4-29-2022

Data Privacy Regulations in the United States, China, and the European Union

Charlsey A. Kelly
Georgia Southern University

Data Privacy Regulations in the United States, China, and the European Union

An Honors Thesis submitted in partial fulfillment of the requirements for Honors in

Accounting

By

Charlsey Kelly

Under the mentorship of Justin Evans

Abstract

This paper compares and discusses the different data privacy regulations found in the United States, China, and the European Union. It is no secret that big tech companies like Facebook and Google continuously collect data on their users. The big question is what protections and rights one has as a consumer. The answer to this question differs when you are in different parts of the world. Currently the United States does not have a federal data privacy law, China recently adopted a new data privacy law called the Personal Information Protection Law, and the European Union has a data privacy law in place called the General Data Protection Regulation. Even though the United States does not have a federal law, individual states do have data protection laws. The big tech companies are pushing hard for the U.S. to create a federal law, and they hope that this will eventually lead to an international data protection law. The lack of consistency between the regulations of different countries has made it more difficult and costly for the technology companies that rely on data collection to fund their websites instead of or in addition to advertising and/or subscriptions from users.

Thesis Mentor: _____

Dr. Justin Evans

Honors Director: _____

Dr. Steven Engel

May 2022
Accounting Department
University Honors Program
Georgia Southern University

Acknowledgments

I would like to give a special thank you to Dr. Justin Evans for guiding me through this process. I have learned so much from you that I will continuously use throughout my academic career. I know that this has been a long process, but you remained supportive, enthusiastic, and helpful the entire time. I could not have asked for a better mentor to take this journey with.

I would also like to thank my family for their constant support not just during this process but throughout my entire life. I love you guys and will be forever grateful for you all.

Introduction

It is no secret that technological advancements are happening rapidly, changing our society as we once knew it. Of particular influence is social media. According to research conducted by Esteban Ortiz-Ospina in 2019, one in three people around the world have some form of social media.[1] With social media reaching into almost every home worldwide it has become a major privacy concern for users and lawmakers alike. Between January 2013 and July 2018 there were six billion records stolen in data breaches in the United States alone.[2] A major and recent example of a breach of confidentiality can be seen in the Cambridge Analytica scandal of 2015. Cambridge Analytica conducted a survey within Facebook which gave them access to personally identifiable information. When the user clicked on the survey and gave consent to Cambridge to obtain their information, Cambridge then began to collect information on other users connected to the consenting user without their consent. This scandal led to the harvesting of the information of around 50 million Facebook users without their consent.[3]

Although this rapid technological change has been underway for decades now, it has taken law makers worldwide much longer to update the laws surrounding technology and data collection. According to one scholar, regulatory regimes have responded in three main ways as it relates to technology. The first response is simply applying old laws to new technology.[4] The second response is to keep the core of the current law but change it

---

[1] Esteban Ortiz-Ospina, https://ourworldindata.org/rise-of-social-media, (2019).

[2] Jordan Yallen, *Untangling the Privacy. Law Web: Why the California Consumer Privacy Act Furthers the Need for Federal Preemptive Legislation*, 53 LOYOLA OF LOS ANGELES L.REV. 787 (2020).

[3] Thomas Gerhart, *AB 2182 And Chapter 55: Enacting Privacy Regulations in the Face of Legislative Complacency,* 50 U. PAC. L. REV. 177 (2019).

[4] Urs Gasser, *Recording Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy*, 130 HARV. L. REV. FORUM 61 (2016).

slightly to encompass the new technology.[5] The final response is to completely change the approach to regulating technology.[6] By examining the European Union, China, and the United States and the responses each is taking toward data privacy regulations, it is apparent that Gasser's typology holds true. Even though the three countries have taken different approaches they all are trying to accomplish the same goal which is to protect specific information of natural persons from illegal collection, dissemination, and processing.[7] Each country is simply trying to protect the interests of individuals.[8]

The United States, the European Union, and China are all seen as major influencers in the world as it relates to technology and legislation. This paper will examine what these three countries are doing to ensure data privacy and protection for their citizens. It will compare the direction taken by each of these countries and the effectiveness of their decisions. By comparing these three countries we will see that the United States is behind when it comes to protecting its citizens from major corporations profiting off of the collection and selling of their consumers personal data.

