Master's Thesis of International Studies

A Critical Juncture in Data Protection Standards

- Comparing Data Protection Legislation in the United States and the European Union -

데이터 보호 표준의 중요한 분기점

미국과 유럽연합의 데이터 보호 법률 비교

August 2020

Graduate School of International Studies
Seoul National University
International Cooperation Major

Kayleen Hyun Min Choi

A Critical Juncture in Data Protection Standards

- Comparing Data Protection Legislation in the United States and the European Union –

Advisor Sheen Seong-Ho

Submitting a Master's Thesis of International Studies

August 2020

Graduate School of International Studies
Seoul National University
International Cooperation Major

Kayleen Hyun Min Choi

Confirming the Master's Thesis written by
Kayleen Hyun Min Choi
August 2020

Chair	Kim Taekyoon	(Seal)
Vice Chair	Ahn Jae Bin	(Seal)
Examiner	Sheen Seong-Ho	(Seal)

Abstract

A Critical Juncture in Data Protection Standards

- Comparing Data Protection Legislation in the United States and the European Union -

Kayleen Hyun Min Choi

International Cooperation Major
Graduate School of International Studies, Seoul National University

In the last few decades, technology has faced an extraordinary evolution that has revolutionized the way we communicate. In particular, the rise of the Internet and digital platforms has turned data into an incredibly powerful, global resource. Yet, through the increasing sophistication of technology, the world now faces a major privacy dilemma, and governments must make critical decisions to determine whether established privacy laws encompass personal data on the Internet.

As leaders in technological innovation and privacy legislation, the world is looking to the United States and the European Union to establish standards in data protection. However, despite ideological similarities between the two powers, it is clear that the U.S. and EU have vastly different approaches to data legislation. On one hand, the EU has passed the most comprehensive and strictest data protection rules in the world, while the U.S. has struggled to institute uniform regulations. A sharp rise in

cyber-attacks and data misuse cases have led many to question why the U.S. has been unable or unwilling to legislate protection laws, while the EU has been quick to do so. With mounting public pressure, the U.S. now faces a critical juncture in its data policies, and must delineate its stance on data protection. In order to unpack the current approaches to data protection in the U.S. and the EU, this research will dive into the historical response to privacy and personal information through comparative analysis and case studies.

Keywords: Data protection, personal information, privacy, GDPR

Student Number: 2018-25674

Table of Contents

I. Introduction

1. Background

The notion of individual privacy has had a long and complicated history in the United States (U.S), dating as far back as the 19th century. In 1890, two U.S. lawyers Samuel D. Warren and Louis Brandeis published, "The Right to Privacy" in the *Harvard Review*, marking the first time that legal scholars in the U.S. advocated for a legal standard to privacy.[1] In time, this article became the founding argument for extended privacy laws in America, making a case for privacy as a fundamental right. Yet, since the days of Warren and Brandeis, aspects of privacy as a human right, and the degree to which privacy should be protected, has been hotly debated.

However, personal information and data protection has changed formidably since these initial conversations on the right to personal privacy. In particular, the prolific use of the Internet has changed conversations of data protection and data privacy. Due to the nature of its low-barrier access, billions of people have been able to use digital platforms to instantaneously communicate and exchange information. As a result, the Internet has built a global network of vast resources of individual user data that has evolved into an incredibly powerful resource. Yet, as more and more users began leveraging the benefits of the Internet, new pockets of security concerns have

[1] Samuel Warren and Louis Brandeis, "The Right to Privacy", *Harvard Law Review* 4, no. 5 (1890): pp. 193-220.

also begun to crop up. Navigating the balance between collecting data for technological automation, innovation and convenience, versus collecting data for illegal use and manipulation has become a moving target that lawmakers are grappling with. As the digital landscape continues to grow, so have the concerns regarding data protection, privacy, and cybersecurity.[2] Thus, legislation has been rushing to keep up with the quickly evolving technology scene.

One core issue on the topic of data privacy is tracking and collecting highly lucrative and private information of individual users. In recent years, the number of online identity theft and fraud cases has increased dramatically, exposing many peoples' personal documentation to Internet thieves. Yet, the elusive nature of the Internet has made cybercrime one of the most difficult types of crime to track and prosecute.

Additionally, the Internet has led to a moral and legal dilemma between ethical versus illegal activity in the field of data usage. For example, political campaigns can gather online information, such as a person's location and political preferences, to target specific voter messages to people on the Internet. In other cases, advertisers may leverage online data to message specific users about a clothing sale and encourage users to purchase an item. While these instances are hardly examples of nefarious activity, the 2016 Cambridge Analytica scandal in the U.S. heightened the impact, and

---

[2] Rachel Finn, David Wright, and Michael Friedewald. "Seven Types of Privacy." Essay in *European Data Protection: Coming of Age*, 3–32. Dordrecht: Springer Netherlands, 2013.

potential consequences, targeted messaging could have on democracy. With little regulation of Internet data, and the increased sophistication of digital technology, the landscape of acceptable levels of personal data collection has changed. Cyber-attacks are on the rise, and governments are facing increased pressure to make critical decisions to online privacy and data regulations.

With that context, this research aims to unpack the differing approaches to data protection and privacy regulations by comparing and analyzing legislation in the U.S. and the European Union. In particular, this study aims to use this analysis to understand why the U.S. has failed to pass comprehensive federal legislation on data protection. Undoubtedly, the U.S. has faced multiple data breaches, bringing major concerns regarding data manipulation and digital privacy laws to light. Yet, the U.S. has hesitated in creating federally mandated protection laws to absolve privacy concerns. On the other hand, the European Union has successfully passed the strictest and most comprehensive data protection regulation in the world through its 2018 General Data Protection Regulation.

2. Literature Review

2-1. The case for data protection

With the onslaught of new digital devices and Internet services, experts and policy makers have made it clear that the need for cyber security and legislative standards in data protection is a necessity. From digital banking to social media,

Internet users are constantly uploading and sharing personal data online, with information ranging from a current location or date of birth. With this, the volume of personal information shared on the Internet has increased exponentially. Even more, login systems for social media platforms and banking services often require multiple layers of very personal information. A Pew Research study found that in 2019, 6 out of 10 U.S. adults believed it to be impossible to go through the day without having information collected about them by either a private company or the government.[3] Our daily routines so often involve tasks, such as checking email, social media, and online banking accounts, that it feels impossible to live in the twenty first century without some entity collecting personal data. Internet services have become so tightly incorporated with daily life that many people have become dependent on digital platforms to complete daily necessities. Furthermore, widespread smartphone and credit card usage has allowed for more intimate play-by-play tracking of peoples' daily activities. This information is eventually all stored and tracked in digital systems, and leveraged by private or public entities.

Furthermore, the Pew study found that the majority of American adults believed that the risks associated with personal data collected by private companies and the government outweighs the benefits.[4] In fact, a 2015 Pew study found that 74% of Americans found it "very important" that they be in control of *who* collects

[3]Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica Turner. Pew Research Center, November 2019, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information." P.2

[4] Ibid, p.7.

information about themselves, and 65% found that it is "very important" for users to control *what* information is collected on them.[5] While many understand that data collection is inevitable due to the integrated nature of technology in everyday lives, people are still concerned that individual privacy can be exploited in potentially harmful ways. In other words, American adults do not feel confident that the current digital protection measures will adequately safeguard them from future fraud or data misuse.

Thus, most Americans are in favor of legislation changes to protect their data. In fact, 68% of Internet users in the U.S. believe that current laws are ineffective in protecting their online privacy, and 64% believe that the government should do more to protect peoples' privacy online.[6] This is a staggering percentage, and sheds light on the need for change in America's data protection policies.

2-2. Increases in digital data misuse and cyber crime

Data breaches have always posed a consistent problem to record systems, stemming as far back as to the very first time private companies and governments began storing any personal information from the public. However, due to the salient

[5] Mary Madden, and Lee Rainie. "Americans' Attitudes About Privacy, Security and Surveillance." Americans' Pew Research Center. Accessed April 18, 2020. https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/, p.4.

[6] Lee Rainie, Sara Kiesler, Ruogu Kang, and Mary Madden. "Anonymity, Privacy, and Security Online | Pew Research Center." Anonymity, Privacy, and Security Online. Accessed May 18, 2020. https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/

use of modern technology, our dependency on digital systems has increased user vulnerabilities to data misuse or infiltration. In fact, the number of data breach cases and cyber-attacks has increased exponentially over time since 2005. Some statistics show that there were 157 data breach cases reported and 66.9 million records exposed in 2005. As shown in **Figure 1** below, there has been an astronomical increase in data breaches since 2005, and across multiple verticals.

Even more alarmingly, in 2019, statistics show that there were 1,473-recorded breaches and over 164 million records exposed.[7] The number of data breaches in less than two decades increased nearly 10-fold, most likely due to the increase in digital social services. For instance, Facebook launched in 2004, and other social media and online retailing sites boomed in the mid-2000s. As a result, the volume of personal information uploaded onto online systems increased, as did attempts to capitalize on digital vulnerabilities.

[7] Julianna De Groot. "The History of Data Breaches." Digital Guardian, October 24, 2019. https://digitalguardian.com/blog/history-data-breaches.

U.S. Data Breaches 2005 to 2017

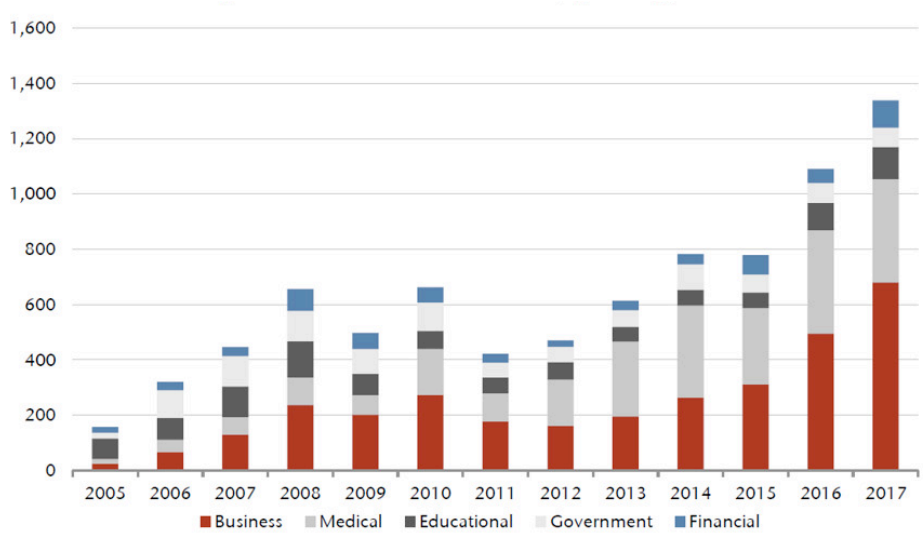

Figure 1. Sharp increases in data breaches from 2005 to 2017

Bar graph by Marketwatch 2018[8]

2-3. Legislative response in the U.S.

While cybercrime and cyber security are not novel concepts, the expansive and global nature of cyberspace has made the issues on the topic a growing and moving target. Even the concept of cyberspace itself has been defined and redefined over a dozen times by the U.S. Department of Defense.[9] For years, there have been major personal information data breaches in the United States, and valid concerns that the

[8] Victor Reklaitis. "How the Number of Data Breaches Is Soaring - in One Chart." MarketWatch. MarketWatch, May 25, 2018. https://www.marketwatch.com/story/how-the-number-of-data-breaches-is-soaring-in-one-chart-2018-02-26.
[9] P. W. Singer, and Allan Friedman. 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press, 13.

government lacked appropriate legislation and adequate safeguards to mitigate data abuse. However, what many people don't know is that the case for more comprehensive data protection laws has remained a constant in U.S. legislation since the 1960s. During this time, the concept of privacy became politicized as concerns over consumer privacy began to grow. Then, in the 1970s, the Information Age brought more traction to data protection policy as data automation became more and more commonplace.[10] Concerns for potential privacy infringements came to the forefront, and data as a tradable commodity began to grow. Today, data and information is so valuable that some American experts argue that the value of data could be more valuable than oil.[11] While it is difficult to quantify and directly compare a physical commodity such as oil to a virtual one such as digital data, big data has definitely proven to be valuable.

