2019

Privacy Law Disparities between the United States and the European Union

Brandon DeLuca
Pace University

Privacy Law Disparities between the United States and the European Union

Brandon DeLuca
Computer Science
Faculty Advisor: Andreea Cotoranu
Seidenberg School of Computer Science and Information Systems
May 8, 2019 Poster Presentation - May 2019 Graduation

Placeholder for Advisor Approval Page

Abstract

Data is the world's most valuable resource today. In the 21st century, big data has overtaken the world's commonly known large industries to become one of the most sought after markets, and companies pay to own this data (The Economist, 2017). Advertisements may have been targeted towards demographics such as race or sex in past years. However, in the digital age, the capability exists to push advertisements to the screens of specific users with known interests. This has been made possible, in part, by unregulated data collection practices across the globe, including in the United States and the European Union. Data collection practices, from the conception of the Internet until the present day, have been disregarding the consent of the user the data represents. This unregulated data collection practice was halted recently in the European Union with the passing of the General Data and Privacy Regulation. However, the practice remains of concern in the United States. This research aims to conduct a classic comparative analysis of the omnibus privacy laws of the United States and the European Union. The existing laws will be compared across the following variables: the right to be informed, right of access, right to rectification, right to erasure, right to restrict processing, right to data portability, and the right to object. Recommendations for improving the United States privacy legislation will be highlighted based on this comparative analysis.

Table of Contents

List of Figures and Tables

Introduction

The world's most valuable resource is no longer oil, but data. According to *The Economist* (2017), in the 21st century, big data has overtaken the world's commonly known large industries to become one of the most sought after markets, and companies pay any price to have this data. Advertisements and marketing in past years may have been specifically targeted towards demographics such as race and sex, but in the digital age, advertisements can be pushed to the screens of specific users with known interests. This has been made possible through unregulated data collection in both the United States and the European Union from the conception of the internet up until the present day. Such collection has been conducted while disregarding the consent of the user the data represents.

As soon as someone purchases a computer to access the Internet, they have established a footprint that is traceable forever. There are multiple identifiers such as a MAC or IP address, which can reveal information about the computer user. Every machine that has the ability to access the internet is equipped with a unique MAC address; this number/letter combination can reveal someone's precise device details such as computer model and operating system. After purchasing an internet connection from a service provider, the connection is given a unique IP address; this number can reveal the name of the internet provider and their general location (state and city). To emphasize their importance, consider the MAC and IP addresses to be the Internet's implementation of social security numbers and addressing systems.

Our digital world mimics many of the features of the physical world, including interactions and conversations between individuals. A person's digital footprint can be traced just as easily as following someone on the street and gathering information about their

whereabouts and habits. In the United States, the right to privacy in the physical world is mostly granted by the Fourth Amendment of the Constitution, which states “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.” (Constitution, 1787)

The Constitution of the United States is a living, breathing document. While the Founding Fathers did not have knowledge of the Internet, one could argue that their ideology should also apply to the Internet space. One of the most debated topics in technology today is the sanctity of data and the right to keep information private. The personal information stored on computers as well as the personally identifiable information (PII) stored on social media websites, should be kept private and only shared as intended by the information owner. However, this personal data is often packaged with a unique identifier, which replaces the owner’s name, and is sold to companies, such as marketing firms, looking to utilize the data to benefit their business.

Benjamin Franklin, one of the Founding Fathers of the United States, spoke strongly about the tradeoff between privacy and security. He has attributed the following statement: "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." Although Franklin’s words were expressed the context of protection against government overreach in the physical world, it does hold weight in the debate of privacy versus security in the digital world. Some of the amendments in the Constitution protect the individual’s and the state’s rights from the federal government. In addition, there is also an explicit clause in the Declaration of Independence stating that if the government is shifting in this direction, it is the right of the citizens to overthrow it. Most of the discussion surrounds the

government spying on its people. However, a larger issue is at stake; the government should implement regulations that do not allow companies to use people's data for financial gain without their consent. The lack of action on the government's side could have consequences as the data could easily fall into the wrong hands, and be manipulated in a malicious manner.