The European Union

The European Union (EU) has been a trailblazer in the field of data privacy regulations. The EU completely shifted from the previous data regulations to an entirely new comprehensive data regulation called the General Data Protection Regulation. The EU has taken an activist approach which means that it has placed the responsibility for the protection of users' data privacy on the company as opposed to on the user.[9] Within

---

[5] Id. at 64.
[6] Urs Gasser, *Recording Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy*, 130 HARV. L. REV. FORUM 61 (2016).
[7] Yi Shao, Personal Information Protection: China's Path Choice, 18 US-CHINA L. REV. 227 (2021).
[8] Id. at 242.
[9] Nandan Nilekani, *Data to the People India's Inclusive Internet* (2018).

this section we will examine past data privacy regulations established by the EU and the current data privacy regulation found there.

Early Data Privacy Regulations

The major legislation passed by the EU regarding data privacy was the European Data Protection Directive. This Directive was adopted by the European Commission in 1995.[10] The directive was created to protect individuals when it came to companies processing personal data.[11] The Directive consisted of 7 main principles. These principles were that data subjects had to be given notice about the collection of their data, subjects had to be informed about who was collecting their data, requirements for data storage had to be met, transferring data that could be used to identify a person was not allowed without consent, subjects could view their data and check for inaccuracies, collected data could only be used for the stated purpose, and companies that collected personal data could be held liable for failing to protect personal information.[12]

The General Data Protection Regulation

The European Union took a large step in advancing regulations related to data privacy when it passed the General Data Protection Regulation (GDPR) in March 2014.[13] The GDPR was the first comprehensive regulation specifically for data privacy. The

[10] Ernst-Oliver Wilhelm, https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation, (2016).
[11] Ernst-Oliver Wilhelm, https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation, (2016).
[12] Jordan Yallen, *Untangling the Privacy. Law Web: Why the California Consumer Privacy Act Furthers the Need for Federal Preemptive Legislation*, 53 LOYOLA OF LOS ANGELES L.REV. 787 (2020).
[13] Id. at 790.

regulation went into full effect in March of 2018 and applied to any business that had a presence in the EU no matter how big or small.[14] The main goal of the GDPR is to protect any information that either directly or indirectly identifies a particular person.[15] With this goal in mind, the GDPR gives several rights to not only EU citizens, but to anyone located in the EU. Some of these rights are the right to be informed, the right of access, the right of portability, the right to rectification, the right to erasure, the right to object, the right to restrict processing, and the right to object to automated decision making.[16] Specifically, the right to be informed requires that companies collecting data must make their purpose for collecting the information, how long it will be stored, and additional parties that the information is shared with available to the data subject.[17] The right of access requires that a copy of the data being collected must be provided.[18] The right of portability ensures that data subjects can move, copy, or transfer personal data easily without altering its usability.[19] The right to rectification ensures that subjects can correct any inaccurate or missing data at any time, and the controller must comply with the request promptly.[20] The right to erasure requires personal data to be deleted when it is no longer necessary, the subject withdraws consent, or the subject objects and there is no legitimate reason to override the objection.[21] This right also requires the controller to respond to a request for erasure within a month.[22] The right to object gives individuals the

[14] Id. at 791.
[15] Jordan Yallen, *Untangling the Privacy. Law Web: Why the California Consumer Privacy Act Furthers the Need for Federal Preemptive Legislation*, 53 LOYOLA OF LOS ANGELES L.REV. 787 (2020).
[16] Id. at 806-810
[17] Id. at 806-807.
[18] Id. at 807.
[19] Id at 808.
[20] Id.
[21] Id. at 808-809.
[22] Id.

ability to object to the processing of their data when it is processed for direct marketing purposes, for scientific historical research, or for statistical research.[23] After a subject objects, the onus is not on them to explain their basis for objecting; rather, it is up to the controller to explain why it is necessary to still process the data.[24] The right to restrict data can be used if the accuracy of the data is contested, the processing is unlawful and the subject does not want the data erased, the controller no longer needs the data, but the subject needs it for legal reasons, or the data subject objects but the controller proves that processing the data is necessary.[25] The right to object to automated decision making is only exempt when it is necessary for a contract, authorized by law, or based on the subject's consent.[26]

A common theme that can be seen when looking at the rights given under the GDPR is the government's policy of recognizing the property rights related to data for the subject, and not for the business that is collecting it. In all the rights in the GDPR, the subject has a say in what happens to their data and the company must abide by their decision. The GDPR also includes enforcement measures to ensure that companies are abiding by the rules and rights established within the regulation. The General Data Protection Regulation requires that every state within the EU have at least one supervisory authority that focuses on protecting the rights given to the people as it relates to processing and storing personal data.[27] The established supervisory authority is also in