This increase in automated data and the need for regulation led to the United States Department of Health and Human Services to create an advisory committee to draft principles of Fair Information Practices. These set of practices, "describe how an information-based society may approach information handling, storage, management, and flows with a view toward maintaining fairness, privacy, and security in a rapidly

[10] Manuel Castells. "Technology, Society, and Historical Change." Essay. In *The Rise of the Network Society (The Information Age: Economy, Society and Culture, Volume 1) (Vol 1)*, 5. Malden, MA: Wiley-Blackwell, 1996.
[11] The Economist. "The World's Most Valuable Resource Is No Longer Oil, but Data." The Economist. The Economist Newspaper. Accessed March 25, 2020. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

evolving global technology environment."[12] In addition, these principles included the following principles:[13]

(1) Transparency/openness: There must be no personal data record-keeping system whose very existence is secret
(2) Individual Participation: There must be a way for an individual to find out what information about him or her is in a record and how it is used
(3) Purpose limitation: There must be a way for an individual to prevent information about him or her that was obtained for one purpose from being used or made available for other purposes without his or her consent.
(4) There must be a way for an individual to correct or amend a record of identifiable information about him or her.
(5) Data quality/integrity: Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

The Fair Information Practices and its five principles eventually influenced the creation of the 1974 Privacy Act, which worked to hold government agencies that collected,

[12] Pam Dixon. "A Brief Introduction to Fair Information Practices." Blog, 2006. https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/.
[13] Stephen D Gantz. *FISMA and the Risk Management Framework: The New Practice of Federal Cyber Security*, 2013.

used, and maintained individuals' information responsible to its constituents. By all accounts in the 1960s and 1970s it seemed that the U.S. was making strides as a leader in safeguarding personal information, and was on its way to empowering its citizens to take control of their personal online information. The U.S. recognized the need to regulate data while balancing the government's role in data privacy. However, it's clear that the U.S. eventually came to a stalemate in making further progress, leading to detrimental consequences for future online users. As of today, some of the largest data breaches of the twenty first century have been targeted to U.S. citizens.

For example, in 2015, the political consulting firm Cambridge Analytica illegally gathered the personal information of over 87 million Facebook users for commercial gain and political microtargeting.[14] The United States Federal Trade Commission (FTC), the only federal agency that oversees data protection and privacy laws in the U.S., found Facebook guilty of violating consumer privacy. As a result, Facebook was ordered to pay $5 billion – the largest penalty in history for this type of violation found by the FTC.[15] This case shocked the American public, and public outcry for greater government regulation increased.

Yet, despite multiple reports of data breaches and calls for government support, the United States has yet to create federally mandated data protection laws. Instead, the U.S. regulates data protection through a muddled patchwork of regulations. For one, legislation is generally done on a state-by-state basis with varying

[14] J. Isaak and M. J. Hanna, "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," in Computer, vol. 51, no. 8, pp. 1 August 2018.
[15] Ibid.

levels of protection. In some states, data protection laws are nonexistent. Any federal-level legislation is done on a sectoral basis, and the FTC is the only federal agency to oversee regulations. Undoubtedly, this has led to fragmentation and confusion in data protection at both federal and state levels. As a result, private companies are unsure on how to legally operate across multiple states, and individual users are unaware of their legal data rights. Even more, the United States has yet to properly and explicitly define "data protection" leading to even greater hesitation in litigating digital privacy concerns.

2-4. Legislative Response in the EU

The EU has had a long history of incorporating privacy laws and data protection into its legislation. In fact, these concepts were borne out of the trauma of World War II, in which data and personal information were weaponized. During the war, European countries experienced how personal information could be exploited for discriminatory actions against minorities.[16] In fact, early data processors during World War II were used to create census cards that would contain an individual's nationality, religion, profession, and native language – all of which were eventually used by Nazi Germany to segregate, discriminate, and attack the Jewish population.[17] In the aftermath of the historical horrors of the War, Europeans vowed to regard and uphold individual information and privacy as a basic human right.

[16] Olivia B Waxman. "GDPR-Disturbing History Behind the EU's New Data Privacy Law." Time. Time, May 24, 2018. https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/.
[17] Ibid

Since the War, the EU has taken regulatory steps to ensure personal information is protected in its legislation and legally viewed as a fundamental right. Perhaps one of the most important steps towards greater data protection in the EU occurred under the 'Lisbon Treaty of 2009'. This treaty established a European Constitution and incorporated data protection into its framework. Under the Constitutional treaty, data protection is recognized as a basic right as stated in Article 16:[18]

(1) Everyone has the right to the protection of personal data concerning them

(2) The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

This marked a huge step for the EU, as it officially elevated data protection as a basic human right.

[18] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (OJ C 306, 17.12.2007)

In addition, the EU further legitimized data protection and privacy under the 'Charter of Fundamental Rights of the European Union of 2000'. Through this Charter, the EU granted its citizens the right to data protection by enacting rules that would enforce personal data collection to be "processed fairly for specified purposes, and with the individual's consent, or some other legitimate basis laid down by law supervised by an independent body."[19] The Charter of Fundamental Rights of the European Union further outlined the rights EU citizens have over personal data, and initiated a consent clause to the law. Both the Charter and the Treaty of Lisbon marked legally binding provisions for individual data protection that would be enforceable in the EU, its institutions, and all Member States.

[19] CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION, 2012/C 326/02

II. Research Plan

1. Research Question

Passing legislation on an ever-evolving topic as complicated as data protection and privacy is undoubtedly a difficult task. However, globalization and the increased use in technology has brought the world to a critical stage in data protection, and countries are now desperately looking for ways to safeguard the public from data misuse. As shown in the literature review, cybercrimes have increased alongside Internet use, and people are becoming more and more concerned with the lack of data protection.

For the past century, the U.S. and EU have been leaders in policy issues regarding newly emerging threats, and these issues in data privacy are no exception. With some of the biggest technology companies based in the U.S., the world is looking to the country as a leader in handling data protection legislation and forging new global standards. Furthermore, the U.S. has experienced some of the largest and most public data protection failures in recent history, further reiterating the country's particular need for a legislative plan to safeguard its citizens' valuable information. However, it is clear that there is no uniform consensus with U.S. policy makers as to what data protection laws should look like across the country. For one, the U.S. has a bi-legislative approach via state-level data protection laws, and sector-based data protection laws. In other words, data protection lives on a state by state level, or an

industry level. This splintered approach has led to confusion from its citizens, and stifled data flows between states.

The EU, however, has been lauded for its clear data protection vision, and definitive steps in safeguarding its citizens' personal information. The interpretation of privacy and data protection as a fundamental right has had a long history in the EU, and is treated as such in its regulations. Furthermore, the EU is a political and economic union of multiple nation states, which makes it all the more miraculous that all 27 members of the Union could agree on a single, unified regulation.

A comparative analysis between the EU and U.S. was chosen for this study for two main reasons. First, the EU has been a historical leader in data protection legislation, and the GDPR rules are currently the most comprehensive and strictest data protection legislation in the world. As for the U.S., the country has faced some of the largest and most public data violations in the 21st century. From the Equifax data breach that exposed the personal information of 40% of the American population, to concerns that political microtargeting had dictated presidential elections, the U.S. is scrambling to put out major fires of data violations. Second, the EU and the U.S. share fundamental, ideological similarities. For one, both powers are leaders in Western democratic values, and have shared a strong military and trade alliance for decades.[20] Both powers are world leaders, and the transatlantic alliance has arguably been one of the most powerful alliances of the last century.

[20] Michael Cohen. "The Common Law in the American Legal System: The Challenge of Conceptual Research." *Law Library Journal* 81, no. 13 (1989): 18.

While both the EU and U.S. share many cultural, political, and economic similarities, they have diverged in their practices on data protection and privacy legislation. This research works to answer, *why does the U.S. have a vastly more limited approach to data protection and privacy laws compared to the EU, despite cases of major personal data breaches? What was the legislative response to safeguard data protection in the U.S. and the EU? How do the data protection laws in each respective power compare to one another?*

Moreover, the U.S. and EU have long displayed a history of high regard for fundamental human rights as collaborators, leaders, and signatories of important international declarations and charters.[21] Yet, the EU has taken explicit steps to protect its citizens and empower them to take control of their data, while the U.S. has been more reluctant to make this step. This has led many to question, *why has the EU taken legislative steps to empower citizens' data as fundamental rights, while the U.S. has not?* Lastly, we will explore the question of, *what are the barriers for the United States in building more comprehensive data protection legislation?*

[21] Jan Wouters, Laura Beke, Anna-Luise Chane, David D'Hollander, and Kolja Raube. "A COMPARATIVE STUDY OF EU AND US APPROACHES TO HUMAN RIGHTS IN EXTERNAL RELATIONS." Publications Office of the EU, 2014, 120-122.file:///Users/kayleen/Downloads/QA0114789ENN.en.pdf.

2. Significance of the Research

Undoubtedly, there is a growing concern among experts, academics, and policy makers that technology is evolving at a pace faster than current laws can adequately address. Innovations in technology will only continue to expand, and the U.S.'s patchwork legislation in data protection is not enough to mitigate breaches. The U.S. stands at a critical point in its data protection legislation, and must decide how the future of its privacy and technology legislation will be handled.

Certainly, there are numerous studies that have analyzed and compared data protection laws in the U.S. and the EU, and reviewed their legal histories and data protection provisions. However, no study has compared the legal framework between the U.S. and the EU through a rights-based approach. While many experts and policy makers argue that data rights should be viewed as a human right, international standards remain indecisive on the matter. With the EU's bold step in coupling personal information with human rights, many are looking to see what the U.S.'s next moves will be. Therefore, this study will investigate the topic from a rights-based framework. First, this research will review the historical understanding of data legislation in the U.S. and EU, and chronicle how data protection legislation and privacy has evolved. Through decoding the differences in the legal interpretation and scope of data rights, we can come to a better understanding as to how the U.S. and EU view current-day legislation.

3. Research Methodology

This research will incorporate both qualitative research and comparative analysis in its methodology. First, the study will define personal information from the EU and the U.S. as the scope of data that is covered under current data protection legislation. As we know, laws today are an iteration of its historical predecessors, and play an important role in our understanding of present-day laws. Then, there will be a review of the history of data protection legislation to establish the progression of data protection.

This will be followed by an analysis of current data protection legislation in both the EU and U.S. However, since the U.S. does not have a unified data protection regulation as the EU does, the pieces of U.S. law for the legislative comparative analysis will be limited to analysis of the major, yet fragmented, data protection regulations in the U.S.: the California Consumer Privacy Act (CCPA), the Gramm-Leach-Bliley Act (or the Financial Modernization Act), the Health Insurance Portability and Accountability Act (HIPAA), and the Children's Online Privacy Protection Act (COPPA), as well as general Federal Trade Commission (FTC) legislation. These laws are the most comprehensive data privacy laws in the U.S. and represent the country's vision on data protection. The EU legislative analysis will be conducted off of the General Data Protection Regulation (GDPR).

Next, the research will examine recent data breach cases and analyze how legislation performed in real situations. As for the case studies, the research will limit the case study review to those that occurred from 2001 to 2019, as this block of time

represents the beginning of the rise in smartphone and social media usage, and more consistent data breach recordings. These two decades represent an era of rapid technological advancements and movements towards data mining and information technology. Since the EU's GDPR laws passed in 2018, this research will interpret its efficacy based off of expert summaries and reviews of the regulation's performance and implementation in the first 18 months of execution.