Increased public scrutiny has thrown the United States data privacy into the fray. At the moment there is no omnibus federal data privacy legislation; there are only regulating bodies and relatively vague rules for companies to follow. The conversation about privacy has been brought into the spotlight recently with the congressional hearings of Mark Zuckerberg, Facebook's founder. Many are calling for the United States to follow in the footsteps of the European Union with the passing of the General Data and Privacy Regulation, an omnibus federal level user data privacy protection law. Some states have already introduced privacy laws like that of the GDPR,. For example, the state of California introduced the California Consumer Privacy Act which has been informally referred to as the "almost GDPR in the US". However, the lack of federal support for privacy laws one leave companies unharmed when it comes to how they treat users' data.

In the United States, although there are no laws obligating them to do so, corporations often try to protect consumer data when it is purchased and sold. This technique is known as anonymization and hides the personally identifiable information that could trace an individual back to his/her data. There are many arguments against data privacy. With most social media platforms being publicly accessible at no cost, many describe the release of personal data as a rite of passage or a toll (Esposito, 2018). Privacy is not about keeping personal information under lock and key, but more so having the ability to choose which parts of our personal

information can be disclosed if any. Although data is anonymized through obfuscation techniques, data deanonymization is possible with the computational power and algorithms available today, rendering current methods of protection useless.

At DEFCON 25, Svea Eckert and Andreas Dewes demonstrated the application of Statistical Deanonymization. In a research paper by Arvind Narayanan and Vitaly Shmatikov from the University of Texas, it is stated that "the adversary can use background knowledge and cross-correlation with other databases to re-identify individual data records" (Shmatikov, Narayanan, 2008). This approach is validated by Angiuli et al.' using publicly available medical data to identify test subjects (Aniguli, 2013). Each URL someone visits often gives away some kind of identifier that can be traced back to them. For example, the only person who can manage the account settings of their own Twitter/Facebook page is the owner of that account; anyone can visit, but only the account owner has access to specific sections of the website. There is a plethora of publicly available information that can be paired with an existing dataset to extract the user; the Twitter API (application program interface) can be manipulated to examine things people are tweeting about and Google Maps stores the latitude and longitude of the person accessing the website.

In recent years, the United States and the European Union have taken different measures towards handling breaches of data privacy. This work aims to perform a comparative analysis of the differences in privacy laws and regulations between the two governmental bodies. While legislating the cyber world can be difficult due to technology changing at a rapid pace, legislative bodies could assist in building a strong foundation for the future.

Methodology

The differences in privacy laws between the European Union and the United States will be identified through a classic comparative analysis. This approach to research seeks to highlight key differences between the two cases. According to the writing center at Harvard Law, a comparative analysis must clearly define four elements, as listed below.

Frame of Reference is defined as "the context within which you place the two things to compare and contrast." The two countries will be juxtaposed solely on the privacy laws and regulations that are enforced by their respective federal level governments. The laws will be compared with the aforementioned seven rights. These rights are dimensions are defined by the GDPR, which is considered to be the worldwide standard of privacy by many sources.

Grounds for Comparison explain "the rationale behind [the] choice, and why [the choice] is deliberate and meaningful." The privacy debate is one of the most important debates of the 21st century, and the issue specifically needs to be addressed with more concern in the US. The EU and US were chosen for comparison as they are two of the largest world powers that also operate with a democratic form of government. The choice is also clear due to the drastic differences between the privacy standards currently in place; on one side, the EU is leading the world standard, while on the other side the US has minimal standards.

Thesis dictates how the objects of comparison will be compared, specifically whether or not they "extend, corroborate, complicate, contradict, correct, or debate" one another. The method used in this research will be an extension, with the goal to determine how the US can properly extend the protections of the GDPR into its own political and regulatory systems. Therefore, the comparisons will not be made on similarities but differences.

Organizational Schemes have two possible organizational schemes in comparative studies, text by text and point by point. Text by text is used when the two objects of comparison extend each other, and point by point alternates points about A with points about B. Since this is along the lines of a "lens analysis" in which one source is used to analyze another, the GDPR will be used as a standard to analyze US regulations, a text by text comparison is appropriate. The two sets of laws "are not strictly comparable," and the GDPR is "a tool for helping discover whether or not" the US privacy law and regulations meet standards and expectations.

Research Questions

1) What are the difference in privacy law between the European Union and the United States when comparing:

1.1) fundamental rights?

1.2) specific industries?

