Saint Louis University Law Journal

Volume 65
Number 4 *Tradeoffs: Technology, Privacy, and the Law (Summer 2021)*

Article 9

2021

Data Privacy: One Universal Regulation Eliminating the Many States of Legal Uncertainty

Tiffany Light

DATA PRIVACY: ONE UNIVERSAL REGULATION ELIMINATING THE MANY STATES OF LEGAL UNCERTAINTY

ABSTRACT

Although privacy has been around for quite some time, it has picked up speed within the last fifty years or so. Triggered by the advancements in technology that make the collection, storage, and use of data commonplace in today's data-driven world, new privacy regulations and data protection standards have begun to spread like wildfire across the globe. Consumers continue to advocate for their right to privacy as they face the privacy paradox—the desire to protect one's own privacy, while at the same time being forced to give it up as the cost of doing business in our data driven world. With the prevalence of data breaches, which are costly to individuals and organizations alike, the European Union took big steps to protect consumer data. In the United States, companies of all sizes like Amazon and Evite are scrambling to achieve compliance with these standards as they come up one at a time. However, the differences between individual regulations make it quite onerous for companies to comply with them all. The ability to comply is directly related to the number of resources an organization possesses. The more resourceful the organization is, the more likely it will achieve compliance. The less resourceful, the less likely the organization will achieve compliance resulting in dangerous practices like feigning ignorance or actively avoiding compliance efforts altogether. Noncompliance hurts consumers as evidenced by the effects of data breaches and identity theft, but it also hurts organizations through loss of business because they cannot compete the way that other organizations can. The best way to ensure data protection is for the United States federal government to implement a universal standard for its companies to adhere to. If this singular standard can incorporate the prominent aspects of other privacy regulations from around the world, organizations will be better equipped to compete and secure their place in the international market.

> Knowledge is power, and in the internet age knowledge is derived from data. Our personal data is what powers today's data-driven economy and the wealth it generates. It's time we had control over the use of our personal data. That includes keeping it private . . . [let us lead] the way [by] putting people first in the Age of the Internet.[1]

INTRODUCTION

We live in an increasingly globalized world where technological advancements have allowed us to engage in electronic commerce and share data across local, national, and international borders. Personal information and consumer data have become monetizable assets, including basic information such as name, address, and telephone number. However, that is just the beginning; physical locations, activity on social media, and even search history are all being monitored as well. This data is collected, stored, and can be "circulated across the globe in a matter of seconds" to those that are willing to pay the right price.[2] The technology industry has worked diligently to produce powerful algorithms with the ability to analyze data, anticipate consumer preferences based on that data, and target advertisements based on those predictions.[3] Technological advancements such as targeted advertising have resulted in a substantial shift and have created an entire subset in the market devoted to consumer data. Indeed, some businesses operate solely on the commercial use of data. Even if just as a secondary purpose, most other businesses use data commercially too. Consumers fear their personal information may end up in the wrong hands and often try to protect their data in cumbersome ways.

It is undeniable that data analytics can be beneficial, but a Pew Research poll discovered that approximately eighty-one percent of adults in the United States felt that the potential risks of data collection outweighed the benefits.[4] Not surprisingly, the majority of adults in the United States also feel that they have either little control over their data once it has been collected or none at all.[5] What is surprising, however, is just how many people consent to the collection

1. Press Release, Xavier Becerra, California Attorney General, Proposed Regulations Under the California Consumer Privacy Act (Oct. 10, 2019), https://www.oag.ca.gov/news/press-releases/attorney-general-becerra-publicly-releases-proposed-regulations-under-california [https://perma.cc/Q7K6-MWGE].

2. Matthew Humerick, *The Tortoise and the Hare of International Data Privacy Law: Can the United States Catch Up to Rising Global Standards*, 27 CATH. U. J. L. & TECH. 77, 78 (2018).

3. Oliver Sylvain, *The Market for User Data*, 29 FORDHAM INTELL. PROP., MEDIA & ENT. L. J. 1087, 1089 (2018).

4. Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/6N9K-F3FC].