[23] Id. at 809-810.
[24] Id.
[25] Jordan Yallen, *Untangling the Privacy. Law Web: Why the California Consumer Privacy Act Furthers the Need for Federal Preemptive Legislation*, 53 LOYOLA OF LOS ANGELES L.REV. 787 (2020).
[26] Id. at 810.
[27] Id.

charge of setting fines for those caught violating these rights.[28] The fines may be either 20 million euro or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[29]

Even though the GDPR was a huge step toward giving individuals control over the data collected on them, the EU did experience some challenges with the initial implementation of this legislation. One example was how expensive it was for companies to implement these needed changes to be in compliance with the legislation. Thirty-nine percent of companies that were expected to comply with the GDPR had not allocated a budget for compliance, and those that did budget for it found that their budget reached millions of dollars annually.[30] This placed a heavy burden on the smaller companies that were expected to comply with the legislation. Another hurdle that the GDPR has caused relates to the understanding of the legislation by US companies. This can be seen by the reaction by US companies to the implementation of the law. On the day that the law became effective several US media outlets and other websites shut down their sites in Europe because they were not completely compliant with the GDPR regulations.[31] Even though the GDPR has been in effect for several years now many Americans, government officials, lawyers, academics, and journalist still misinterpret the law.[32]

China

[28] Id.
[29] Id. at 811.
[30] Tiffany Light, Data Privacy: *One Universal Regulation Eliminating the Many States of Legal Uncertainty*, 65 St. Louis U. L.J. 873 (2021).
[31] Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365 (2019).
[32] Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93 (2020).

China is also a major technology hub, so it is instructive to examine the data privacy regulations put in place there. It is reported that as of December 2020, China had around 989 million internet users which represented approximately 20% of the global total.[33] China also has more than 4 million internet websites and more than 3 million applications.[34] Before the passage of any of its data privacy laws, China was used as a laboratory for big data experimentation, data intelligence, and mass surveillance because of its inadequate protection of personal data.[35] It is also important to examine the regulations put in place by the Chinese government because China differs from the United States and the European Union in terms of political censorship and in denying global digital platforms access to its domestic market.[36] China began its data privacy regulations by relying on a network of laws to provide protection to their citizens, but recently they have established a comprehensive data privacy regulation called the Personal Information Protection Law. Within this section we will examine the past data privacy regulations in China and the new Personal Information Protection Law.

Early Data Privacy Regulations

Before the passage of China's comprehensive data regulation, China strongly resembled the United States' stance on data privacy, which is to say that citizens of China received protections from various other laws that were not exactly related to data

---

[33] Grace Pyo, *An Alternate Vision: China's Cybersecurity Law and Its Implementation in the Chinese Courts*, 60 COLUM. J. Transnat'l L. 228 (2021).

[34] Yi Shao, *Personal Information Protection: China's Path Choice*, 18 US-CHINA L. REV. 227 (2021).

[35] Yongxi Chen & Anne Sy Cheung, *The Transparent Self under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System*, 12 J. COMP. L. 356 (2017).

[36] Dongsheng Zang, Revolt against the U.S. Hegemony: Judicial Divergence in Cyberspace, 39 INT'l L.J. 1 (2022).

collection and processing. China's personal information protection rules were scattered in more than 30 domain specific laws and administrative regulations.[37] The Chinese government had not provided privacy protections for its citizens until China's 1982 Constitution.[38] The United States and the EU on the other hand began to establish data protection during the 1970s.[39] The Chinese relied on laws like the General Principles of Civil Law of 1986, the Criminal Law and its amendments, Article 252 of the Tort Liability Law of 2010, the Telecommunications and Internet Personal User Data Protection Regulation of 2013, and the Cybersecurity Law of 2016 to provide data protection.[40] The Cybersecurity Law of 2016 (CSL) was the first major step to a definitive comprehensive data protection law.[41] The Cybersecurity Law was the first systematic approach at the highest level of legislation to regulate cyberspace.[42] The CSL was a very broad set of regulations and was only applicable to companies located within the country.[43] The CSL required companies to make their rules for collection and use public to everyone. [44] The purpose specification principle is also included within the CSL. This principle prohibits a data collector from processing data for a purpose other than the one specified without consent.[45] The CSL also allows for a person to request the