Lastly, a comparative analysis will be made to review how data protection legislation and practical application of the legislation compare in the U.S. and EU, and apply the conceptual framework outlined below in an effort to present the contextual reasons as to why the two powers have vastly different protection standards.

4. Conceptual Framework

The rights-based approach to public policy and development is a broad framework that has been used by multiple United Nations agencies such as the United Nations Office of the High Commission of Human Rights (OHCHR), United Nations Children's Fund (UNICEF), and the United Nations Sustainable Development Group (UNSDG).[22] While the exact construct and definition of the framework is broad, the conceptual model is typically used in the frame of centering human rights in policy and development (Cornwall and Nyamu-Musembi 2004). While development is not typically associated with technology and data, considering the ongoing changes in the

[22] "Introduction to a Rights-Based Approach." Social Protection and Human Rights, August 3, 2015. https://socialprotection-humanrights.org/introduction-to-a-rights-based-approach/.

industry, this research posits that data protection could also be considered a developing topic in public policy. Therefore, this development framework can apply to this newly emerging and evolving sector.

As for the main conceptual framework, multiple United Nations agencies have outlined the following as the rights-based framework to development:[23] [24]

(a) A human rights-based approach identifies rights holders and their entitlements and corresponding duty bearers and their obligations, and works towards strengthening the capacities of rights holders to make their claims and of duty bearers to meet their obligations.
(b) As policies and programs are formulated, the main objective should be to fulfill human rights.
(c) Principles and standards derived from international human rights treaties should guide all policies and programming in all sectors and in all phases of the process.

For the purposes of this study, the research will focus on all of the points listed under the rights-based framework, but with some minor adjustments. In this study, 'duty bearers' will be any entity that collects, stores, utilizes, and transfers personal

[23] "The Human Rights Based Approach to Development Cooperation Towards a Common Understanding Among UN Agencies." *Https://Unsdg.un.org/*, September 2003. https://unsdg.un.org/sites/default/files/6959-The_Human_Rights_Based_Approach_to_Development_Cooperation_Towards_a_Common_Understanding_among_UN.pdf.
[24] Ibid.

information for commercial or security purposes. Additionally, ‘rights holders’ will be those whose data has been collected, stored, utilized or transferred. In regards to principle (c), wince there are no current international standards on data protection, this study will focus on whether data protection policies, treatment, and standards have been positioned as a human right, and analyze the consistency of data protection policies across all sectors of a country or union. With this in mind, this research hopes to analyze how effectively each power has held to this framework, if at all, and whether the laws were appropriate measures.

III. Data Protection Legislation in the European Union

1. Defining "personal information" in the EU

The EU's General Data Protection Regulation (GDPR) states that it works to protect and regulate any personal information related to citizens in the EU that is processed by "an individual, a company or an organisation" in a commercial capacity. According to the GDPR, personal data is viewed as any "information relating to an identified or identifiable natural person ('data subject')," which includes "an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[25] The GDPR definition of personally identifiable data is purposefully broad in order to stay ahead of the curve and encompass any future changes to the technology.

Under GDPR, the scope of the regulation only applies to protect 'natural persons' as opposed to 'legal persons,' such as corporations (Regulation EU 2016/679, 2016). In terms of the word 'process', GDPR Article 4 defines data processing as "any action, automated or manual" which includes the "collecting, recording, organizing, structuring, storing, using, or erasing" data. In addition, personal data is defined as any

[25] The General Data Protection Regulation 2008 (EU) 2016/679

identifiable information relating to an individual, including email addresses, location, ethnicity, gender, web cookies, and political opinions.[26]

2. A History of Data Protection in the EU

The EU has been a consistent leader in data protection legislation since the end of World War II. As mentioned in the literature review, the important history of European data protection came in the aftermath of the Second World War where European nation states saw firsthand how personal information databases could be exploited to target and attack minority groups.[27] The trauma of World War II highlighted the need for protections on personally identifiable information. However, it wasn't until the 1970s when companies began using information technology to leverage personal data and store government population census information that the concerns of personal data abuse re-surfaced. With Europe's history in mind, and the boom of electronic data in the 1960s and 1970s, the Council of Europe eventually adopted Resolutions (73) 22 and (74) 29. These resolutions established rules of protecting personal data in data banks in the private and public sectors. With these resolutions came two main principles:[28]

[26] Ibid.
[27] Ibid.
[28] Council of Europe Resolutions (73) 22 and (74) 29.

- The principle of publicity, i.e. that the existence of automated data files should be publicly known; and
- The principle of control, i.e. that public supervisory authorities as well as the individuals directly concerned by the information can require that the rights and interests of those individuals are respected by the data users.

Then, in 1981, the Council passed the 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data'.[29] This Convention introduced additional regulations on personal data processing at an international level and ensured that the "fair and lawful collection and automatic processing of data, storage for specified legitimate purposes and not for use for ends incompatible with these purposes, nor kept for longer than is necessary."[30] Moreover, the resolution established that companies cannot store excessive or unnecessary data, and that data subjects are granted the right to maintain the accuracy, confidentiality, access, and rectification of personal information. Next, in 1995, the Union adopted the Data Protection Directive, which regulated the flow of personal data within the EU, and regulated the process of personal data transfer of EU citizens.[31] This directive was the predecessor to GDPR,

[29] Cécile de Terwangne (2014) The work of revision of the Council of Europe Convention 108 for the protection of individuals as regards the automatic processing of personal data, International Review of Law, Computers & Technology, 28:2, 118-130.
[30] Council of Europe. *European Treaty Series - No. 108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* Strasbourg, 28, 1981. Accessed April 14, 2020. https://rm.coe.int/1680078b37
[31] Neil Robinson, Hans Graux, Maarten Botterman, and Lorenzo Valeri. Tech. *Review of the European Data Protection Directive*. RAND Corporation, 2009, 6.

and its seven principles laid the path to the GDPR principles for individual rights. The Data Protection Directive principles are as follows:[32]

- Notice – individuals should be notified when their personal data is collected
- Purpose – use of personal data should be limited to the express purpose for which it was collected
- Consent – individual consent should be required before personal data is shared with other parties
- Security – collected data should be secured against abuse or compromise
- Disclosure – data collectors should inform individuals when their personal data is being collected
- Access – individuals should have the ability to access their personal data and correct any inaccuracies
- Accountability – individuals should have a means to hold data collectors accountable to the previous six principles

However, The Protective Directive was a non-binding resolution, and therefore, many countries still had national-level data laws. This made for confusion among EU citizens, and difficulties in data flow across EU member states. As a result, GDPR

[32] Nate Lord. "What Is the Data Protection Directive? The Predecessor to the GDPR." Digital Guardian, September 12, 2018. https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr.

eventually replaced the Data Protection Directive in an effort to make data protection legislation uniform across the EU.

2-1. Data protection as human rights in the EU

In 2000, the European Parliament, the Council, and the European Commission came together to catalogue 'fundamental rights' under the Charter of Fundamental Rights of the EU (the Charter). This marked the first time that all three major EU institutions agreed to a catalogue of rights for the union. The Charter based its catalogue of fundamental rights from its Member States' "constitutional traditions and international obligations"[33], which made for a much easier agreement on The Charter among Member States. Under this Charter, Article 8 titled "Protection of Personal Data" establishes data protection as a fundamental right and signaled perhaps one of the most definitive answers to the question of whether personal data protection should be seen as a human right. Specifically, the Article states:[34]

i. Everyone has the right to the protection of personal data concerning him or her.
ii. Such data must be processed fairly for specified purposes on the basis of the consent of the person concerned or some other legitimate basis

[33] Charter of Fundamental Rights of the European Union. 2000. (2000/C 364/01) HHS Office of the Secretary, Office for Civil Rights, and Ocr. "Summary of the HIPAA Security Rule."
[34] Ibid

laid down by law. Everyone has the right of access to data, which has been collected concerning him or her, and the right to have it rectified.

iii. Compliance with these rules shall be subject to control by an independent authority.

This set a precedent for how data protection would be viewed from a legal standpoint for future privacy regulations, and how EU citizens regard digital information. The Charter established both privacy and data protection as fundamental to preserving rights and freedoms, similar to those such as free speech or free elections. Therefore, data protection became a highly important topic, guaranteeing that data breach cases would be taken seriously in the Union.

3. The EU's General Data Protection Regulation

The EU's GDPR laws came into effect on May 25, 2018 and are perhaps some of the most comprehensive and explicit data protection regulations currently in place. This piece of legislation was not the first attempt to regulate personal data in the EU, but rather an updated response to the 1995 Data Protection Directive. The 1995 Data Protection Directive (hereafter, 'Directive 95/46/EC') was a binding, country-by-country guideline, rather than a unified regulation, and although the guidelines were innovative, it was less extensive than GDPR. Nonetheless, Directive 95/46/EC used the seven key principles outlined by the OECD's '*Recommendations of the Council*

Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data' to build the comprehensive data principles in the guidelines.[35] These principles outlined by the OECD regarding data subject rights were: notice, purpose, consent, security, disclosure, access, and accountability. Each of these principles gives the individual user considerable autonomy in ensuring hers or his data will only be used with consent and notice. Furthermore, these principles place the burden of data security on data processing companies.

In part, Directive 95/46/EC was adopted in response to correct the difficulties of data free-flow among EU states with disparate data privacy laws. This was due to the fact that the OECD Personal Data protection guidelines were non-binding, and some states had not adopted its rules. However, due to the country-by-country nature of the regulation, there were slight differences among the EU Member States during implementation, and data flow issues continued to occur. This inevitably led to difficulties enforcing a cohesive regulation across the Member States, and greater administrative costs. Therefore, the European Commission worked to create a single, unified regulation to simplify data protection laws. In doing so, this allowed for true, free flow of information among EU Member States, and greater cross-border cooperation to fight crime, such as terrorism.[36] This ambitious regulation eventually culminated into the General Data Protection Regulation of 2018.

---

[35] Nate Lord. "What Is the Data Protection Directive? The Predecessor to the GDPR." Digital Guardian, September 12, 2018. https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr.
[36] Ibid

In passing the GDPR guidelines, the EU made a powerful move signaling its commitment to building a unified response in protecting its citizens' privacy from data misuse and manipulation. Furthermore, these laws reiterated the fundamental values of privacy as a human right, giving more freedom and control to individual users than any other comprehensive data reform regulation. Many companies and countries marveled at the severity of the penalties involved in violating the guidelines, and questioned how countries could implement the regulations.[37] While GDPR is a long and complex piece of legislation, the biggest elements in the regulations could be categorized into four major components: [38]

(1) Limitations to the scope of data processing

(2) Explicit data processing privacy designs for companies

(3) Individual rights for data subjects, and

(4) Independent impact assessments to monitor protection.

First, the regulations explicitly outline that companies processing any EU citizens' data must comply with lawful, fair and transparent forms of data processing. In other words, this means that any processed personal information must be done for a legitimate reason, and companies must be transparent with its users. In addition, the legislation explicitly outlines limitations in data usage and storage. For instance,

[37] Ibid
[38] Ibid

companies cannot process data outside of the scope of the company's purpose, and must delete any personal data once the purpose has been served.

Second, GDPR has outlined that companies must implement privacy and protection in the design of new processing systems, and ensure company accountability when transferring personal data to third parties. While GDPR doesn't outline specific security implementation rules for companies, it does request companies maintain the highest levels of cyber security, and implement safeguards to protect the private data collected in their systems. This regulation covers instances of hacking or accidental data leakage and holds companies accountable for weak security systems. GDPR seeks to protect the transfer of personal data, putting the burden of ensuring the protection and privacy of the information on companies making the transfer to third parties, rather than on individuals.