5. *Id.*

of data despite its risks. Therein lies the privacy paradox. People care about their privacy, yet they are willing to hand over their personal data—without hesitation—when asked to do so.[6] Even when consumers can opt-out, only ten percent actually say no to having their data collected, used, or sold.[7] After Europe's comprehensive privacy protection called the General Data Protection Regulation ("GDPR") went into effect, some reports show that "ninety-five percent of consumers still chose to be tracked in exchange for access to websites and services."[8] This is likely because consumers that do not have experience with the choice to opt-out think they can only use online services by agreeing to the privacy policy, accepting the cookies, and handing over their personal information.[9]

The data-collection process has become so routine that people do not think twice until a data breach occurs. In the first half of 2019 alone, more than four *billion* records were compromised due to data breaches around the world.[10] These breaches can result in significant damage to individual lives and corporate reputations—both of which can take a long time to heal—the average global cost to a company is around $3.86 million.[11] Everyone is affected by data breaches in one way or another, so finding the balance and affording the right level of privacy through privacy protections should be a priority nationally and internationally as well.

This article suggests that the United States needs to develop a long-term solution to protect consumer privacy from data breaches if it wants to remain a serious competitor in the global market, specifically a comprehensive federal statute. Privacy standards have significantly evolved in over 100 countries around the world including countries in the European Union ("EU"), South America, and Asia.[12] The United States is lagging behind as it has only just

6. Susan Athey et al., *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*, (Nat'l Bureau of Econ. Rsch., Working Paper No. 23488, 2017).

7. Sam Dean, *California is Rewriting the Rules of the Internet and Businesses are Scrambling to Keep Up*, L.A. TIMES (Dec. 26, 2019), https://www.latimes.com/business/technology/story/2019-12-26/california-internet-data-privacy-law [https://perma.cc/7SZ5-8HD7].

8. *Id.*

9. Humerick, *supra* note 2, at 78–79.

10. Davey Winder, *Data Breaches Expose 4.1 Billion Records in First Six Months of 2019*, FORBES (Aug. 20, 2019), https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#7d1d7121bd54 [https://perma.cc/V3JX-388J].

11. Alison Grace Johansen, *What is a Data Breach?*, NORTON SECURITY (Mar. 10, 2020), https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html [https://perma.cc/MT8Y-G4SK].

12. 107 countries around the world have legislation in place concerning data privacy. *See Data Protection and Privacy Legislation Worldwide*, UNITED NATIONS CONF. ON TRADE & DEV., https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx [https://perma.cc/FQ98-ZKEM].

begun to develop cursory regulations at the state level. Although these individual regulations share a similar goal in protecting consumer privacy, they are not uniform, and they do not offer the extensive protections that are being developed by countries across the world. The differences between individual regulations in the United States, compared with those in other countries, will inevitably lead to a compliance nightmare. Small businesses may be disproportionately affected, and the costs associated with compliance may be passed on to the consumer. The United States may suffer a disadvantage if this developmental lag results in not being able to use data commercially in accordance with the law of other countries, while those same countries are ahead of the game having already worked out some of the kinks. Therefore, in order for the United States to effectively compete in the international market, the only true solution is to enact a federal data privacy regulation with breadth similar to that of the GDPR.

I. THE DEVELOPMENT OF PRIVACY STANDARDS: LOOKING AT THE LAST FIFTY YEARS

The general concept of privacy has been around for ages, and the protections in place to help people feel secure have developed along the way. Internationally, privacy is considered a human right according to Article 12 of the United Nations Declaration of Human Rights, which states: "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence . . ."[13] However, the definition and scope of the right to privacy depends on where one is located in the world. Some countries, like members of the EU, have robust and comprehensive protections in place, while others, such as the United States, only protect certain sector-specific types of information. This section will explore some of the most recent developments in the area of data privacy, focusing specifically on those in the EU since 1980 and those in the United States since the mid 1990s.

A. Data Privacy in the European Union Since 1980

When it comes to data privacy, the Organization for Economic Co-operation and Development ("OECD") first published Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in Europe in 1980.[14] Although these guidelines provided a solid foundation for privacy protection across the EU, they were not binding on the EU as a whole, so privacy laws still varied by country. Over a decade later, in response to this dilemma, the EU tried harmonizing data protection laws through its adoption of the 1995 Data Protection Directive ("1995 Directive").[15] This Directive held for over twenty

13. G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948).

14. *How Did We Get Here*, EUGDPR.ORG (Sept. 16, 2019), https://eugdpr.org/the-process/how-did-we-get-here/ [https://perma.cc/8LHJ-HHEF].