[37] Xu Duoye, *The Civil Code and the Private Law Protection of Personal Information*, 13 Tsinghua CHINA L. REV. 187 (2020).
[38] Emanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. And The E.U.*, 8 PENN. JOURNAL OF LAW & INTERNATIONAL AFFAIRS 1 (2020).
[39] Id. at 56.
[40] Id. at 67-68.
[41] Emanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. And The E.U.*, 8 PENN. JOURNAL OF LAW & INTERNATIONAL AFFAIRS 1 (2020).
[42] Chen Ji, *Cybersecurity and Data Protection: A Study on China's New Cybersecurity Legal Regime and How It Affects Inbound Investment in China*, 51 INT'l LAW. 537 (2018).
[43] Emanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. And The E.U.*, 8 PENN. JOURNAL OF LAW & INTERNATIONAL AFFAIRS 1 (2020).
[44] Id. at 92.
[45] Id. at 93.

erasure of their data if the data collector has violated laws, or the agreement established between the two parties.[46] After looking at the CSL it is evident that this document does not directly give rights to individuals, but instead protects individuals by imposing requirements on data controllers.[47]

Another aspect of the legal framework in China is the use of non-binding rules.[48] The 2018 Specification was the non-binding rule that accompanied the CSL.[49] The 2018 Specification defined the major terms within the CSL such as who qualifies as a data controller and a data subject.[50] Above we discussed how the CSL requires companies to make their rules for collection and use public, but the 2018 Specification takes this a step further and states that a data controller should express the purpose, methods, scopes, and rules for processing personal information to the data subject.[51] With respect to the right to erasure the 2018 Specification goes a step further and requires data controllers to notify third parties that received the data to also erase the data collected.[52] The 2018 Specification also grants the right to data portability, and it requires that when automated decision making is used that there has to be a way for a data subject to lodge a complaint if they feel that profiling was involved.[53] The CSL does establish fines up to $150,000 or 10 times the amount of unlawful gains from the misuse of data to any entity found in

[46] Id. at 99.
[47] Sarah Wang Han & Abu Bakar Munir, *Information Security Technology – Personal Information Security Specification: China's Version of the GDPR*, 4 EUR. DATA PROT. L. REV. 535 (2018).
[48] Pernot-Leplay defines non-binding rules as text that provides details and guide a laws' implementation; they set best practice standards that companies are to implement themselves voluntarily in theory. Id. at 74.
[49] Emanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. And The E.U.*, 8 PENN. JOURNAL OF LAW & INTERNATIONAL AFFAIRS 1 (2020).
[50] Id. at 79 -80.
[51] Emanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. And The E.U.*, 8 PENN. JOURNAL OF LAW & INTERNATIONAL AFFAIRS 1 (2020).
[52] Id. at 99.
[53] Id. at 101.

violation of the law.[54] Even though the Chinese government decided to improve the CSL, this law along with its accompanying measures are in many ways more advanced than the analogous U.S. legislation, even in light of its vagueness.[55]

Personal Information Protection Law

In 2021 the Chinese government implemented the Personal Information Protection Law (PIPL).[56] By implementing this regulation the Chinese government progressed from a fragmented legal framework that only applied to certain sectors, like we have in the United States, to a uniform cybersecurity legal regime requiring data protection for all personal data.[57] The PIPL was modeled very strongly after the GDPR implemented in the EU. The Personal Information Protection Law applies to any business within the country or outside of China that handles any personal information of anyone within the country.[58] Like the GDPR, the PIPL provides several rights to the people protected under the regulation. These rights include the right to access, the right to rectification, the right to erasure, the right to withdraw consent, the right to cancel an account, the right to obtain copies, and the right to file a complaint in cases where automated decision making had a significant impact on the subjects' rights and

[54] Id. at 91.
[55] Matthew S. Erie & Thomas Streinz, *The Beijing Effect: China's Digital Silk Road as Transnational Data Governance*, 54 N.Y.U. J. INT'l L. & POL. 1 (2021).
[56] Philip J. Bezanson, Seth D. DuCharme, Lucy Tyson, Claire E. Cahoon, https://www.natlawreview.com/article/china-s-new-data-privacy-law-sweeping-and-serious-avoid-high-cost-noncompliance, (2021).
[57] Linxin Dai, *A Survey of Cross-Border Data Transfer Regulations through the Lens of the International Trade Law Regime*, 52 N.Y.U. J. INT'l L. & POL. 955 (2020).
[58] Philip J. Bezanson, Seth D. DuCharme, Lucy Tyson, Claire E. Cahoon, https://www.natlawreview.com/article/china-s-new-data-privacy-law-sweeping-and-serious-avoid-high-cost-noncompliance, (2021).