Literature Review

We surveyed the literature on differences between privacy regulation in the European Union (EU) and the United States (US). We highlight the critical aspects of the privacy of consumer data, the details and impact of the General Data and Privacy Regulation (GDPR) and privacy regulation in the US. According to a study in the US, "93% of adults say being in control of who can get information about them is important" (Pew Research Center, 2017). Most research on privacy discusses laws related to the rights of the consumers in the US and the EU.

With the US compared to the EU, we are aiming to highlight a key limitation of data protection practices, as well as policy flaws in US law.

Privacy and Anonymization

The anonymization of data has been rendered ineffective in the obfuscation of data. Such limitations are due in part to technology-related factors, including the availability of computers with high processing power and the structure of web addresses (URLs). In the article "*Big Data Analytics and the Right to Privacy*," anonymization of data is discussed. The article states "Privacy is explicitly stated under Article 12 of the Universal Declaration of Human Rights and is seen as an enabler of other communication rights..." (Winter, 2017). In some jurisdictions, laws require that sensitive data be stripped of PII; this renders data as just information without having a name attached to it. However, the sophistication of the tools used to mine data makes it possible to re-identify it quite easily. It is also difficult for legal protections on personal privacy to address the complexity of technical changes, especially in bureaucracy. Most data transferred over the Internet is personal information. In this article, medical researchers matched anonymized DNA sequences on Internet genealogy forums with other public data and were able to trace the data back to the person of origin. The article company goes on to explain that insurance companies may abuse such capabilities and utilize deanonymize big data to charge different insurance rates to people with medical conditions or creating profiles for refugees.

The journal publication "*Privacy and Security in a Digital Age"* is a question and answer dialog with Gus Hosein, the executive director of Privacy International and former UN advisor on terrorism and human rights. He states that "The United States is fairly advanced in the legislative debate over surveillance. However, it is very backward in the protection of privacy

and of the rights of individuals and their data." (Marciniak, 2017) Another interesting point he makes is that private companies do not have the right to refuse to provide information to the government. Part of the reasons it is not regulated in the industry ties back to this gap. The journal states that "For the most part, we think that companies are just using our data to help us be customers and to make us happier. But the reality of how we increasingly see data being used is that, firstly, companies are very happy to profit off your data by selling it to other parties."(Marciniak, 2017).

Deanonymization techniques, whether they be algorithm based or critical thinking based, have proven to be extremely successful. On March 23, 2017, the United States Senate voted to eliminate broadband privacy rules that would have required Internet Service providers to get consumers' explicit consent before selling or sharing web browsing data. When data is sold to companies, the PII is often obfuscated to protect the names of the people involved in the transaction/activity. This is similar to blurring faces on a reality television show when there is no consent. Whether or not this is legal, this is an unethical practice, as outlined by Jennifer Winter in her article "*Big Data Analytics and the right to privacy*." Winter's work as a scholar is dedicated to "documenting instances where citizens feel that their information has been inappropriately collected, used, or shared" (Winter, 2016).

Although one would argue that this kind of research would contribute to exposing corrupt individuals, Winter would argue that they are violating individual's rights. Such practices can be applied to data collected from all individuals, and not only data of individuals of interest.

As highlighted earlier, statistical deanonymization is easy to achieve. Data sets sold by companies are typically insufficiently obfuscated, allowing them to be reclassified to a person.

Deanonymization presents a significant problem as best practices for data protection are not being implemented across the industry, and there is no regulatory oversight.

European Union Privacy Law

The General Data and Privacy Regulation (GDPR) is the omnibus privacy law for the European Union. The GDPR was adopted in 2016 and went to effect on May 25th, 2019. The main goal of the GDPR was to regulate the way businesses collect and manage consumer data, as well as protect user privacy. In an article written for the ACM Magazine titled "*Weighing the Impact of GDPR*," Samuel Greengard describes the GDPR framework. According to Greengard, "The European Union takes the position that a person owns his or her data, and their privacy is a fundamental right that is basic to the integrity of a human being." (Greengard, 2018) The GDPR gives European citizens control over their data and establishes penalties for companies that do not comply with the law. The original law in the EU that the GDPR replaced is the Data Protection Directive (DPD) 95/46/EC, passed in 1995.