Next, and perhaps one of the most unique elements of GDPR, are the rules regarding the rights of data subjects. EU citizens have incredible autonomy when it comes to the commercial use of personal data. In particular, GDPR establishes the following individual rights for data subjects:[39]

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure

[39] Regulation (EU) 2016/679 (General Data Protection Regulation)

- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Through these established rights, a data subject can request the data collected on them from companies, ask for information correction, request data deletion or transfer, and object to having their personal data processed. Moreover, companies must clearly and explicitly receive consent from the data subject to collect any information used for processing – consent of which can be rejected at any time. In addition, companies must notify data subjects within 72 hours of a severe data breach. It's significant to note that GDPR has outlined an article dedicated to the rights of users, as it highlights the importance the EU has placed on individuals in these guidelines. Data subjects have incredible control over personal information, and can erase or rectify information upon request – no other data protection law allows this, unless the data is extremely sensitive information, such as medical or financial records.

Lastly, GDPR has outlined ways in which companies and organizations can be educated on GDPR legislation, and maintain continuous adherence to the regulations. For one, GDPR has requested companies hire a Data Protection Officer (DPO) as an advisor on GDPR compliance. This falls in line with GDPR's requirements that organizations must conduct regular training on personal data and data breach measures, and ensure that employees are educated on GDPR regulations. These rules ensure that

companies and their employees fully comprehend data privacy laws in the EU, are regularly trained on their responsibilities to mitigate data breaches, and rely on the DPO for guidance. This extra step vies to make the regulation transition smooth and seamless.

Not only are there strict requirements outlining data usage and notifications to users, GDPR also clearly marks penalties to those who violate the regulations. The penalties for GDPR non-compliance are split into two tiers, and are dependent on the degree of the transgression. These tiers are broken up into the lower and higher level penalties. The lower level penalty consists of a fine of up to 10 million Euros, or 2% of the company's revenue from the previous financial year, whichever is greater. The higher level penalties are based on more serious violations, and consist of either a fine of up to 20 million Euros, or 4% of the firm's worldwide annual revenue from the previous financial year, whichever is greater.[40] In this two-tier penalty system, the data subject rights and consent are considered serious violations and subject to the highest financial penalties. GDPR experts believe that the massive penalties, and the clear consequences for violations, will be deterrence factors for companies to comply with the regulations.

[40] Ibid.

4. Initial Reactions to GDPR

While GDPR is a relatively new legislation, an assessment made by the European Data Protection Board (EDPB) found that just nine months after GDPR went into effect, there were 206,000 cases of regulation violations, with over 95,000 cases related to complaints, and 65,000 initiated by data breaches. While this seems like a lot of cases, the EDPB predicts that even more cases will be filed in 2019 and 2020 as companies adjust to and implement the new guidelines. Nonetheless, the 206,000 cases yielded over $55 million Euros in fines across multiple industries.[41] However, Google paid a massive $50 million of the $55 million in fines in those first nine months for violating privacy rules and transparency requirements in France. GDPR rules had found that Google was not transparent with its users as to how the service was retrieving data for tailored advertisements. This marked the first major GDPR fine against the technology giant, and signaled to other technology companies that massive fines could be coming their way.

While it is too early to understand the efficacy of GDPR solely through case studies, the number of cases indicates that data many breaches are not going un-notified. According to the EDPB, despite over 200,000 cases of regulation violations, about 52% of the 200,000 cases have been closed, and 1% of the cases were challenged

[41] European Data Protection Board. First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities. 2019. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV 2019/02-25/9_EDPB_report_EN.pdf (Accessed April 12, 2020).

in national court.[42] According to the EDPB, this has been a huge success, considering over 100,000 cases of data breaches and violations have been handled and closed within just nine months.

5. Analysis of EU Data Protection Laws

Although it is too early to realize the full impact of GDPR, this research can analyze and unpack the history of privacy and data protection laws in the EU, and determine how the legislation views data protection in the context of the framework. For one, it's clear that the EU has established explicit and thorough regulations to both the duty bearers and data subjects. GDPR legislation has clearly defined the meaning of data protection, personally identifiable information, the regulation scope and territory of the regulation, and penalties for specific violations. As for individual rights, GDPR has outlined the 'Rights of the Data Subject' in Article 3 with clear wording as to what data subjects are entitled to. Through the specificity and clear scope of regulations in GDPR, it's apparent that these rules recognize the importance of data protection, and entitles individuals the tools and rights to control unnecessary data collection, empowering the data subjects.

However, many are concerned with the implementation and execution of GDPR legislation, and overall, companies seem unprepared to execute such complex

[42] European Data Protection Board. First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities. 2019. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf (Accessed April 12, 2020).

regulations. In fact, one year after GDPR came into effect, one in five companies believed full GDPR compliance would be impossible, and by December 2018, "only 50% of companies believed they were GDPR compliant."[43] Therefore, additional time must be spent to allow companies and governments to adjust to the new regulations.

[43] Rob Sobers. "GDPR's Impact So Far: Must-Know Stats and Takeaways - Varonis." Inside Out Security, March 30, 2020. https://www.varonis.com/blog/gdpr-effect-review/.

IV. Data Protection Legislation in the United States

1. Defining "personal information" in the U.S.

Perhaps one of the most difficult aspects in creating a unified data protection law in the United States stems from the lack of consensus on what data protection and data privacy means in the country. Certainly, there are legal scholars and experts who have defined the phrase, but there is no federal mandate that explicitly defines the matters and scope of data protection. Furthermore, the definition of personal information differs state by state. This inherently makes it more difficult to construct meaningful, federal legislation around data violations, proving that policy makers and experts have not sufficiently analyzed the concepts of personal privacy and how it should be defended in legislation.[44] Even the Federal Trade Commission (FTC), which is the only federal agency to regulate any data privacy and security laws in the U.S., remains elusive in stating a true definition for 'data protection' or 'personal information'.

Therefore, this research will use the California Consumer Privacy Act's (CCPA) definition of personal information, as the CCPA contains the strictest data protection regulations among all of the U.S. states. According to the CCPA, personal information is defined as "*information that identifies, relates to, describes, is*

[44] David H Flaherty. "Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies." *Science, Technology, & Human Values* 11, no. 1 (1986): 7–18. https://doi.org/10.1177/027046768601100102.

reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[45] In fact, the CCPA constitutes any personally identifiable information as any of the following:[46]

- *Direct identifiers* such as real name, alias, postal address, social security numbers, driver's license, passport information and signature.
- *Indirect identifiers* such as cookies, beacons, pixel tags, telephone numbers, IP addresses, account names, etc.
- *Biometric data* such as face, retina, fingerprints, DNA, voice recordings, health data…
- *Geolocation data* such as location history via devices,
- *Internet activity* such as browsing history, search history, data on interaction with a webpage, application or advertisement.
- *Sensitive information* such as personal characteristics, behavior, religious or political convictions, sexual preferences, employment and education data, financial and medical information.

This definition coincides very closely with that of the personally identifiable information given by GDPR, and carves out the scope of protection in data legislation to meet these elements.

[45] California Consumer Privacy Act of 2018, TITLE 1.81.5.
[46] Identified by the CCPA https://oag.ca.gov/privacy/ccpa

2. U.S. Data Protection Legislation

2-1. The Fourth Amendment to the U.S. Constitution

The highest semblance of privacy protection legislation comes through in the Fourth Amendment of the U.S. Constitution.[47] The Fourth Amendment states that people have the right "in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated" (Fourth Amendment, Bill of Rights). Traditionally, this meant that people could not have their personal belongings or homes searched without probable cause or a court-ordered warrant. Overall, this protected people from having their personal property unduly searched or seized. However, the intention of the Fourth Amendment was to restrict government powers on its people, rather than to protect individuals from private companies.

Today, the Fourth Amendment has been greatly debated as it relates to the Internet and technology. Many question what jurisdiction the government has and how far can it go to "search and seize" information, and whether searching the web in pursuit of evidence could be considered illegal activity. Furthermore, courts disagree as to how government officials should differentiate between what is public and what is private information in a borderless, digital world. The Fourth Amendment is a piece of legislation that leverages a property-based approach at the crux of its argument. In other words, this Amendment guarantees privacy within the confines of a person's

[47] Jim Harper. "National Constitution Center." National Constitution Center – constitutioncenter.org. Accessed April 12, 2020. https://constitutioncenter.org/digital-privacy/The-Fourth-Amendment-in-the-Digital-Age.

property. The confusion and modern-day interpretation must come from parsing out what is considered property on a borderless medium, such as the Internet, and whether data could be constituted under that definition.

Historically, through a series of court case rulings from the 1960s to the 1970s, personal information or documentation shared on the Internet is not subject to the jurisdiction under the Fourth Amendment because the information is no longer deemed 'private'. This is because information shared online was considered as having been 'shared' with someone else, such as another person or an Internet provider, and is no longer within the confines of personal property. For example, under this logic, emails sent from a private email address could be considered "public" information because the user knowingly shared data with the email provider. However, digital technology has come a long way since the early 60s and 70s, and the type of data and the volume of information shared on digital platforms have changed enormously. Since this time, some digital information, such as cell phone records and email passwords are considered personal property and can only be gathered with a court-ordered warrant. These changing interpretations alongside technological innovation exemplify the difficult nature in pinning legal regulations to an evolving topic.

2-2. U.S. Privacy Act of 1974

Since the Fourth Amendment, the next largest privacy legislation in the country was the U.S. Privacy Act of 1974. This act worked to safeguard individual

privacy from potential misuse. Innovative for its time, this act codified practices that governed the collection, use, maintenance, and dissemination of information held by individuals in federal agencies. Furthermore, citizens could access government documents, and required that government agencies only collect "necessary and relevant" information on constituents.[48] According to the U.S. Department of Justice (DOJ), under his act, individuals must give written consent for the DOJ to release personal information unless the disclosure of information falls under one of twelve legal exceptions.

Lastly, individuals may access and amend personal records on file, allowing for greater autonomy over individual information. However, the Act has fallen short in many ways. For example, the act has not been updated since the 1970s, and is not adequate to handle the technological advances of today. Moreover, there are exemptions to data disclosure rules for 'routine' uses of data.[49] However, "routine uses" has not been clearly defined in the Act, and due to the broad interpretation, many agencies have taken liberties with the term.[50]

2-3. Post-9/11 government surveillance

In the aftermath of the September 11, 2001 terrorist attacks the U.S. government expanded its powers in public surveillance in an effort to mitigate future

[48] The Privacy Act of 1974, as amended, 5 U.S.C. § 552a.
[49] Ibid.
[50] Angelique Carson. "So the Privacy Act Falls Short, But What To Do?" So the Privacy Act Falls
Short, But What To Do? 2014. https://iapp.org/news/a/so-the-privacy-act-falls-short-but-what-to-do/.

offenses.[51] The shock and fear of 9/11 reverberated throughout the world, and allowed U.S. government surveillance to go relatively unexamined by its citizens for years. However, as surveillance expanded under the guise of national security, advances in digital technology also improved, and Internet usage expanded. While concerns for cyber security had always been a threat, social media platforms, deep web sub-channels, and propaganda videos began flooding the Internet. As a result, greater concerns for possible data misuse began to grow.

Big data mining and behavior modeling from online data became more sophisticated and widely used in digital advertising. With the launch of Facebook in 2004, the volume of personal data exploded onto the Internet, and retailers clamored to leverage Facebook's data to target users with advertisements. A few years later, in 2007, Apple Inc. launched its innovative iPhone, changing the landscape of smartphone usage and technology. The combination of social media and widespread smartphone usage contributed to a surge in digital platform servers in the early 2000s, increasing the amount of data subjects using Internet services. This attention-shift into the digital sphere has motivated more companies to invest in digital services, perpetuating the incentive for more people to use the Internet.