interests.[59] The PIPL requires that certain information be provided to the data subject before the collection of data can even take place. This information includes the types of data being collected, the purpose of the data being collected, and the rules of collecting and using personal data which includes things like storage location, storage period, and manner and frequency of collection.[60] Unlike the GDPR, the PIPL also applies to biometrics like facial recognition.[61] The Personal Information Protection Law also requires that certain data be stored on servers within China.[62] This keeps certain data within the country and keeps it from being stored by companies outside of China. The PIPL requires that data being transferred to other countries must be proven as a necessity and specific consent must be given by the government.[63] Another key factor of the Personal Information Protection Law is that it is the first document in China that draws a clear distinction between personal information protection[64] and the right to privacy[65].[66] The Personal Information Protection Law does have the harshest punishment for violators

[59] Riccardo Berti, *Data Protection Law: A Comparison of the Latest Legal Developments in China and European Union*, 2020 EUR. J. PRIVACY L. & TECH. 34 (2020).
[60] Id. at 69.
[61] Philip J. Bezanson, Seth D. DuCharme, Lucy Tyson, Claire E. Cahoon, https://www.natlawreview.com/article/china-s-new-data-privacy-law-sweeping-and-serious-avoid-high-cost-noncompliance, (2021).
[62] Id.
[63] Id.
[64] Defined as information that can identify a specific natural person separately or in combination with other information. Xu Duoye, *The Civil Code and the Private Law Protection of Personal Information*, 13 Tsinghua CHINA L. REV. 187, 192 (2020).
[65] Defined as the tranquility of the private life of a natural person, and the private space, private activities, and private information that he is unwilling to be known to others. Id. at 193.
[66] Raymond Yang Gao, *Personal Information Protection under Chinese Civil Code: A Newly* Established *Private Right in the Digital Era*, 13 Tsinghua CHINA L. REV. 165 (2020).

to date. If a company violates the PIPL they can be fined up to 50 million Yuan (which is around $7.7 million), or 5% of annual revenue.[67]

The major downside to the PIPL is that none of the regulations put forth in the document is applicable to any governmental agency. Even though this piece of legislation was a huge step forward for the Chinese government there are people who believe that it could be improved. Robin Hui Huang, Oiang Han, and Xiuwen Zhu argue that China should improve the requirements of consent and disclosure, strengthen the application of the principles of purpose limitation and data minimization, establish a unified law enforcement agency, and enhance private and public enforcement.[68]

The United States

Unlike the European Union and China, the United States does not have data protection regulations at the federal level. The U.S. is one of the non-European countries in the G20 that does not meet the minimum international standards related to data privacy created by the OECD standards.[69] The United States relies on past laws related to privacy as well as state laws to provide data protection to its citizens. Like most topics in the US there is a divide between those who want data privacy regulations at the federal level and those that believe the states should oversee passing these regulations. In this section we will examine the laws at the federal level being applied to data privacy, the regulation

[67] Philip J. Bezanson, Seth D. DuCharme, Lucy Tyson, Claire E. Cahoon, https://www.natlawreview.com/article/china-s-new-data-privacy-law-sweeping-and-serious-avoid-high-cost-noncompliance, (2021).

[68] Robin Hui Huang, Qiang Han & Xiuwen Zhu, *Protecting Data Privacy for Mobile Payments under the Chinese Law: Comparative Perspectives and Reform Suggestions*, 20 CHI.-KENT J. INTELL. PROP. 226 (2021).

[69] Briseida Sofia Jimenez-Gomez, *Cross-Border Data Transfers between the EU and the U.S.: A Transatlantic Dispute*, 19 Santa CLARA J. INT'l L. 1 (2021).

passed by the states, and the benefits and disadvantages of having a comprehensive data privacy regulation.