Europe's competition commissioner stated that you pay for the websites you use, such as Facebook, through data and advertisements; in summary, citizens data has value. The GDPR implements an OPT-IN system for data sharing; companies require explicit consent from someone to have control over their data. The penalties are strong, ranging up to 4% of global annual revenue. The article also cites strong opposition in the corporate world, which was be expected. It states that Siri, Alex, and Cortana add layers of complexity to the issue of maintenance of Personal Identifier Information (PII) and introduce additional compliance issues. Companies are also concerned that the GDPR could inhibit innovation by limiting how they handle data; they cited that they may need to have two separate databases – one for compliance

and one for needs. This article details the GDPR as an ethical checklist, not a law checklist; these are moral foundations according to the author. The strong response from the EU is attributed to a litany of security breaches and breakdowns, from Equifax to Cambridge Analytica. This article while well researched does not compare the EU with the US.

In a publication from the Journal of Accountancy titled "*Getting ready for the EU's stringent data privacy rule*," part of how the GDPR affects the US is reviewed. The GDPR replaced the DPD, which was passed in 1995 due to post World War II anxiety. The GDPR affects all companies that use personal data of persons in the EU, regardless of where that company is located. For example, even though Google operates out of the US, they are subject to GDPR when handling the search history of an EU citizen. While the article does not specifically mention this, companies can have two sets of rules: one in compliance with the GDPR for EU citizens, and one for everyone else (Journal of Accountancy, 2018). Just because a company operates in two regions does not mean it has to have one privacy policy for all its consumers. In accordance with the GDPR, companies must maintain detailed records of personal data processing activities and conduct yearly privacy impact assessments. All companies must also appoint a Data Protection Officer as an executive position. If a company is breached, it must report the breach to the proper authorities and all its customers within 72 hours or be subject to the aforementioned penalties. Individuals also reserve the right to request their data be permanently removed from a company's systems, even if they are no longer a customer.

An interesting comparison is drawn in the Journal of Healthcare Compliance October 17th titled "*Equifax Breach Affects 143M: If GDPR Were in Effect, What Would Be the Impact?"* According to the journal, "On September 7th, 2017, headlines around the world reported that

Equifax revealed that personal data of roughly 143 million consumers in the US, UK, and Canada had been compromised." (Journal of Healthcare Compliance, 2017). Equifax was subject to no repercussions other than attempting to maintain its consumer base through apologies and discounts on protection plans. The journal states that implications on the company would be significant and that a large portion of the fallout that followed the breach could have been avoided had proper policy been implemented. Notification obligations would apply in the EU's GDPR, even post Brexit; the deadline to report a breach to customers is 72 hours, however, Equifax waited months. The security breach timeline in the US is governed by state laws, with most stating "report in the most expeditious time possible," (Journal of Healthcare Compliance, 2017) which leaves room for interpretation. If Equifax had notified its customers earlier, customers could have changed bank account information and cancelled credit cards immediately to avoid identity theft. The journal states that breaches like these should be a "sobering wake-up call to multinational organizations collecting, processing, storing, or transmitting data." (Journal of Healthcare Compliance, 2017)

United States Privacy Law

According to a publication from George Washington Law entitled "*Implementing Privacy Policy*," the GDPR is considered a success for the privacy sector. The EU is the dominant influence in setting privacy standards that govern behavior by companies engaged in transatlantic commerce. The author notes that the US should learn from it and implement parallel ideas that align with the US government structure. Although the author does not discuss the differences between EU and US and where improvements can be made to privacy laws, he outlines how privacy is handled in the US in the present day. US privacy regulation has "overshadowed

consideration of how and by whom privacy policy should be formulated and implemented." (Hymen D. et al, 2018). The Federal Trade Commission (FTC) is the closest agency the US has to a national privacy authority. The author argues for a centralized system for creating a privacy policy, citing that "the development and implementation of US privacy policy are compromised by the murky allocation of responsibilities and authority among federal, state, and local government entities." (Hymen D. et al, 2018).