15. *Id.*

years until advancements in technology and the growing number of data breaches encouraged the EU to enact the General Data Protection Regulation ("GDPR") in 2016.[16] Prior to the GDPR, there was still not one all-encompassing regulation for notification after a privacy breach in the EU because the 1995 Directive allowed each member state to pass its own legislation.[17] This meant that although countries might have agreed that notification of a breach was mandatory, their individual approaches to regulating the notification process varied greatly, which understandably led to confusion amongst countries.[18]

The GDPR is an extensive data protection law designed in 2016 to expand the reach of the 1995 Directive to consistently cover all member states of the EU and protect individuals from the widespread leakage of private information.[19] It is the "toughest privacy and security law in the world," because it is far-reaching and imposes obligations on anyone that collects data on EU individuals, no matter where they are from.[20] The GDPR represents a "firm stance on data privacy and security at a time when more people are entrusting their personal data . . . and breaches are a daily occurrence."[21] It has been in effect since May 25, 2018, and the rest of the world has taken notice over the last couple of years.[22] Countries outside of the EU are implementing their own comprehensive data privacy legislation similar to the GDPR. For example, Brazil's law goes into force starting in August of 2021[23] and Thailand's law went into force on May 28, 2020.[24] These developments indicate that we are potentially in the midst of a data privacy revolution.

16. *Id.*

17. Josephine Wolff, *How Is the GDPR Doing?*, SLATE (Mar. 20, 2019), https://slate.com/technology/2019/03/gdpr-one-year-anniversary-breach-notification-fines.html [https://perma.cc/XVS3-8WHR].

18. *Id.* For example, Austria required its companies to notify only those whose data had been affected. *Id.* Meanwhile, Norway required its companies to notify the data protection authority, and Germany required its companies to notify both. *Id.* Other countries, such as Ireland and Italy, simply had voluntary reporting systems. *Id.*

19. *What is GDPR, the EU's New Data Protection Law?*, GDPREU.ORG, https://gdpr.eu/what-is-gdpr/ [https://perma.cc/HVH8-RMP9].

20. *Id.*

21. *Id.*

22. *Facts and Questions*, GDPREU.ORG, https://www.gdpreu.org/faq/ [https://perma.cc/85G4-U997].

23. Aaron K. Tantleff et al., *Brazilian Government Makes the LGPD Effective Immediately*, 11 NAT'L L. REV. 18 (Sept. 10, 2020), https://www.natlawreview.com/article/brazilian-government-makes-lgpd-effective-imminently [https://perma.cc/3DN8-2XW8].

24. Annie Greenley-Giudici, *Thailand's Personal Data Protection Act (PDPA) Comes into Effect*, TRUSTARC (July 2, 2019), https://www.trustarc.com/blog/2019/07/02/thailands-personal-data-protection-act-pdpa-comes-into-effect/ [https://perma.cc/GGS8-PD3U].

B. Data Privacy in the United States Since the Mid-1990s

In contrast to development in the EU, privacy standards in the United States have been moving at glacial speed because progress in bi-partisan politics is a piecemeal process. The primary focus thus far has been the adoption of new legislative acts to protect individual sectors, one at a time. Today, there are "more than 20 sector specific federal data security laws, as well as hundreds of privacy laws among [the United States]."[25] Perhaps the most well-known is the Health Insurance Portability and Accountability Act ("HIPAA"), which regulates both the use and disclosure of a patient's protected health information.[26] Other acts that focus on specialized areas of privacy are the Gramm-Leach-Bliley Act ("GLBA"), which requires financial institutions to explain how they share and protect their customer's private information;[27] the Family Educational Rights and Privacy Act ("FERPA"), which regulates access to school records for both the parent and the student;[28] the Children's Online Privacy Protection Act ("COPPA"), which regulates data of children under the age of thirteen;[29] and the Telephone Consumer Protection Act ("TCPA"), which regulates telemarketers and imposes penalties on callers that disregard the "Do-Not-Call" registry.[30]