Current Federal Laws

At the federal level the United States relies on a patchwork of laws that are not directly related to data privacy to provide certain rights to consumers. Some of the major laws that make up this patchwork include the Children's Online Privacy Protection Act, the Gramm Leach Biley Act, the Health Insurance Portability and Accountability Act, the Family Educational Rights and Privacy Act, and the Privacy Act of 1974.[70] The Children's Online Privacy Protection Act was passed in 1998 and it required that children under the age of 13 must have verifiable parental consent for a company to gather personally identifiable information, and the company must give notice of what information is collected and how it is being used.[71] The Gramm Leach Biley Act relates to financial institutes.[72] This act requires that every financial institution has an obligation to respect the privacy and protect the security and confidentiality of its customers.[73] The act also gives the customer an option to inform the institution if they do not want their information shared.[74] The Health Insurance Portability and Accountability Act passed in 1996 focuses on the healthcare industry and addresses providing notices, protecting personal health information, and releasing personal health information.[75] This act also

[70] Shaun G. Jamison, *Creating a National Data Privacy Law for the United States*.
[71] Id. at 8.
[72] Id. at 9.
[73] Id.
[74] Shaun G. Jamison, *Creating a National Data Privacy Law for the United States*.
[75] Id. at 10.

gives the patient the right to access their information.[76] The Family Educational Rights and Privacy Act gives parents and eligible students the right to review student records and make any necessary corrections.[77] The Privacy Act of 1974 pertains to information gathered by the federal government.[78] This act gives individuals the right to access and correct records.[79] It also requires that individuals give their consent for the federal government to release information about the individual.[80]

When looking at the rights and protections protected by these acts it is clear that these rights and protections can be used as it relates to data privacy. The right to correction, the right to access, and the right of portability are all addressed in the different acts discussed above, but they are also key rights as it relates to data privacy. The United States does not have a legal body directly in charge of data privacy like we have seen in the EU and China. The US does, however, have the Federal Trade Commission which is the leading federal agency addressing privacy issues.[81] The FTC is charged with addressing practices that are unfair or deceptive, but the FTC can only act when the unfair act is causing or likely will cause harm to consumers, not reasonably avoidable by the consumers, and outweighed by the need to compete or the benefits to customers.[82]

Current State Laws

[76] Id.
[77] Id.
[78] Id. at 11.
[79] Id.
[80] Id.
[81] Id. at 7.
[82] Id.

In the absence of direct federal protections for data, the states have taken on the responsibility of creating data privacy regulations. All fifty states have some form of data breach notification laws.[83] These laws require that a company alert its consumers of any data breach in which their information could be compromised[84]. [85]Three states – California, Illinois, and Vermont – have gone a step further and imposed more data privacy regulations. California has led the way to data privacy regulations in the United States. In 2018, California passed the California Consumer Privacy Act.[86] California was able to use the General Data Protection Regulations as a guide when creating their own regulation. The act requires businesses to provide notice to consumers about how they plan to share the collected information and give consumers at least two ways to opt out of data collection.[87] The act also requires companies to provide a clear link on their website that gives the consumer the option not to sell their personal information.[88] The company cannot make it mandatory for a consumer to create an account with them in order to have the option to opt out.[89] The act allows consumers to seek damages against a business if they are the subject of a data breach.[90] The consumer can seek damages anywhere between $100 and $750 per customer per incident or actual damages, whichever is greater.[91]

---

[83] Shaun G. Jamison, *Creating a National Data Privacy Law for the United States*.
[84] Compromised is defined as the disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. https://csrc.nist.gov/glossary/term/compromise
[85] Shaun G. Jamison, *Creating a National Data Privacy Law for the United States*.
[86] Thomas Gerhart, *AB 2182 And Chapter 55: Enacting Privacy Regulations in the Face of Legislative Complacency,* 50 U. PAC. L. REV. 177 (2019).
[87] Id. at 189.
[88] Id.
[89] Id.
[90] Id.
[91] Id.

Illinois passed the Illinois Biometric Information Privacy Act in 2008.[92] This act protects the collection, use, retention, and destruction of individuals' biometric identifying information. This includes things like fingerprints, retina scans, and facial recognition.[93] The state of Vermont passed the Vermont Data Broker Law in 2019.[94] This law applies to companies that buy and sell access to data.[95] The law requires brokers to specify if there is an option to opt out of data collection.[96] Unlike other data privacy regulations this law does not require an opt out procedure, right of access, disclosure of how the data was obtained, or private right of action.[97] It is evident that each state has taken a unique approach to providing protection to its residents when it comes to protecting their data.