According to the author, privacy laws in the US perform two basic functions. The power to create these rules and regulations is mandated to the FTC. The first function is to restrict the collection and use of information about individuals, meaning to monitor circumstances in which service providers can collect information about their customers, use the information, and transfer the information to third parties. The second function is to ensure that consumer personally identifiable information (PII) is protected from unauthorized use. Although these appear to be good mandates, it is important to note that the US has no omnibus federal privacy law. The implications of this are monumental, as there is a disparity among laws at the state level leaving citizens scattered across the United States unprotected. Privacy in the US is mostly handled by interdependent organizations at all levels of government; success is determined by how well each institution handles their individual responsibilities. The only omnibus law the US has regarding citizen data is the Department of Justice's Computer Fraud and Abuse Act, which protects citizens from hackers seeking to commit fraud or steal identities.

A publication from New York University entitled "*Federal and State Preemption of Local Privacy Regulation"* discusses government surveillance, which is out of the scope of this research. However, some points the authors make are relevant to US privacy law and are

important to note. The article contradicts the George Washington Law publication in that it advocates for privacy localism, and encourages small oversight bodies to oversee different sectors of business as the solution. Local oversight agencies, acting on behalf of government offices, can provide parallel oversight for different types of businesses, like social media, medical, etc. (Rubenstein, 2018). Each business uses data for different reasons and may need to be regulated differently. In order to construct a framework for comparing the EU and the US on privacy, the debate between Federal and Local governments should be settled.

A magazine article from IEEE entitled "*User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection*," discusses the need for consumer data protection in the US following major ethical issues. The article states that "With the revelation that Facebook handed over PII of more than 87 million users to Cambridge Analytica, it is now imperative that comprehensive privacy laws be developed. Technologists, researchers, and innovators should meaningfully contribute to the development of these policies." (IEEE, 2018). The CONSENT Act, proposed by Senator Richard Blumenthal and Ed Markey, is similar to the GDPR in that it requires explicit opt-in from users before transactions regarding their data can be made.

According to an article by Lotrea entitled "*Mr. Zuckerberg and the Internet"* the power relation and the technological gap is discussed. In order to draft balanced and intelligent privacy regulation like that of the GDPR, national regulators should be educated.

Comparative Analysis

For this analysis, we use two terms: data subject and data controller. The data subject is any consumer that has their data collected. A data controller is any company/government agency responsible for maintaining and using data that they have collected (Jambekar, 2017).

The GDPR outlines seven fundamental privacy rights that should be guaranteed to consumers. In this study, these seven rights will be used as a baseline for comparison. These rights are listed below:

1) The right to be informed.
Companies must inform a consumer when their data is being collected, and what the purpose of it is.

2) The right to access.
After data has been collected, a user should be able to access what has been collected about them.

3) The right to rectification.
If the data that has been collected contains misleading or incorrect information, the user should be able to correct the record.

4) The right to erasure.
At any time the user should be able to request that data relating to them be removed, and the company must comply.

5 The right to restrict processing.
At any point after the time of collection the data processing rules change, which can be how it is being used or stored, the user must be informed and can restrict their data from being sent.

6) The right to data portability.
Allows individuals to obtain and reuse their personal data for their own purposes across different services.

7) The right to object.
The right to object to data processing.

To illustrate the comparison between privacy law in the US and EU, two tables were created. Figure 1 compares United States law and European law against the fundamental rights laid out in the GDPR. Figure 2, located on page 26, compares United States industry-specific law to the fundamental rights. Using this comparison, we can determine where the US falls short of protecting basic consumer rights in regard to data. The GDPR was chosen as the lens because it was written and passed in reaction to the growth of big data as an industry. Outlined in Articles 5-8, the GDPR states that "The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased." and "Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities.".

	Right To Be Informed	Right Of Access	Right To Rectification	Right To Erasure	Right To Restrict Processing	Right To Data Portability	Right To Object
United States Law	Not Covered - Right not Granted. Data processors may choose to inform/ ask for consent in their privacy policy to be transparent.	Employees are entitled to receive copies of data held by employers. Parents can receive copies of info collected about children under 13. Individuals can request medical records. Individuals can receive credit report information	Not Covered - Data Processors do not have to change data by law.	Not Covered - Data Processors do not have to delete data. State law in California allows for this, but not a federal law.	Not Covered	**Not Covered** - But not specifically a privacy issue. This is to ensure there is no vendor locking in regards to certain services.	Not Covered - CAN-SPAM gives you the right to opt out of emails and phone calls. GDPR has a different definition of objection
European Union Law	Article 12, Article 13, Article 14	Article 12, Article 15, Article 46	Article 16	Article 17	Article 18	Article 20	Article 21

Figure 1 - Comparison of Laws based on Fundamental Rights

Figure 1 Key
In Compliance
Partial Compliance
Not in Compliance

The GDPR guarantees each of the seven rights listed above. A key factor that was not included in the seven rights is consent, although it is partially incorporated in the right to be informed. Article 6 of the GDPR states that processing of the data subject's personal data is lawful only under circumstances in which the individual gives consent to the processing of the personal data for a specific purpose.