These acts cover privacy from a narrow lens and leave the majority of areas unprotected, including consumer data privacy. Enforcement of privacy and data security, through these acts and others, has been primarily conducted by the Federal Trade Commission ("FTC").[31] To date, the FTC has brought hundreds of enforcement actions against both well-known and lesser-known companies to protect the privacy of consumer information.[32] It has the authority to "police unfair and deceptive trade practices," including corporate privacy policies; however, there are very few judicial decisions to demonstrate its impact because most cases result in a settlement.[33] While the FTC is powerful and possesses the competency to protect consumer privacy, there are concerns that it does not have

25. WILLIAM LEICHTER & DAVID BERMAN, GLOBAL GUIDE TO DATA PROTECTION LAWS: UNDERSTANDING PRIVACY AND COMPLIANCE REQUIREMENTS IN MORE THAN 80 COUNTRIES 26 (2017).

26. Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936, 1992, 2009, 2021, 2030, 2033 (1996).

27. Gramm-Leach-Bliley Act, Pub. L. 106–102, 113 Stat. 1338, 1436 (1999).

28. 20 U.S.C. § 1232g (2013).

29. 15 U.S.C. § 6501–6505 (1998).

30. 47 U.S.C. § 227 (2019).

31. Press Release, Federal Trade Commission, 2018 Privacy and Data Security Update (Mar. 15, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-releases-2018-privacy-data-security-update [https://perma.cc/D5N2-AX2Y].

32. FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2018 3 (2018).

33. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585 (2014).

the resources necessary to enforce regulations across all levels.[34] It seems to have developed a top-down approach by focusing its resources on large players and using them as an example to small and mid-sized companies.[35] This strategy is largely effective, but the allocation of additional resources—or the creation of an enforcement agency devoted to privacy—would further support consumer protection efforts.[36] That being said, the federal process to develop robust privacy regulations, much less new agencies, is "too slow and incremental to keep pace with the ever-changing technological environment."[37]

All fifty of the United States have adopted their own—at least baseline—privacy regulations, including the proper way to respond to data breaches.[38] Many of these regulations have existed for years and cover basic concepts such as how organizations use information, the type of information collected, and variants based on specific industry. The first state to expand and adopt a comprehensive consumer data privacy law was California when it enacted the California Consumer Privacy Act ("CCPA"), that went into effect on January 1, 2020.[39] It was designed to give consumers the right to know what personal information companies have collected, to have companies delete the data, and to forbid them from sharing the data.[40] It also requires companies to give consumers upfront notice regarding the information they collect so consumers have the choice to opt-out.[41] After the CCPA was enacted, experts were concerned with the ambiguities in its provisions that could result in confusion and a wide array of differing applications.[42] For instance, one company may be advised to give consumers a chance to opt-out if they do not want their data shared, while another company may be advised to ask those who wish to opt-out to simply delete their accounts.[43] These interpretation issues and a demand for

34. Chris Jay Hoofnagle et al., *The FTC Can Rise to the Privacy Challenge, but Not Without Help from Congress*, BROOKINGS (Aug. 8, 2019), https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/ [https://perma.cc/V45B-WHM7].

35. *Id.*

36. *Id.*

37. Humerick, *supra* note 2, at 114.

38. Michael Beckerman, *Americans Will Pay a Price for State Privacy Laws*, N.Y. TIMES (Oct. 14, 2019), https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html [https://perma.cc/QGB7-U64E].

39. Jeff John Roberts, *Here Comes America's First Privacy Law: What the CCPA Means for Businesses and Consumers*, FORTUNE (Sept. 13, 2019), https://fortune.com/2019/09/13/what-is-ccpa-compliance-california-data-privacy-law/ [https://perma.cc/5ZRK-AENT].

40. *Id.*

41. *Id.*

42. Natasha Singer, *What Does California's New Data Privacy Law Mean? Nobody Agrees*, N.Y. TIMES (Dec. 29, 2019), https://www.nytimes.com/2019/12/29/technology/california-privacy-law.html [https://perma.cc/HQ72-W8DP].