By examining the passage of data related laws by the states it is evident that the passage of the GDPR has inspired some measure of imitation in the United States.[98] As of May 2019, 25 states had enacted laws addressing the data security practices of private sector entities which is double the amount enacted before the passage of the GDPR.[99]

Benefits and Disadvantages

Like most topics, the question of whether the US should adopt comprehensive data rules at the federal level has its proponents and skeptics. Notwithstanding this split,

---

[92] Quinn Emanuel Urquhart & Sullivan, LLP, https://www.jdsupra.com/legalnews/avoiding-liability-under-the-illinois-, (2021).
[93] Id.
[94] Shaun G. Jamison, *Creating a National Data Privacy Law for the United States*.
[95] Id. at 14.
[96] Id.
[97] Id. at 15.
[98] Elizabeth L. Feld, *United States Data Privacy Law: The Domino Effect after the GDPR*, 24 C. BANKING Inst. 481 (2020).
[99] Id. at 489.

most Americans do believe that there needs to be some form of protection as it relates to data collection. A poll conducted by Politico and Morning Consult found that 56% of registered voters would either strongly or somewhat support a proposal to make it illegal for social media companies to use personal data to recommend content via algorithms.[100] The major divide comes when discussing who should have the ability to regulate the tech industry. Many of the big tech industries that rely on data collection to be a profitable business are pushing for data regulations to come from the federal level rather than the state level. These companies would prefer not to have 50 different sets of regulations to follow. When looking at the established state data privacy regulations we can see how they differ from state to state. This could be costly and time consuming for companies as they strive ensure that they are following all of the regulations established in each state. On the other hand, there are people that believe that the power to regulate data collection should remain exclusively with the states. Many believe that a federal law will not provide enough protection to individuals because of the large influence of the tech lobby. Another problem is that the Constitution does not address the issue of individual privacy on the internet. Here in the United States any powers not given directly to the federal government by the Constitution goes to the states. Those that believe that data protection should be the responsibility of the federal government are relying on the commerce clause within the constitution to support their argument.[101] The commerce clause gives Congress the power to regulate commerce with foreign nations, and among the several

[100] C. Blair Robinson, https://www.jdsupra.com/legalnews/new-poll-underscores-growing-support-8066824/, (2022).
[101] Shaun G. Jamison, *Creating a National Data Privacy Law for the United States*.

states.[102] The argument being made is that the selling of data takes place between organizations within different states and countries which gives Congress the right to regulate the industry.

A major downside of the United States' sluggishness as it relates to creating data privacy regulation is the inadvertent effects it is having on major U.S. based companies that have a strong presence in other countries. In 2014, one estimate showed that cross border data flows added $2.8 trillion to the world GDP.[103] It is safe to say that with the increase in technology that allows data to be processed faster and larger storage capabilities that this number has greatly increased. China and the EU both have placed restrictions for cross border data flow within their legislation. The EU, under the GDPR, requires countries outside of the EU to receive an adequacy decision in order to continue the collection and processing of data of individuals protected by the GDPR outside of the EU. This is because the EU believes that protecting privacy is a fundamental right that must continue regardless of where the personal data is processed.[104] The requirements put in place for a country to receive an adequacy decision is that the country must comply with the core principles of data privacy.[105] These principles are the purpose limitation principle, the data quality principle, the proportionality principle, the transparency principle, and the security principle.[106] The United States has never tried to get an

[102] Randy E. Barnett, Andrew Koppelman, https://constitutioncenter.org/interactive-constitution/interpretation/article-i/clauses/752.
[103] W. Gregory Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, 29 Wash. INT'l L.J. 485 (2020).
[104] Briseida Sofia Jimenez-Gomez, *Cross-Border Data Transfers between the EU and the U.S.: A Transatlantic Dispute*, 19 Santa CLARA J. INT'l L. 1 (2021).
[105] Id. at 12.
[106] Id.

adequacy decision because there is a high probability that the request would be denied because the US does not comply with the core principles listed above.[107]

Because the US does not have an adequacy decision, companies located here must rely on agreements between the United States and the EU. The most recent agreement between the two is the Privacy Shield. The purpose of this document is to protect the fundamental rights of EU citizens whose personal data is transferred to the US for commercial purposes.[108] Under this agreement US companies that want to collect and process data from the EU must receive a certain certification which shows they are compliant with major data privacy regulation put forth by the GDPR. The Privacy Shield places stricter obligations on certified companies regarding how long the company can retain personal data and the conditions under which data can be shared with third parties outside of the framework. [109]

A major issue with relying on agreements rather than receiving an adequacy decision is that companies that receive certification can be found to no longer be in compliance and receive heavy fines. An example of this can be seen when looking at Microsoft. Less than a month after the GDPR was put into effect, Microsoft Office, which was certified under the Privacy Shield, was found to no longer be compliant with the GDPR in Germany.[110] Microsoft decided to close the data servers they had located in

---

[107] Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93 (2020).