Recital 58 of the GDPR requires data controllers to provide EU citizens with details about how personal information is used and is often hailed as establishing the principle of transparency. This places the burden of educating consumers about their rights on corporations. Transparency and open government are fundamental ideas the US was founded on. As in a republic system of government, public officials are held accountable by the people. Authority figures are required to answer for decisions they make, in both the public and private. In this context, it appears natural for the US to adopt this approach to protect consumer data.

Research Question 1.1 - Comparison by Rights

Article 13 of the GDPR details the informing of the collection of data. It states that at the time of data collection, the data controller must provide the data subject with contact details, the purposes of the processing, legal basis for processing, the recipients of the data, and whether or not the controller intends to send this data to another company/country. The data controller must also state the period for which the data will be stored, and the existence of the other rights. There is no solidified legislation in the United States to cover this, and the FTC act is the closest thing but is regarded as abstract and subjective. The FTC Act established the eponymous agency and established their jurisdiction over the privacy realm, but the process for the creation of rules and policy was never clearly defined and for the most part, the FTC operates without any oversight.

Article 15 of the GDPR details the right of access by the data subject. At any point from the time of collection to the time of erasure, the data subject has the right to obtain the information collected as well as what it has been used for. Some of the information data subjects are entitled to include the purpose of processing and categories of personal data concerned. The right to "lodge a complaint with a supervisory authority" is also included; this can be to the Data Protection Officer (a new required position for companies operating in the EU) or the government. This also requires websites to allow its users to easily access their data, with a turnover time of 30 days. The ideas presented in this article are covered in fragments throughout specific agencies in the US, specifically relating to employee/employer relations, parents and children, medical records, and credit report information. There is no reason that an omnibus privacy law cannot apply this rule across all business areas, with the enforcing agent being the FTC.

Article 16 of the GDPR details the right to rectification. The data subject has the right to obtain and correct inaccurate personal data. This is done by means of providing a supplementary statement. Incorrect or misleading information can negatively affect data sets and their proper use, as well as may misrepresent an individual. Some companies that participate in data collection offer rectification by default, simply because incorrect data would undermine their mission. This is specifically important in the financial industry, where false credit score reporting and other incorrect information can lead to false financial instability. There is no US law to enforce the rectification of data, and for good reason, there should be one.

Article 17 of the GDPR details the right to erasure. The data subject has the ability to request the erasure of all personal data without delay. When the personal data is no longer

needed, the data subject withdraws consent or the data has been unlawfully processed. Withdrawing consent can be done at any time, so a general rule for this article is that the data subject has the ability at any time to completely erase their data from a system. Article 21 of the GDPR details the right to object at any point to data processing. California has implemented a great example of how the rights granted in the GDPR can be incorporated into the US at the state level by guaranteeing the right to erasure in the California Consumer Privacy Act. However, there is no law at the federal level to protect this right.

Article 18 of the GDPR details the right to restriction of the processing. The data subject has the right to know about changes to data processing and at any point after the time of collection, the data processing rules change, the data subject must be informed and can restrict their data from being sent. There is no US law to protect this right.

Article 20 of the GDPR details the right to data portability. The data subject can receive personal data regarding him or her in a commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance. After further analysis of this right, it appears to be less about privacy and more so an anti-monopoly law. A company should not be able to restrict a data subject from switching companies just because of the methods of data storage. This is a very similar concept to the tenure of software engineers; their code should be clearly documented so that it can easily be passed on to another employee in case of termination or leave.

