendments to the aforementioned PHI (Medical). Individuals have the right to request an account of all disclosures made to anyone without the individual authorizing disclosure (Medical). The individual has a right to request a notice of privacy practices (Medical). However, HIPAA does allow the provider to release healthcare information to caretakers as necessary for the best interest of the patient without explicit consent (Medical).

HIPAA seeks to strike a balance between protecting the patient, but being sure the provider is able to properly care for said patient. With high stakes, such as $250,000 fines or 10 years of imprisonment, if the act is violated, HIPAA compliance is strictly adhered to in the healthcare industry. It is noteworthy to point out the similarity between HIPAA and the EU Directive in that there is the attempt to strike a balance between data flow and data protection. Any suggestions made for the US law framework should also consider this balance as paramount to its success; however, the balance should lean with the side of the data subject, and seek to protect it.

Children's Online Privacy Protection Act (COPPA)

That last piece of the US privacy law patchwork that will be reviewed is the Children's Online Privacy Protection Act or COPPA. To begin, the act defines a child as any individual under the age of 13 (Regulation). This act provides clear restrictions to the operator, as in the operator of any system that is seeking to collect children's data, and rights to both the child and parent or guardian of said child.

First, to items must be met by the operator seeking to utilize the data of children: it must provide a notice of how the data is or will be collected, what data will be collected, and how the data will be used (Regulation). Next, the operator must obtain "verifiable" consent from the parent or guardian as defined in the COPPA (Regulation).

Addtionally, the parent or guardian is afforded several rights regarding this protected data. First, the operator must provide a description to the guardian about which type of information is collected (Regulation). Secondly, the operator must provide the parent's right to refuse the collection of the data. It is noteworthy, that COPPA does protect the operator by allowing it to terminate services upon the denial of parental consent (Regulation). Lastly, the operator must meet the right of the parent to have "reasonable" opportunities to obtain the information gathered (Regulation). Addtionally, the parent may have this data deleted in some cases (Regulation).

COPPA concludes the discussion of the US data protection laws that are being reviewed in this comparison. After providing the foundational requirements necessary to understand the nature of US laws for data protection, the next section shall compare the EU laws to what is now in the US in an effort to better understand where there is need for improvement, and in hopes of suggesting reasonable additions based upon the knowledge of the European system.

Highlights of EU Data Protection Laws

European Data Protection laws provide the foundation to begin highlighting areas in which the United States does not protect its citizens. Law professor Joel Reidenberg presents these highlights in an article he wrote for the Wall Street Journal. With the foundation given by the overview of EU data protection laws, the following highlights serve to provide the holes within the US' data protection laws. As described by Reidenberg, the US has "piecemeal" laws.

First, it is important to view the US under the scope of the EU laws, as according to Reidenberg, the EU laws put the citizens first (Reidenberg). As mentioned and mandated by the Directive, privacy is a right. Data subjects in the EU have the right to certain fundamental information about what data is being collected, how, and how the automatic decisions are being made (Luxembourg). Reidenberg asserts that the US

companies control what data that they give an individual, and they are capable of revising policies after collecting an individual's data (Reidenberg).

Next, in the words of Reidenberg, "Redress is available." As explored prior, the Directive provides the data subject with clear rights to rectification of inaccurate data (Luxembourg). Moreover, the burden of proof is not unduly placed on the data subject. The piecemeal approach used by US laws will protect users from some inaccuracies, while not others. As in health information illegally disclosed by a provider may be legally addressed, while if that same data is disclosed by a non-healthcare website is not protected by any laws (Reidenberg). This lack of consistency leaves a lack of trust according to Reidenberg.

Lastly, Reidenberg highlights another key area to the EU data protection laws: Independent Oversight. The EU has specific measures in place to assure that the ISA has the authority and responsibility to protect and serve the data subject. Here that is left to the subject, their ability to acquire legal counsel, and to prove the non-governed data was used illegally.

When finalizing the review of the EU data protection system in comparison to that of the US, it provides the areas that should be addressed in the US. In short, the US could benefit from a blanket law, such as the Directive in the EU, which serves its citizens with a unified law that clearly states their rights, the responsibilities of the

collector, and the means by which these regulations shall be upheld and enforced. Doing so would eradicate the need for a guideline for "best practices," as it would create a mandate of required practices. This could be augmented as industry authorities deemed necessary, but regulated independently by those authorities with the capability to do so.

Next, the US needs to focus on the rights of the individual citizen. Here, as mentioned by Reidenberg, the burden of proof in the US lies solely on the citizen, with no measures in place to create a means for the citizen to prove this, or to what extent. The EU has the ISA which regulate the Directive, and there are measures in place which clearly state that the individual does not hold sole burden to prove that the data collected is inaccurate or illegally acquired. The US would benefit from a similar measure.

Conclusion

In conclusion, the purpose of this thesis was to review two data protection and privacy law frameworks, that of the European Union and the United States, in order to compare how they are structured. This thesis provides an overview of both the European Union's privacy law framework and that of the US. It does so with the intent to better understand the inner workings of the systems to attempt to provide a suggestion about the future needs of the US data protection legislation. The cohesive

nature of the EU Data Protection Directive served as the basis for the discussion, through providing a complete and cohesive foundation to understand the necessary rights and restrictions within data protection law. In contrast, we reviewed what proved to be a particularly piecemeal system in the United States, as the data protection laws exist in the US as a patchwork of state and federal laws. Several of the most important federal Acts provided the reader with the necessary background information to understand the nature of the US laws in their current state. By reviewing both frameworks, this thesis attempted to contrast the two in hopes of highlighting problematic areas within US law, or areas which could use improvement.