[108] Elaine Fahey & Fabien Terpan, *Torn between Institutionalisation & Judicialisation: The Demise of the EU-US Privacy Shield*, 28 IND. J. GLOBAL LEGAL Stud. 205 (2021).

[109] Elaine Fahey & Fabien Terpan, *Torn between Institutionalisation & Judicialisation: The Demise of the EU-US Privacy Shield*, 28 IND. J. GLOBAL LEGAL Stud. 205 (2021).

[110] Elisabeth Meddin, *The Cost of Ensuring Privacy: How the General Data Protection Regulation Acts as a Barrier to Trade in Violation of Articles XVI and XVII of the General Agreement on Trade in Services*, 35 AM. U. INT'l L. REV. 997 (2020).

Germany which was the driving factor of them no longer being in compliance.[111] This left Microsoft with two options, either reopen the server or pay the hefty fines delineated within the GDPR.[112]

China also requires that companies that process data outside of the country receive special consent from the government to collect, process, and store the data of Chinese citizens. Because the United States does not provide the basic principles of data protection US companies are struggling to maintain a strong presence in the countries that do provide these protections to its citizens. US companies are having to either adopt separate compliance measures for users of their sites based on the user's location or adopt a single platform that complies with all of the requirements of the countries the company is located within.[113] Both options carry tradeoffs, but the adoption of one comprehensive privacy standard worldwide for the collection and processing of personal data has a clear strategic advantage.[114] Countries will not fine a company for providing more protection then required, but will have consequences for companies that do not provide enough protection. The United States needs to pass legislation that will allow countries to trust that US companies will protect the data privacy rights of their citizens. The traditional foreign allies of the United States were once willing to tolerate the United States' laissez faire approach to data privacy and protection, but it is becoming evident that this

[111] Id. at 1008.
[112] Id.
[113] W. Gregory Voss & Kimberly A. Houser, *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies*, 56 AM. Bus. L.J. 287 (2019).
[114] Id. at 340.

approach will no longer be the strategically optimal posture from the perspective of US companies.[115]

Conclusion

In 1890 Samuel Warren and Justice Brandeis stated that common law should grow to meet the demands of society and that the development of the law was inevitable as the legal community identified new rights.[116] that the spirit of their insight seems to be reflected in the data privacy regulations of the European Union, China, and the United States. All three countries have stated that data privacy is a right that should be given to all. Despite this general consensus, only two of the three have done anything to adapt to this newfound right. The European Union and China have both taken steps to create new legislation that helps protect this newly-recognized right. The United States, however, has not taken acted at the national level to provide comprehensive data privacy protections. The US at the federal level is relying on old laws to solve a new problem. The states in the United States are starting to take matters into their own hands. The desirability of this approach has caused a divide in public policy circles.

I believe that the United States should follow the lead of the EU and China by establishing basic data privacy regulations at the federal level as well as a committee that is focused on data regulations. Companies like Google, Facebook, and TikTok are all receiving a financial gain by collecting, storing, and selling data, so it is necessary to provide restrictions and rights to protect individuals just like those given in relation to any other industry. It is essential for lawmakers to adapt to the ever-changing world that

---

[115] Kevin D. Benish, *Whose Law Governs Your Data: Takedown Orders and Territoriality in Comparative Perspective*, 55 WILLAMETTE L. REV. 599 (2019).
[116] Thomas Gerhart, *AB 2182 And Chapter 55: Enacting Privacy Regulations in the Face of Legislative Complacency,* 50 U. PAC. L. REV. 177 (2019).

we live in. Technology is a very powerful tool that must be regulated in order to provide safety and comfort to everyone who takes part in it. By examining the reaction of countries like the EU and China, the United States can see that it is possible to establish regulations at the federal level, and that doing so would allow American citizens to see what rights and protections are available to individuals in other countries. This research is important to establish a comparative overview of the approaches surrounding the idea of providing data privacy in a world that relies on the collection of data. This topic will continue to expand and evolve, so it is important as individuals that we do our own research to understand how to protect ourselves in the ever-changing world of technology.