Research Question 1.2 - Comparison by Industry

Right To Be Informed	Right Of Access	Right To Rectification	Right To Erasure	Right To Restrict Processing	Right To Data Portability	Right To Object
FTC Act (15 U.S. Code 41)	Fair Credit Reporting Act (15 U.S. Code 1681)	N/A	California Consumer Privacy Act (STATE LAW)	N/A	Health Insurance Portability and Accountability Act (HIPPA)	CAN-SPAM Act (15 U.S. Code 7704)

Figure 2 - Mapping Existing US Laws to US Industries

The general trend of the data gathered through research is that US data protection law is focused on the security of data as it relates to a specific industry, while the GDPR is focused on transparency, the lawful basis for processing, purpose, and data retention across all business practices. The US laws that are included in the chart are elaborated on below.

1) Gramm Leach Bliley Act (15 U.S. Code 6802(a)) – Protection of personal information in banks and financial institutions. Requirements for securing PII, disclosure, and notifying users upon breaches.

2) Health Information Portability and Accountability Act (29 U.S. Code 1181) – Protects information regarding health status or health care providers. Regulates collection and disclosure.

3) FTC Act (15 U.S. Code 41) – Bring enforcement against deceptive practices and failure to have clear published privacy promises.

4) Driver's Privacy Protection Act (DPPA) of 1994 (18 U.S. Code 2721) – Privacy of disclosure of DMV information. The DPPA regulates how info is released, including photographs, social security numbers, client identification numbers, address, telephone number, medical information, and disability information.

5) Fair Credit Reporting Act (15 U.S. Code 1681) – restricts the use of information on credit standing and reputation.

6) CAN-SPAM Act (15 U.S. Code 7704) – requires technical information to be included in unsolicited emails and permits consumers to opt out of emails.

7) Telephone Consumer Protection Act – regulates all calls and texts made for telemarketing to follow certain guidelines.

8) Children's Online Privacy Protection Act(15 U.S. Code 6501) – prohibits data collection on anyone under the age of 13.

9) Video Privacy Protection Act (VPPA) (18 U.S. Code 2710) – protect wrongful disclosure of video-tape rental or sale records.

Using the fundamental rights as variables, five out of the seven right are upheld in their respective United States industries. The industries that protect fundamental privacy rights are health insurance, finance, telemarketing, and any industry that handles the data of a child. The complications arise in that the rights do not extend across the industry; health insurance companies have to keep certain personally identifiable information private but others don't.

One key similarity between the GDPR and US law is the handling of children's data, specifical children under the age of 13. The GDPR states "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences, and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.", and almost identical ideas are present in the Children's Online Privacy Protection Act. Parental consent is required in both the EU and the US to collect data on children. The importance of this is the naivety of children, and the inability to make proper decisions regarding their personal information.

There are three government agencies that are responsible for privacy regulation in the United States, and these are the Federal Trade Commission (FTC), Office of Comptroller of the

Currency (OCC), and the Department of Health and Human Services (DHHS). The FTC's is an independent agency of the US government and its principal mission as described by their website is the promotion of consumer protection and the elimination and prevention of anti-competitive business practices. The OCC's principal mission is to charter, regulate, and supervise all national banks." The DHHS's principal mission, also described by their website, is protecting the health of all Americans. Each agency is the sole enforcer privacy regulations in their respective area of interest, with the FTC being a general oversight agency while the OCC protects bank and credit card records and DHHS protects medical records, as listed in the aforementioned list of US privacy laws. Other listed laws are regulations enforced without an independent oversight agency; they are rules for individual agencies to follow.

An omnibus privacy law is a proper solution to the US' disparity in the shifting world of privacy regulation. Although the US maintains a republic form of government with states operating as independent actors, as seen in the federalist approach by the founders, the rights granted to US citizens are maintained at the federal level. The GDPR states that "In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States." The purpose of this is to create a cohesive atmosphere in which companies have to operate the same way in all areas of the country and regardless of state, rights are ensured. This could be achieved in two ways, constitutional amendments or federal law passed by Congress. Amending the constitution requires a national convention, and can often be a lengthy and cumbersome process as opposed to drafting and signing the legislation.