However, the U.S. data protection laws are patch-worked by state or industry, with no unified, federally mandated data protection law. Therefore, one could contend that there are nearly fifty data protection standards U.S. companies must comply with,

[51] Gary L. Gregg II. "George W. Bush: Foreign Affairs." Miller Center, July 10, 2017. https://millercenter.org/president/gwbush/foreign-affairs.

which leaves the potential for many unregulated holes in data laws. Currently, the Federal Trade Commission (FTC) is the only agency that has the power to enforce data protection regulations at the federal level, and the FTC does so on a sectoral basis. Other than the FTC, there are no federal data privacy laws or independent agencies that regulate data protection, or even address the topic of information privacy. Nonetheless, data protection legislation became seriously derailed after 9/11, and the U.S. has yet to recover and push for a federal data law.

2-4. State-level data provisions

Every state in the U.S. has differing levels of comprehensive data laws that are mandated, statewide. Today, the only states with statewide comprehensive data privacy laws are California, Maine and Nevada. In Maine, statewide data protection, labeled LD 946, only requires the following four elements:

- The right to restrict processing (LD 946, 2019)
- The right to opt out of the sale of personal information (LD 946, 2019)
- Notice/transparency requirements (LD 946, 2019)
- Prohibition on discrimination against a consumer for exercising a right (LD 946, 2019)

Nevada's statewide legislation (SB 220/Ch. 603A) offers even fewer obligations, with only the following three that must be met:

- The right to opt out of the sale of personal information (SB 220/Ch. 603A, 2019)
- Notice/transparency requirements (SB 220/Ch. 603A, 2019)
- Data breach notification (SB 220/Ch. 603A, 2019)

Most of the remaining states do not have state-level consumer privacy laws, and very few are in the process of building legislation. However, many states have been stonewalled with disagreements as to the depth and scope that data protection legislation should maintain. **Figure 2** below displays the current status of the proposed or enacted privacy bills of each state's data protection legislation, and identifies whether the state bill included sixteen of the most common privacy statutes. As shown in the table, most bills are in the very early stages of committee hearings, and the provisions vary across each state.

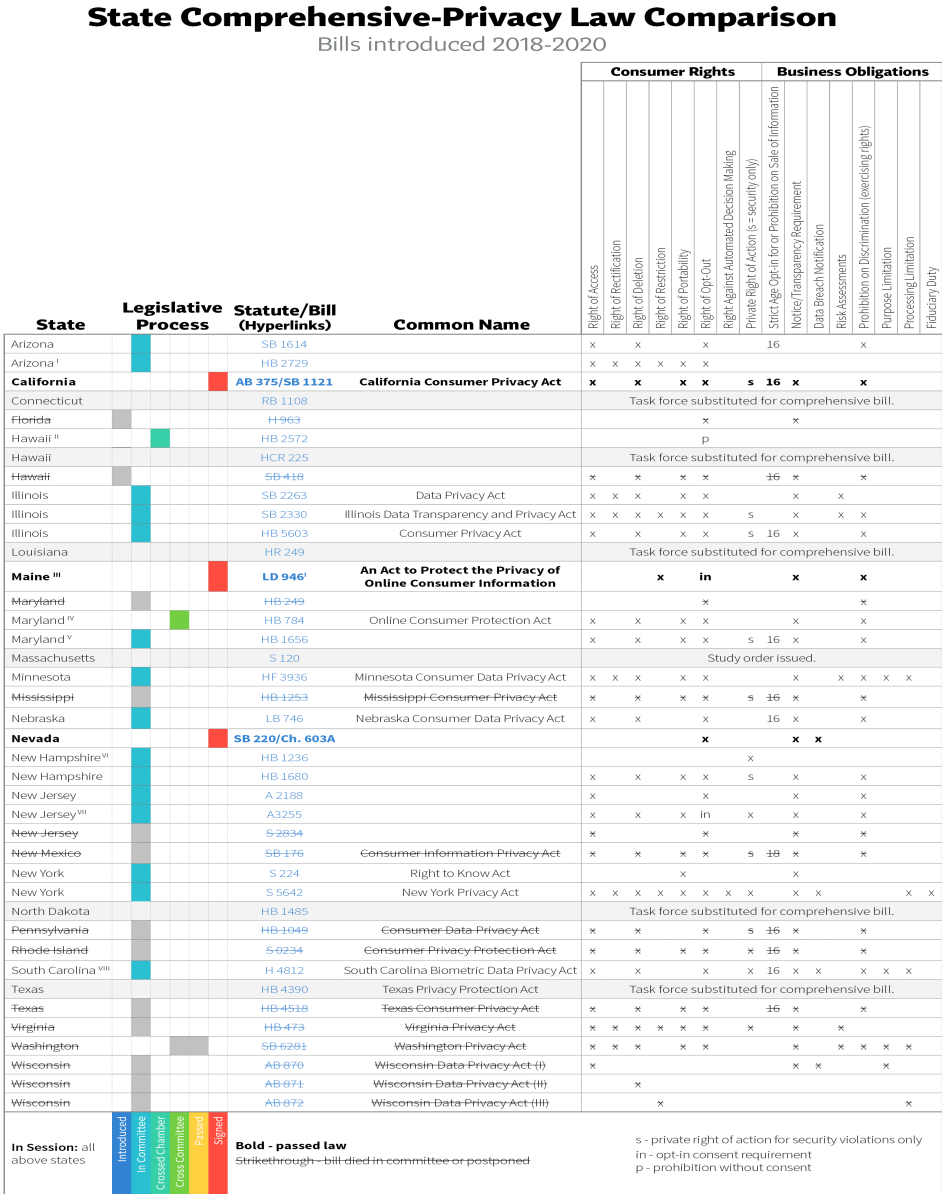

Figure 2. Figure illustrates 16 main elements of U.S. state-level data protection laws. Made by the IAPP Westin Research Center, 2020[52]

[52] Mitchell Noordyke. US State Comprehensive Privacy Law Comparison, 2020. https://iapp.org/resources/article/state-comparison-table/.

2-5. California Consumer Privacy Act (CCPA)

Undoubtedly, the most comprehensive state-level data protection legislation in the United States is the California Consumer Privacy Act. This bill passed into law in 2018, and will be enforced in January of 2020. Under CCPA, consumers will have a wide range of rights when it comes to personal data, and these rules are very similar to that of GDPR. These are the following individual rights granted under CCPA:[53]

(a) The right to know what personal information is collected, used, shared or sold, both as to the categories and specific pieces of personal information;
(b) The right to delete personal information held by businesses and by extension, a business's service provider;
(c) The right to opt-out of sale of personal information. Consumers are able to direct a business that sells personal information to stop selling that information. Children under the age of 16 must provide opt in consent, with a parent or guardian consenting for children under 13.
(d) The right to non-discrimination in terms of price or service when a consumer exercises a privacy right under CCPA.

As provided earlier in the definition of "personal information," the CPPA's definition of personal information is meant to be broad in scope to cover a wide net of personally identifiable factors. Unique to CPPA was establishing "probabilistic

[53] California Consumer Privacy Act of 2018, TITLE 1.81.5.

identifiers" as a personally identifying marker. This, in theory, could mean that any data that has the ability to identify a person at a 50% margin or greater, could be classified as a deterministic identifier, and therefore, protected under the law. Clearly, CCPA has similar elements to GDPR, and grants a wide range of individual rights to its constituents.

2-6. Industry specific data protection legislation

Other than state-specific standards listed above, the U.S. mainly approaches data protection through a sectoral approach. Specific industries have carved out data breach and protection standards that apply to verticals. Perhaps some of the biggest sectors with industry-wide privacy legislation are the health and financial industries, regulated through Health Insurance Portability and Accountability Act, and Gramm-Leach-Bliley Act, respectively. The Children's Online Privacy Protection Rule is the only non-sectoral based legislation that contains an overarching data protection and privacy law.

In the health industry, the Health Insurance Portability and Accountability Act (HIPAA) regulates the privacy of certain health information. The HIPAA Privacy Rule was created in 1996 and has established "national standards to protect individuals' medical records and other personal health information, and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health

care transactions electronically."[54] Similar to GDPR, this Act established ways to improve the free flow of information between health care providers. In doing so, this allows for fluid transactions between health care providers and health insurance companies, while implementing a standard to protect patients from fraud or theft. Patients are also given rights to release, examine, or correct medical information, and limits disclosure of information without the patient's consent. This rule gives power to the patients to control their own medical information, and allow personal documentation to be sealed from public authority. In addition, the burden of providing secure services and protecting patient confidentiality falls on the healthcare providers.

Under the financial sector, the Gramm-Leach-Bliley Act (GLBA Act) of 1999 protects personal financial information stored in financial institutions, such as banks. The FTC oversees the enforcement of this act, and requires financial and banking institutions to safeguard sensitive customer data, and inform consumers of their information sharing practices. The financial institution must inform their consumers of any information that could be shared with third parties, and the consumer can opt out of sharing personal information.[55] Once again, the burden of clearly informing consumers of any shared personal data falls on the financial or banking institution, and consumers have the option to not disclose any information.

Lastly, the Children's Online Privacy Protection Act (COPPA) passed in 2000 to impose guidelines to protect information collected from children on websites.

[54] Health Insurance Portability and Accountability Act of 1996.
[55] The Gramm-Leach-Bliley Act of 1999

Similar to the GLB Act, this is also regulated by the FTC. Under this Act, operators of commercial websites and online services are required to:[56]

- Post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from children;
- Provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information online from children;
- Give parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties (unless disclosure is integral to the site or service, in which case, this must be made clear to parents);
- Provide parents access to their child's personal information to review and/or have the information deleted;
- Give parents the opportunity to prevent further use or online collection of a child's personal information;
- Maintain the confidentiality, security, and integrity of information they collect from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security; and
- Retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use.

[56] Children's Online Privacy and Protection Rule, 1999

In this provision, a "child" is identified as any person under the age of thirteen, and a "parent" is considered any legal guardian over the 'child.'[57] In addition, it's clear that this rule retains the burden of informing privacy rules and receiving consent on the company, rather than the consumer.

One common denominator in each of these privacy and protection acts is that the burden of ensuring the data protection of its consumers is placed on the institution providing the service. The consumer is given considerable power to request data and information changes, and deny public distribution of personal data for very specific types of data.

However, the provisions and their links to the marketplace or capitalism are not overlooked. In fact, many may question why the FTC, a federal trade body that generally regulates antitrust enforcement, also regulates information protection in key industries. The FTC reports that it governs data protection in these verticals to ensure consumer confidence in the marketplace, and regulate the free flow of information (FTC Privacy & Security Update 2018). However, in allowing the FTC to control data protection provisions, capital growth and data protection are inextricably linked. While consumers can request and deny access to information, since the FTC regulates and enforces the rules, it can also control the extent of power consumers have over their own information. Furthermore, in allowing the FTC to regulate personal information privacy, it can control the market from monopolies that vie to use consumer data for

[57] Ibid.

market advantage. Therefore, the largest federally mandated data protection laws in the U.S. have been inextricably linked to the marketplace.

3. U.S. Case Studies

The United States has had some of the largest and most public data breaches and data misuse cases in the world. Industries from technology, to finance, to retail have all felt the impact of data hacking or mishaps in inappropriate data transfers. For example, one of the largest failures in data protection measures happened with the 2017 Equifax data hack. This data breach impacted 143 million Americans or 40% of the total U.S. population.[58] While Equifax may have had insufficient security measures to handle a large-scale hack of this kind, the biggest violation in the scandal was the company's extremely delayed response in notifying its consumers that their data had been compromised. Reports estimate that Equifax was hacked sometime in May or June of 2017, but did not notify its customers of the breach until September of that year.[59] This meant that the hacking had exposed and left vulnerable pockets of people and their information open to identity theft and fraud for nearly five months.

[58] Josh Fruhlinger. "Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?" CSO Online. CSO, February 12, 2020. https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.
[59] Ibid.