Having reviewed both frameworks, the findings indicated two things: the EU data protection framework is a cohesive system which regards privacy and data protection as a fundamental right. Data protection laws are built upon this foundation, and augment the existing legislation. All states that are within the control of the Directive must maintain *at least* the regulations stated in the Directive. Additionally, the Directive provides the necessary authority for the ISAs to enforce these regulations, and serve the individual. In contrast, the findings about US laws proved that the legislation in the United States was not founded upon a single cohesive legislation; instead industries were regulated by individual federal acts, and state laws, which would sometimes contradict one another. The comparison, which attempted to provide suggestions for additions or improvements to the current US law framework, provided

the assertion that the US could benefit from a European-style data protection framework. This framework would contribute a basis for the fundamental right that is privacy and data protection in the world with sophisticated collection techniques, and rising risks. Additionally, it is crucial that the proposed addition seek to provide the necessary representation and rights to the individual, by not placing all burdens of proof upon him or her. This assertion would be the first step to augmenting the current US framework.

This thesis only began to scratch the surface in the astronomically large field of information privacy and protection law in the United States. The implications of the laws that need to be enhanced within the US go further than the leaking of embarrassing healthcare information, or marketing analytics collected by internet searches. The implications reach far into the world of transparency, and the role of the government to protect its citizens: not only from external military and ideological threats, but from the threats of companies capitalizing on information that should be fundamentally protected. This illustrates that the US needs to take a step, and draw a line in the sand to protect the information and privacy of its citizens by emphasizing and enforcing this fundamental human right. More frameworks should be reviewed; more legislation should be drafted; more companies and organizations should be held responsible for the possession and use of US citizen private information. The implications of this issue reach each citizen in the United States.

Works Cited

"15 U.S. Code § 6502 - Regulation of Unfair and Deceptive Acts and Practices in Connection with Collection and Use of Personal Information from and about Children on the Internet." *LII / Legal Information Institute*. Cornell University School of Law, n.d. Web. 30 Nov. 2015.

"Data Breach FAQ." *Target Corporate*. Target, n.d. Web. 30 Nov. 2015.

"Edward Snowden: Timeline - BBC News." *BBC News*. The BBC, 20 Aug. 2013. Web. 30 Dec. 2015.

"Essential Guide: EU Data Protection Regulation." *Essential Guide: What the EU Data Protection Regulation Changes Mean to You*. Computer Weekly, n.d. Web. 27 Oct. 2015.

"EU Data Protection Directive." *EPIC - EU Data Protection Directive*. Electronic Privacy Information Center, n.d. Web. 30 Oct. 2015.

European Union. European Commission. *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*. Brussels: European Commision, 2012. Print.

"Federal Trade Commission Act." *Dictionary of Marketing Communications* (2004): n. pag. Federal Trade Commission. Web. 30 Oct. 2015.

"Federal Trade Commission Act." *FTC.gov*. Federal Trade Commission, n.d. Web. 27 Oct. 2015.

"The Gramm-Leach-Bliley Act." *EPIC - The Gramm-Leach-Bliley Act*. Electronic Privacy Information Center, n.d. Web. 27 Oct. 2015.

"H.R.2048 - 114th Congress (2015-2016): USA FREEDOM Act of 2015." *Congress.gov*. United States Congress, n.d. Web. 30 Nov. 2015.

Humer, Caroline. "Anthem Says Hack May Affect More than 8.8 Million Other BCBS Members." *Reuters*. Thomson Reuters, 24 Feb. 2015. Web. 30 Nov. 2015.

Jolly, Ieuen. "Data Protection in United States: Overview." *Practical Law*. Thomson Reuters, 1 July 2015. Web. 27 Oct. 2015.

Luxembourg. European Union Agency for Fundamental Rights. *Handbook on European Data Protection Law*. Luxembourg: European Union, 2014. Print.

"Max Schrems v Irish Data Protection Commissioner (Safe Harbor)." *EPIC - Max Schrems v Irish Data Protection Commissioner (Safe Harbor)*. Electronic Privacy Information Center, n.d. Web. 30 Oct. 2015.

"Medical Record Privacy." *EPIC - Medical Record Privacy*. Electronic Privacy Information Center, n.d. Web. 30 Nov. 2015.

Reidenberg, Joel R., and Thomas H. Davenport. "Should the U.S. Adopt European-Style Data-Privacy Protections?" *The Wall Street Journal*. The Wall Street Journal, 10 Mar. 2013. Web. 27 Oct. 2015.

"Senate Passes FREEDOM Act, Ends NSA Bulk Collection." *EPIC - Senate Passes FREEDOM Act, Ends NSA Bulk Collection*. Electronic Privacy Information Center, n.d. Web. 30 Nov. 2015.

"Summary of the HIPAA Privacy Rule." (n.d.): n. pag. United States Department of Health and Human Services. Web. 30 Nov. 2015.

"U.S.-EU & U.S.-Swiss Safe Harbor Frameworks." *Export.gov*. United States Government, 9 Oct. 2015. Web. 27 Oct. 2015.

"U.S.-EU Safe Harbor Framework." *U.S.-EU Safe Harbor Framework*. Federal Trade Commission, 6 Nov. 2015. Web. 30 Nov. 2015.