Conclusion and Recommendations

The fundamental rights of consumers supported by the GDPR in the European Union should also be supported by laws in the United States. The comparative analysis breaks down the GDPR into seven variables to analyze where the United States succeeds or does not succeed in upholding privacy rights of consumers operating with financial institutions, healthcare institutions, or in online interactions and transactions. Of the seven fundamental rights, five are upheld in their respective industries. The industries that protect fundamental privacy rights are health insurance, finance, telemarketing, and any industry that handles the data of a child. The complications arise in that the rights do not extend across the industry; health insurance companies have to keep certain personally identifiable information private but others do not. By and large, the United States falls short of meeting the standards the same way the European Union does. In the context of the United States government, the Federal Trade Commission (FTC) could play a larger role in the regulation of privacy, and such administrative duties could be granted to the agency by congressional legislation. FTC fits the role as defined in their mission statement by Woodrow Wilson in 1914, outlining their role in the promotion of consumer protection and the elimination and prevention of anti-competitive business practices. The United States has a federalist system, and states are usually left to create laws for issues not explicitly stated in the constitution, but in the case of privacy, this has proven to be extremely ineffective. As it is a right, it is an issue that should be handled at the federal level. Research question 1.1 points out how well the GDPR, a federal level bill, is effective in ensuring the privacy of consumers. Legislation implemented at the federal level to regulate all industries will resolve a problem found in the analysis of question 1.2, which is the disparities between industry.

Some rights protected in only specific industries should extend to social media platforms and beyond. Implementing GDPR-esq legislation in the United States is expected to protect not only consumers but also prevent possible disaster due to the mishandling of information by private companies.

Works Cited

The world's most valuable resource is no longer oil, but data. (2017, May 06). Retrieved from https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

Satariano, A. (2018, May 24). G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog. Retrieved from https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html

How to Write a Comparative Analysis. (n.d.). Retrieved from https://writingcenter.fas.harvard.edu/pages/how-write-comparative-analysis

Top 10 Most Powerful Countries in the World 2019. (2019, January 06). Retrieved from https://improb.com/top-powerful-countries-in-the-world/

Greengard, S. (2018, November 01). Weighing the Impact of GDPR. Retrieved from https://cacm.acm.org/magazines/2018/11/232192-weighing-the-impact-of-gdpr/fulltext

Getting ready for the EU's stringent data privacy rule. (2018, January 01). Retrieved from https://www.journalofaccountancy.com/issues/2018/jan/eu-data-privacy-rule.html

Winter, J. (2016, February 13). Retrieved from http://www.waccglobal.org/articles/big-data-analytics-and-the-right-to-privacy

Lotrea, C. (n.d.). Mr. Zuckerberg and the Internet. An essay on power relations and privacy negotiation. Retrieved from http://compaso.eu/wpd/wp-content/uploads/2018/08/Compaso2018-91-Lotrea.pdf

Angiuli, O., Blitzstein, J., & Waldo, J. (2015, October 25). How to De-identify Your Data. Retrieved from https://queue.acm.org/detail.cfm?id=2838930

User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. (2018, August 16). Retrieved from https://publications.computer.org/computer-magazine/2018/08/16/user-data-privacy-facebook-cambridge-analytica-privacy-protection/

Rubinstein, I. (2018, March 01). Federal and State Preemption of Local Privacy Regulation. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124702

Hyman, D., & Kovacic, W. (2018, February 25). Implementing Privacy Policy: Who Should Do What? Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3123115

Ng, V., & Marciniak, D. (2018, July 04). Privacy: System Failure | An Interview with Gus Hosein. Retrieved from https://hrbdt.ac.uk/privacy-system-failure-an-interview-with-gus-hosein/

Equifax Breach Affects 143M: If GDPR Were in Effect, What Would Be the Impact? (n.d.). Retrieved from https://www.foley.com/equifax-breach-affects-143m-if-gdpr-were-in-effect-what-would-be-the-impact-09-12-2017/

General Data and Privacy Regulation (2018) (enacted).

Data Protection 2018 | Laws and Regulations | USA | ICLG. (n.d.). Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

Esposito, F. (2018, April 12). Cashless tolls: Welcome to the dark future. Retrieved from https://www.lohud.com/story/news/investigations/2018/04/11/cashless-tolls-dark-future/439131002/

Jambekar, S. (2017, October 04). GDPR: Data Subjects, Controllers and Processors, Oh My! Retrieved from https://www.twilio.com/blog/2017/10/gdpr-data-subjects-controllers-processors.html