3-1. The 2016 Cambridge Analytica Case

While some cases of data hacking are clear-cut incidents of weak security systems, one case truly changed the way policy makers and experts view data protection and its future impact: the 2015 Cambridge Analytica scandal. In 2015, political consulting firm Cambridge Analytica was hired to run Donald Trump's political campaign in his bid for the President of the United States. The firm built a personality quiz application on Facebook with a buried "Terms and Conditions" statement that allowed the company to collect information from the quiz user's Facebook profile.[60] Cambridge Analytica then scraped the Facebook profiles of millions of users to gather information such as age, location, and education, as well as behavioral information from liked posts and shares on their Facebook feed. This information allowed Cambridge Analytica to collect thousands of data points on peoples' behavior and build extensive models to predict voting behavior.[61]

However, the key data misuse issue with Cambridge Analytica arose when it was revealed that the firm also targeted the data of Facebook friends of the users who took the quiz. In other words, those who never took the quiz, but were Facebook friends of someone who did, were also subject to data mining without their consent or knowledge. Even information from profiles with explicit privacy controls were illegally scraped by Cambridge Analytica. This meant that the firm profited off of the

[60] Paul Lewis, David Pegg, and Alex Hern. "Cambridge Analytica Kept Facebook Data Models through US Election." The Guardian. Guardian News and Media, May 6, 2018. https://www.theguardian.com/uk-news/2018/may/06/cambridge-analytica-kept-facebook-data-models-through-us-election.
[61] Ibid.

collection, storage, utilization, and data transfer of 87 million Facebook profiles, many of which did not consent to sharing personal information.[62] The Cambridge Analytica team then leveraged this information obtained by the Facebook profiles to model 'dark posts', or individually tailored advertisements and messages, to micro-target undecided voters.[63] With this illegally gathered data, Cambridge Analytica built extensive algorithms and behavioral models to predict voting behavior for the upcoming presidential election, and used highly sensational messaging to micro-target key voters in swing states. Some of these key states included Wisconsin, Michigan, and Pennsylvania – all three of which would eventually vote for Donald Trump in the 2016 Presidential elections.

Perhaps more troubling is the fact that Facebook learned Cambridge Analytica had retrieved Facebook profile information, including friends' information, in 2015, but did not notify the public until a whistleblower came forward three years later in 2018.[64] While Facebook did request that the firm delete any profile data in 2015, Cambridge Analytica informed Facebook that it deleted the data harvested from its application, but did not inform Facebook that it saved derivative data from their models. Derivative data includes "predictive models, or clusters of populations in psychological groupings, can be highly valuable to companies involved in micro-

[62] J. Isaak and M. J. Hanna, "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," in Computer, vol. 51, no. 8, pp 56-59, August 2018.
[63] Wakefield, Jane. "Cambridge Analytica: Can Targeted Online Ads Really Change a Voters Behaviour?" BBC News, 2018. https://www.bbc.co.uk/news/technology-43489408.
[64] Ibid.

targeting advertisements to voters."[65] According to experts and data scientists, these types of models and analyses can be more valuable than any raw data retrieved directly from Facebook profiles. Furthermore, this scandal was a major violation of peoples' online data privacy, and displayed the potentially disastrous offline effects digital manipulation can have. At one point, Cambridge Analytica advertised that it had over 5,000 data points on nearly every voter in the United States, giving the company enormous power in political campaign strategies.[66] Most alarmingly, knowing that this information could have influenced voting behavior in the largest and most important democratic elections of the Western world erodes at the very fabric of a free and democratic society.

While it is difficult to definitively state that Cambridge Analytica's microtargeted campaign leveraging Facebook user profiles won the election for Donald Trump, the facts of the case remain clear. A company gathered peoples' personal information without explicit consent, and leveraged the data beyond the scope of its believed purpose. In more so, arguably the largest social media platform, Facebook, did not do their due diligence in ensuring the safety of millions of its users. The 2016 Cambridge Analytica scandal brought data misuse to new heights, forcing industry heads and policy makers to begin discussing where regulations need to draw the line in collecting and leveraging data.

---

[65] Ibid.

[66] Gina Chon. "Breakingviews - Review: Blaming Big Data Is Political Diversion." Reuters. Thomson Reuters, July 19, 2019. https://www.reuters.com/article/us-usa-technology-breakingviews/breakingviews-review-blaming-big-data-is-political-diversion-idUSKCN1UE1NL.

4. Barriers to Legislation in the U.S.

The United States undoubtedly has a unique state-federal system with an expansive and diverse constituency. Oftentimes, this makes it difficult for federal powers to come to a consensus on legal matters, and this is no exception for data protection laws. The separation of powers and the large number of members in Congress make it very difficult to pass major legislation, particularly ones as sensitive as data protection and data privacy.[67]

Furthermore, the American public notoriously favors policies with less government involvement and bureaucracy, and more market and capital freedoms. Many in the U.S. argue that data protection and privacy are actually in conflict, and surveillance methods will harm privacy more than safeguard it.[68] In fact, when Congressman Gilbert Gude of Maryland proposed a committee to merely oversee the implementation of the provisions for amendments to the Privacy Act of 1974, he was met with fierce criticism. The proposed committee would "provide for the establishment an administrative body to mediate conflicts between agencies and individuals, to investigate complaints, hold hearings, and make findings of fact."[69] In other Western democracies, data protection agencies are generally granted extraordinary independence from government powers and are allowed freedoms to

[67] David H Flaherty. "Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies." *Science, Technology, & Human Values* 11, no. 1 (1986): 309. https://doi.org/10.1177/027046768601100102.
[68] Ibid, 312.
[69] Ibid, 312.

hold governments accountable to their constituents.[70] However, Committee members vetoed the implementation and oversight committee on the argument that it could increase bureaucracy. As a result, some argued that the failure to create an overarching agency had "inhibited effective implementation of the Privacy Act Law."[71]

4-1. The U.S. technology industry

Some of the most famous and most valuable technology companies in the world are U.S.-based firms: Google, Facebook and Amazon. In fact, **Figure 3** below shows that 65% of the world's biggest technology companies are based in the U.S.[72] Not only is each company a tech leader in their respective niches, they also generate billions of dollars in revenue each year and provide for thousands of jobs. One thing all three-tech companies have in common is that each of these companies built an extensive business model that capitalizes on the massive volume of personal data in their systems. In fact, it's estimated that more than $2 out of every $3 spent on digital advertisement goes either to Google, Facebook or Amazon.[73] So, what makes these three companies so enticing for advertisers? These companies have billions of users who have shared thousands of data points of personal information on the platforms. In essence, these

[70] Ibid, 8.
[71] David H Flaherty, "The Need for an American Privacy Protection Commission," Government Information Quarterly, Volume 1 (August 1984), 233-38.
[72] Forbes Magazine, May 1, 2019. https://www.forbes.com/sites/ajdellinger/2019/04/30/how-the-biggest-tech-companies-spent-half-a-billion-dollars-lobbying-congress/.
[73] Alexei Oreskovic. "This Chart Shows Just How Much Facebook, Google, and Amazon Dominate the Digital Economy." Business Insider. Business Insider, June 16, 2019. https://www.businessinsider.com/facebook-google-amazon-dominate-digital-economy-chart-2019-6.

tech behemoths have a massive leg up in the business of consumer data, and have made billions selling this information to companies for advertisement targeting.[74] In fact, Amazon, Facebook and Google have been so successful in leveraging user data that they now control the top three digital ad platforms in the U.S., and profited a combined revenue of $73 billion in 2018 alone.[75]

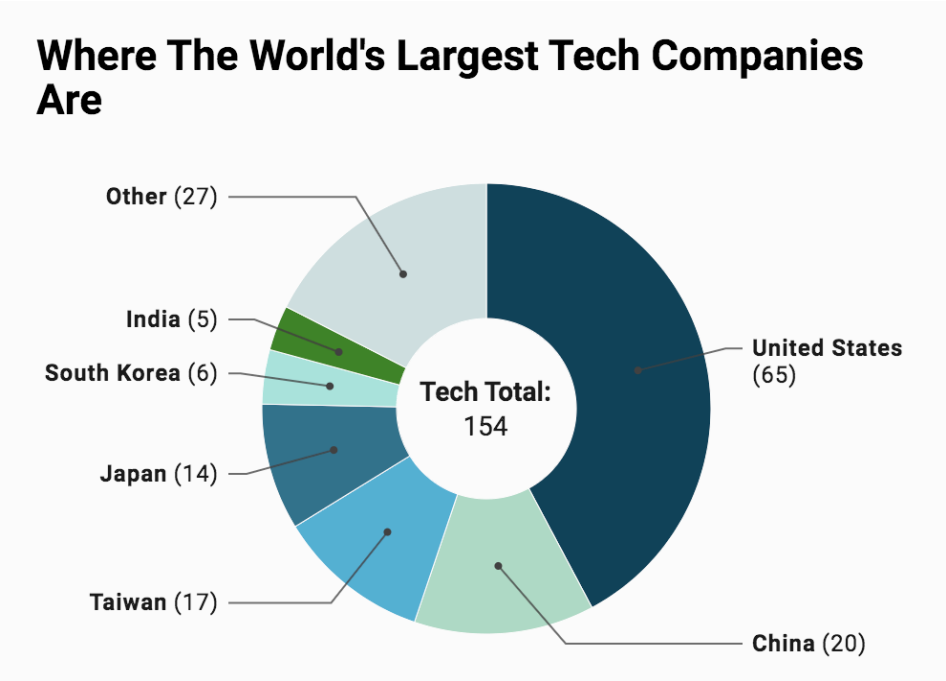

Figure 3. As of 2019, 65% of the largest technology companies are based in the U.S.

Figure by Forbes, 2019

[74] Daniel Cuonz, Scott Loren, and Metelmann Jörg. *Screening Economies: Money Matters and the Ethics of Representation*. Bielefeld: Transcript Verlag, 2018.
[75] Greg Sterling. "Almost 70% of Digital Ad Spending Going to Google, Facebook, Amazon, Says Analyst Firm." Marketing Land, June 17, 2019. https://marketingland.com/almost-70-of-digital-ad-spending-going-to-google-facebook-amazon-says-analyst-firm-262565.

With the success and massive revenue streams of these tech companies, one could argue that data protection laws could inhibit or strain a massive industry that relies on buying and selling user data for digital advertisement space. In order to curry favor in public policy, technology companies have made a powerful presence in the U.S. lobby industry. Since the mid-2000s, technology giants have become some of the fastest growing companies spending in political lobbying. For instance, the five largest technology firms in the U.S., Apple, Amazon, Google, Facebook and Microsoft, have spent more than half a billion dollars from 2005 to 2018 on lobbying.[76] Since 2006, yearly lobbying spend from the tech industry reached well over $110 million in total, while the industry's lobbying expenditure never even hit the $50 million mark before 2000.[77] From 2016 to 2018, Google remained the biggest corporate spender, outspending the traditional lobby giants, Boeing and AT&T.[78] Yet, in 2018, the major technology company, Google, spent $21.7 million on lobbying, which was a 38% increase from its spend in 2016.[79] Two other tech leaders, Facebook and Amazon, were also within the top 20 corporate lobby spenders in the U.S. in 2019.

[76] AJ Dellinger. "How The Biggest Tech Companies Spent Half a Billion Dollars Lobbying Congress." Forbes.
[77] Eric Chiu. "Google, Facebook Lead New Generation of Technology Companies Pressing Government for Favorable Treatment." OpenSecrets News, August 16, 2018. https://www.opensecrets.org/news/2011/02/google-facebook-lead-new-generation/.
[78] Aditi Roy. "Google Is Tech's Top Spender on Lobbying - Facebook and Amazon Are Also at Record Levels." CNBC. CNBC, June 10, 2019.
[79] Ibid.

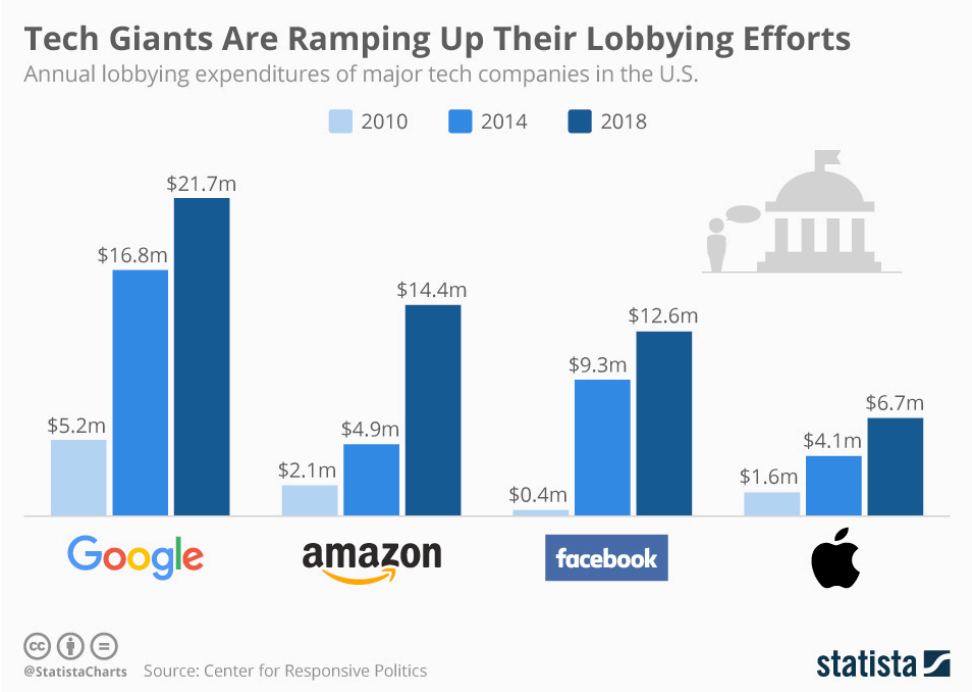

Figure 4. Total lobbying spend across these four technology companies increased nearly 6-fold from 2010 to 2019. Figure by Statista 2019

It's clear that technology companies have made a major splash in Washington, DC politics, and with revenues as high as they currently are, there doesn't seem to be a slow-down in the near future. In fact, the only FTC Internet privacy regulation lives under Section 5, and it only prohibits "misleading representations" of consumer data privacy.

Furthermore, not only do these companies have the pockets to influence policy makers, American technology companies also bring valuable innovation and prestige to the United States. Technology development can play a major role in bolstering the economy, military, and even national security. Therefore, in a time when the U.S. is

fighting to stay ahead of global competition, these companies have evolved as a major asset to the country.

5. Analysis of U.S. Data Protection Laws

Current U.S. data protection laws and its history are fragmented and often confusing to follow. While the U.S. has publicly supported data subject rights and the need for greater protection, the country's inability to pass comprehensive legislation with clear steps to strengthen and empower citizens is troublesome. Furthermore, recent data breach cases show that data misuse is not only happening at a massive scale in the U.S., but also at levels that could greatly compromise the integrity of the democratic system. Despite these warnings, it seems that the massive tech industry and illogical fear of government bureaucracy has hindered the country's ability to create more effective and efficient rights-based data protection laws.

Nonetheless, some states are taking it upon themselves to build legislation that has been difficult to execute at a federal level. California's Consumer Privacy Act has been hailed as the "mini GDPR," and contains legislation that will empower consumers to request access to personal information, receive personal data transfer notifications, and can opt out of or delete personal information upon request. Some expect that other states may follow suit with similar rights-based approaches to data protection, but a unified federal legislation seems difficult to achieve.

V. Comparative Analysis

In reviewing the differing interpretations of data protection and privacy between the EU and U.S, analyzing the history and the application of data protection laws, and researching the effectiveness of the legislation, it is clear that both powers have a vastly different approach to the subject. In all, the EU clearly adheres to a rights-based approach with data protection legislation, whereas the U.S. does not. The EU has been extremely proactive in its quest to protect citizens from data manipulation, and worked to empower its citizens to understand their rights in the matter. Certainly, European history and experience in World War II influenced the Member States' current views on information privacy. Remnant memories of knowing that unchecked privacy violations could lead to discrimination have led to more stringent protection measures today.

As a result, data privacy has been regarded as an implicit right, and the EU has made steps to safeguard personal data as fundamental. The European Convention and the Charter of Fundamental rights have both made provisions regarding privacy, and Article 8 of the Convention explicitly outlines the rights of individuals and their authority in protecting personal information. In Article 8, paragraphs 2 and 3 give EU citizens the right of "access to data which have been collected concerning him or her, and the right to have it rectified; and that compliance with these rules shall be subject

to control by an independent authority."[80] Overall, it's clear that the EU believes data protection is a human right, vital in protecting the well-being of its citizens, and maintaining a sustainable democracy.

On the other end, the U.S. FTC has been extremely slow in remedying privacy violations that don't have public interest or economic interests attached. In the U.S., personal information is viewed as a commodity, and therefore, data misuse and violations are weighed against the potential economic impact they may have. As a result, data laws are passed on an as-needed basis, and the burden of implementation and regulation is placed on private companies.

This method of privacy legislation adopted on an ad hoc or a sectoral-basis is evident through legislation such as the Health Insurance Portability Act or the Children's Online Privacy Protection Rule. These regulations are protective, but limited in scope. Furthermore, the U.S. does not explicitly refer to or mention privacy or data protection on a Constitutional level, whereas the EU does. It would seem that U.S. data protection legislation contains elements of a laissez-faire approach, allowing markets, companies and individuals to regulate the system. In fact, data protection is viewed as a civil matter rather than a fundamental liberty in the U.S.

Furthermore, the U.S. has hesitated in creating protection legislation that could cause difficulties in data collection and transfer for tech companies. The collection, transfer and utilization of personal data plays an integral part in a multibillion dollar advertising industry in the country, and a source of income for major technology

[80] GDPR 2018.

companies.[81] Fears of restrictive data and privacy laws could threaten America's booming technology sector and economy, and has hampered bigger, more restrictive regulation. With lowered incentives to give consumers power over their own data, individual users are at an inherent disadvantage.

The U.S. is, however, making some strides in statewide legislation with the CCPA. The CCPA is very similar to GDPR in that both regulations allow consumers the right to opt-out of having their data processed, and the right to access or delete personal information held by a company. This is a step towards empowering consumers to control their personal information. Nonetheless, GDPR is still a more comprehensive and strict guideline than CCPA. For one, GDPR allows consumers to rectify incorrect personal data, and requires explicit consent from the data subject. CCPA does not yet allow a consumer to correct incorrect personal data, and only requires that a privacy notice be made on websites for data subjects, although the notice does not have to be "explicit".

[81] Jacques Bughin, Michael Chui, and James Manyika. "Clouds, Big Data, and Smart Assets: Ten Tech-Enabled Business Trends to Watch." Rep. *Clouds, Big Data, and Smart Assets: Ten Tech-Enabled Business Trends to Watch*. McKinsey, 2007: 8.

VI. Conclusion

Through innovations in technology and the increasing use of the Internet, future regulations on data protection will be paramount to maintain freedom, peace, and order in democratic societies. The 2016 Cambridge Analytica scandal already showed the potential ramifications lax data protection measures could have on American democracy, and allowing further transgressions to arise could be detrimental. The European Union has already proven itself to be a leader in this field by incorporating human rights into its data protection and privacy laws for decades, prioritizing security and notification systems, and setting clear boundaries for companies. Today, GDPR has set the standard model for future data protection regulations, and through a thorough review of the EU's data protection standards and regulations, it's clear that the EU adheres to a rights-based approach in data policy. Through the lens of a rights-based conceptual framework, the EU has adhered to all three principles below:

(a) A human rights-based approach identifies rights holders and their entitlements and corresponding duty bearers and their obligations, and works towards strengthening the capacities of rights holders to make their claims and of duty bearers to meet their obligations.

(b) As policies and programs are formulated, the main objective should be to fulfill human rights.

(c) Principles and standards derived from international human rights treaties should guide all policies and programming in all sectors and in all phases of the process.

In particular, GDPR has set aside provisions dedicated to the rights of the individual in Article 8, and provided the data subject's entitlements and rights, as well as processes to remedy damages. GDPR has also clearly stated the duties and obligations of any entity collecting, storing, transferring, or utilizing personal data, and outlined a two-tier penalty system for violators. Furthermore, the EU has officially recognized data protection and privacy as a fundamental human right, and has remained consistent in this declaration across all of its industries. There are no sector-biased policies, as there are in the U.S.

The U.S. has, to some degree, met the basic necessities of the rights-based provision in principle (a), but has only done-so in patches. The industry-level protection laws such as HIPAA, COPPA, and the GBL Act empower data subjects to understand their data protection rights and control publicly available information. However, this very segmented approach negates principle (c) of the rights-based framework, as data protection standards are not uniform across sectors. While children,

financial information, and health information are granted more privacy privileges, the Internet is widely unregulated.

With that said, the U.S. is certainly making some strides towards more comprehensive data protection. The California Consumer Privacy Act is a step towards GDPR-level protection, and many states could follow in California's steps. In addition, by massive backlash from previous data breaches, many technology companies are working on ways to protect consumer privacy and appease public opinion. Facebook admitted to its past failures to protect consumer information during the 2016 Cambridge Analytica scandal, and was forced to pay a hefty fine. Since then, the company has committed to more security measures and to safeguard its consumers' information privacy. Time will tell if Facebook will follow through with more explicit measures in the future.

As for the current study, research conclusions remain limited. First, GDPR is a relatively new regulation, and its efficacy is yet to be fully realized. Despite its comprehensive nature, 45% of EU citizens still express concern about their data privacy, even after the regulations came into effect.[82] Although this percentage does not compare to the nearly 70% of Americans that are concerned about their data privacy, the concerns in the EU still remain intact. Therefore, future studies should be conducted on the effectiveness of GDPR, whether it truly deters data abusers, encourages companies to follow through with compliance, and whether public

[82] Rob Sobers. "GDPR's Impact So Far: Must-Know Stats and Takeaways - Varonis." Inside Out
Security, March 30, 2020. https://www.varonis.com/blog/gdpr-effect-review/.

sentiment and confidence in protection regulations improve. Furthermore, this study did not touch upon the efficacy of CCPA, which was initiated on January 1, 2020. Just like GDPR, it is yet to be seen whether CPPA will be effective in curbing data breaches, protecting data misuse, and empowering data subjects. Future studies should also review the nuances of government surveillance and its effect on government response to data protection legislation. Due to the limited nature of publicly available information, and the narrow scope of this study, this research was not able to dive into government surveillance programs and its implications on data regulation.

Overall, the urgency for further study on this matter remains clear. Many academics believe the U.S. must thoroughly review its data protection standards, clearly outline its rules, and explicitly define penalties for violations today, before it is too late. Growing fears of future data misuse weigh heavily on potentially devastating political implications that could seriously damage public sentiment at best, and democratic norms at worst. While the U.S. CCPA rules are now in effect, this legislation will be rendered useless without uniform legislation passed in other states. Now, more than ever, the U.S. stands at a critical moment in its data protection legislation, and must make important consideration for consistent, federal-level data protection provisions.

The discussions on data protection and personal information privacy, and whether these should be considered a fundamental right will continue to be an ongoing subject of debate. As long as technology continues to grow and more processes turn to digital automation, policy makers and experts will have to figure out how to protect

consumer rights without stifling the economy, data flow, and innovation. Governments must decide how to regulate a borderless, virtual world before cybercrimes render millions of people vulnerable. As a world leader in both political ideology and technological innovation, the U.S. is perhaps facing the most public scrutiny in this field. It is now, more important than ever, for the U.S. to re-evaluate its legal concepts of privacy, digital data, and protection, and come to a definitive conclusion as to how its legislation will move forward. Hopefully, the U.S. will strike the balance before long-term damages manifest.

Bibliography

Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica Turner. Pew Research Center, November 2019, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," 2, 7.

Bhatia, Punit. "GDPR Summary: Overview of 10 Key Requirements." EUGDPRAcademy, March 3, 2020. https://advisera.com/eugdpracademy/knowledgebase/a-summary-of-10-key-gdpr-requirements/.

Bughin, Jacques, Michael Chui, and James Manyika. "Clouds, Big Data, and Smart Assets: Ten Tech-Enabled Business Trends to Watch." Rep. *Clouds, Big Data, and Smart Assets: Ten Tech-Enabled Business Trends to Watch*. McKinsey, 2007: 8.

California Consumer Privacy Act of 2018, TITLE 1.81.5.

Castells, Manuel. "Technology, Society, and Historical Change" essay in *The Rise of the Network Society (The Information Age: Economy, Society and Culture, Volume 1) (Vol. 1)*, 5. Malden, MA: Wiley-Blackwell, 1996.

Carson, Angelique. "So the Privacy Act Falls Short, But What To Do?" So the Privacy Act Falls Short, But What To Do? 2014. https://iapp.org/news/a/so-the-privacy-act-falls-short-but-what-to-do/.

Chiu, Eric. “Google, Facebook Lead New Generation of Technology Companies Pressing Government for Favorable Treatment.” OpenSecrets News, August 16, 2018. https://www.opensecrets.org/news/2011/02/google-facebook-lead-new-generation/.

Charter of Fundamental Rights of the European Union. 2000. (2000/C 364/01)

HHS Office of the Secretary, Office for Civil Rights, and Ocr. “Summary of the HIPAA Security Rule.”

Chon, Gina. “Breaking views - Review: Blaming Big Data Is Political Diversion.” Reuters. Thomson Reuters, July 19, 2019. https://www.reuters.com/article/us-usa-technology breakingviews/breakingviews-review-blaming-big-data-is-political-diversion-idUSKCN1UE1NL.

Cohen, Michael. “The Common Law in the American Legal System: The Challenge of Conceptual Research.” *Law Library Journal* 81, no. 13 (1989): 18. Cornwall, Andrea, and Celestine Nyamu-Musembi. “Putting the ‘Rights-Based Approach’ to Development into Perspective.” *Third World Quarterly* 25, no. 8 (2004): 1415–37.

Council of Europe. *European Treaty Series - No. 108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* Strasbourg, 28, 1981. Accessed April 14, 2020. https://rm.coe.int/1680078b37

Council of Europe. *Resolution 73(22), On the Protection of the Privacy of*

Individuals vis-à-vis Electronic Data Banks in the Private Sector. Committee of Ministers September 26, 1973. Accessed April 14, 2020. https://rm.coe.int/1680502830

Council of Europe. *Resolution 74(29), On the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector*. Committee of Ministers September 20, 1974. Accessed April 14, 2020. https://rm.coe.int/1680502830

Cuonz, Daniel, Scott Loren, and Metelmann Jörg. *Screening Economies: Money Matters and the Ethics of Representation*. Bielefeld: Transcript Verlag, 2018.

Dellinger, AJ. "How The Biggest Tech Companies Spent Half a Billion Dollars Lobbying Congress." Forbes.

De Groot, Julianna. "The History of Data Breaches." Digital Guardian, October 24, 2019. https://digitalguardian.com/blog/history-data-breaches.

De Terwangne, Cécile (2014) The work of revision of the Council of Europe Convention 108 for the protection of individuals as regards the automatic processing of personal data, International Review of Law, Computers & Technology, 28:2, 118-130.

Dixon, Pam. "A Brief Introduction to Fair Information Practices." Blog, 2006. https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/.

Duffin, Erin. "Total Lobbying Spending in the United States from 1998 to 2019."

Rep. Total Lobbying Spending in the United States from 1998 to 2019. Statista, n.d.

European Parliament, Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council. Regulation (EU) 2016/679. 2016. https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG Accessed April 2020.

European Data Protection Board. First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities 2019. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV 2019/02-25/9_EDPB_report_EN.pdf (Accessed April 12, 2020).

European Union. "European Union Agency for Fundamental Rights (FRA)." European Union, February 13, 2019. https://europa.eu/european-union/about-eu/agencies/fra_en.

Federal Trade Commission, *Privacy & Data Security Update: 2018*. 2018. https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf. Accessed April 20, 2020

Finn, Rachel, David Wright, and Michael Friedewald. "Seven Types of Privacy." Essay in *European Data Protection: Coming of Age*, 3–32. Dordrecht:

Springer Netherlands, 2013.

Flaherty, David H. Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States. Chapel Hill, NC: Univ. of North Carolina Press, 1992.

Flaherty, David H. "Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies." *Science, Technology, & Human Values* 11, no. 1 (1986): 7–18, 309, 312. https://doi.org/10.1177/027046768601100102.

Flaherty, David H, "The Need for an American Privacy Protection Commission," Government Information Quarterly, Volume 1 (August 1984). 233-58 Forbes Magazine, May 1, 2019. https://www.forbes.com/sites/ajdellinger/2019/04/30/how-the-biggest-tech-companies-spent-half-a-billion-dollars-lobbying-congress/.

Federal Trade Commission. "*FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*." *FTC*, 2019. https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

Fruhlinger, Josh. "Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?" CSO Online. CSO, February 12, 2020. https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

II, Gary L. Gregg. “George W. Bush: Foreign Affairs.” Miller Center, July 10, 2017. https://millercenter.org/president/gwbush/foreign-affairs.

The General Data Protection Regulation 2008 (EU) 2016/679

Harper, Jim. “National Constitution Center.” National Constitution Center – constitutioncenter.org. Accessed April 12, 2020. https://constitutioncenter.org/digital-privacy/The-Fourth-Amendment-in-the-Digital-Age.

HHS.gov. US Department of Health and Human Services, July 26, 2013. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html. “Introduction to a Rights-Based Approach.” Social Protection and Human Rights, August 3, 2015. https://socialprotection-humanrights.org/introduction-to-a-rights-based-approach/.

J. Isaak and M. J. Hanna, "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," in Computer, vol. 51, no. 8, pp. 1, 56-59, August 2018.

Lewis, Paul, David Pegg, and Alex Hern. “Cambridge Analytica Kept Facebook Data Models through US Election.” The Guardian. Guardian News and Media, May 6, 2018. https://www.theguardian.com/uk news/2018/may/06/cambridge-analytica-kept-facebook-data-models-through-us-election.

Lord, Nate. “What Is the Data Protection Directive? The Predecessor to the GDPR.” Digital Guardian, September 12, 2018.

https://digitalguardian.com/blog/what-data-protection- directive-predecessor-gdpr.

Madden, Mary, and Lee Rainie. “Americans’ Attitudes About Privacy, Security and Surveillance.” Americans’ Pew Research Center. Accessed April 18, 2020. https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/, 4.

Marris, Paul, and Sue Thornham. Media Studies: A Reader. Edinburgh: Edinburgh University Press, 1996.

Noordyke, Mitchell. US State Comprehensive Privacy Law Comparison, 2020. https://iapp.org/resources/article/state-comparison-table/.

Olivia B. Waxman, “GDPR-Disturbing History Behind the EU's New Data Privacy Law,” Time (Time, May 24, 2018), https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/.

Oreskovic, Alexei. “This Chart Shows Just How Much Facebook, Google, and Amazon Dominate the Digital Economy.” Business Insider. Business Insider, June 16, 2019. https://www.businessinsider.com/facebook-google-amazon-dominate-digital-economy-chart-2019-6.

Price, Michael. Journal of National Security Law & Policy 8, no. 247 (2016). Https://Www.law.nyu.edu/Sites/Default/Files/upload_documents/Price%20Rethinking-Privacy-Fourth-Amendement-Papers_2.Pdf

Ponciano, Jonathan. “The Largest Technology Companies in 2019: Apple Reigns As Smartphones Slip and Cloud Services Thrive.” Forbes. Forbes

Magazine, May 8, 2020. https://www.forbes.com/sites/jonathanponciano/2019/05/15/worlds-largest-tech-companies-2019/.

Rainie, Lee, Sara Kiesler, Ruogu Kang, and Mary Madden. “Anonymity, Privacy, and Security Online | Pew Research Center.” Anonymity, Privacy, and Security Online. Accessed May 18, 2020. https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1). Accessed April 24, 2020.

Reklaitis, Victor. “How the Number of Data Breaches Is Soaring - in One Chart.” MarketWatch. MarketWatch, May 25, 2018. https://www.marketwatch.com/story/how-the-number-of- data-breaches-is-soaring-in-one-chart-2018-02-26.

Robinson, Neil, Hans Graux, Maarten Botterman, and Lorenzo Valeri. Tech. *Review of the European Data Protection Directive*. RAND Corporation, 2009, 6.

Roy, Aditi. “Google Is Tech's Top Spender on Lobbying - Facebook and Amazon Are Also at Record Levels.” CNBC. CNBC, June 10, 2019. https://www.cnbc.com/2019/06/09/google-is-techs-top-spender-on-

lobbying-but-facebook-amazon-also-up.html.

Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890): pp. 193-220.

Singer, P. W., and Allan Friedman. 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press, 13.

Sobers, Rob. "GDPR's Impact So Far: Must-Know Stats and Takeaways – Varonis." Inside Out Security, March 30, 2020. https://www.varonis.com/blog/gdpr-effect-review/.

Sterling, Greg. "Almost 70% of Digital Ad Spending Going to Google, Facebook, Amazon, Says Analyst Firm." Marketing Land, June 17, 2019. https://marketingland.com/almost-70-of-digital-ad-spending-going-to-google-facebook-amazon-says-analyst-firm-262565.

The Economist. "The World's Most Valuable Resource Is No Longer Oil, but Data." The Economist. The Economist Newspaper. Accessed March 25, 2020. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

Torre, Lydia F de la. "What Is 'Convention 108'?" Medium. Golden Data, September 17, 2019. https://medium.com/golden-data/what-is-coe-108-3708915e9846.

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (OJ C 306, 17.12.2007)

The U.S. Department of Health and Human Services, The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191.

https://www.hhs.gov/sites/default/files/privacysummary.pdf

The U.S. Federal Trade Commission, The Gramm-Leach-Bliley Act of 1999, Public Act 106-102

The U.S. Federal Trade Commission, The Children's Online Privacy and Protection Rule of 1999, 15 U.S.C. 6501–6505

The U.S. Department of Justice, The Privacy Act of 1974, as amended, 5 U.S.C. § 552a. United Nations Sustainable Development Group. "The Human Rights Based Approach to Development Cooperation Towards a Common Understanding Among UN Agencies." *Https://Unsdg.un.org/*, September 2003. https://unsdg.un.org/sites/default/files/6959The_Human_Rights_Based_Approach_to_Development_Cooperation_Towards_a_Common_Understanding_among_UN.pdf.

Wakefield, Jane. "Cambridge Analytica: Can Targeted Online Ads Really Change a Voters Behaviour?" BBC News, 2018. https://www.bbc.co.uk/news/technology-43489408.

Waxman, Olivia B. "GDPR-Disturbing History Behind the EU's New Data Privacy Law." Time. Time, May 24, 2018. https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/.

Wouters, Jan, Laura Beke, Anna-Luise Chane, David D'Hollander, and Kolja Raube. "A COMPARATIVE STUDY OF EU AND US APPROACHES TO HUMAN RIGHTS IN EXTERNAL RELATIONS." Publications

Office of the EU, 2014, 120-122.

file:///Users/kayleen/Downloads/QA0114789ENN.en.pdf.

Tables and Figures