43. *Id.*

greater consumer protection sparked the passage of California's Proposition 24, better known as the California Privacy Rights Act ("CPRA"), in November of 2020.[44] The CPRA is being called the "CCPA 2.0" because it effectively expands the CCPA and will supersede it on January 1, 2023, although some provisions are effective immediately.[45]

The enactment of the CCPA, and subsequent CPRA, has sparked the "California Effect" in the United States—the "tendency of the other states to follow California's lead in areas such as consumer rights and environmental standards."[46] This was an impactful move because the strength of California's economy and size alone provide a huge impetus to encourage companies to adopt its regulations across the nation.[47] Several other states have started to follow in California's footsteps to develop their own data privacy legislation and allow consumers to have more control over what data companies have about them and how that data is used. One of the first states to take action was New York when it proposed the New York Privacy Act ("NYPA"), which would require consumers to affirmatively opt in and allow their data to be used for commercial purposes instead of having the option to opt out.[48] The NYPA is currently facing opposition based on its private right of action, which would allow individual consumers to bring suit against companies over violations of the law.[49] It would also require businesses to act as "data fiduciaries" and "act in the best interest of the consumer."[50] The company would be unable to benefit from the use of consumer data in a way that would be detrimental to the consumer.[51] Virginia was the second state to enact a comprehensive data privacy regulation called the Consumer Data Protection Act ("CDPA") on March 2, 2021, that will go into effect on January 1, 2023.[52] It exempts certain kinds of

44. Joseph J. Lazzarotti et al., *California Passes Prop 24: Here Comes the CCPA 2.0*, NAT'L L. REV. (Nov. 5, 2020), https://www.natlawreview.com/article/california-passes-prop-24-here-comes-ccpa-20 [https://perma.cc/3GW4-CQSF].

45. *Id.*

46. Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 405 (2019).

47. *Id.*

48. Dan M. Clark, *Private Right to Sue Under NY Data Privacy Bill Could Clog Courts, Business Leaders Say*, N.Y. L. J. ONLINE (Nov. 22, 2019), https://www.law.com/newyorklawjournal/2019/11/22/private-right-to-sue-under-ny-data-privacy-bill-could-clog-courts-business-leaders-say/?slreturn=20200005185546 [https://perma.cc/J5GP-2BKS].

49. *Id.*

50. Issie Lapowsky, *New York's Privacy Bill Is Even Bolder Than California's*, WIRED (June 4, 2019), https://www.wired.com/story/new-york-privacy-act-bolder/ [https://perma.cc/V5CZ-NDJX].

51. *Id.*

52. Gretchen A. Ramos, *Virginia Enacts Comprehensive Data Privacy Legislation*, NAT'L L. REV. (Mar. 3, 2021), https://www.natlawreview.com/article/virginia-enacts-comprehensive-data-privacy-legislation [https://perma.cc/N8Q8-EP6K].

data, including those individually regulated through HIPAA, GLBA, FERPA, COPPA, and TCPA.[53] The CDPA, like the CCPA and CPRA, provides consumer rights to receive notice, access personal data, data portability, correct errors in personal data, delete personal data, opt out, and non-discrimination.[54] However, it does not provide a private right of action, and is only subject to enforcement through the state's attorney general's office, and provides a thirty-day right to cure an alleged violation.[55] New York and Virginia are not alone in their efforts, as more than twenty other states have also introduced or passed similar bills in their state legislatures.[56] It is evident from this new wave of proposed legislation that change is coming and it is only a matter of time before the United States has fifty different privacy standards.

This kind of patchwork system of state laws will likely lead to conflict and confusion based on terminology, requirements, and standards. As an example, consider how the State of Illinois defines personal information:

> An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredacted or otherwise read the name or data elements have been acquired without authorization through the breach of security: (A) Social Security number; (B) Driver's license number or State identification card number; (C) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; (D) Medical information; (E) Health insurance information; (F) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.[57]

Virginia, on the other hand, defines personal information as:

> Any information that is linked or reasonably linkable to an identified or identifiable natural person. 'Personal data' does not include de-identified data or publicly available information.[58]

53. *Id.*

54. *Id.*

55. *Id.*

56. THE BUREAU OF NAT'L AFFAIRS, INC., CCPA COPYCAT LEGISLATIVE PROPOSAL TRACKER (Bloomberg Law ed., 2020) (Arizona, Connecticut, Florida, Hawaii, Illinois, Maine, Maryland, Massachusetts, Minnesota, Mississippi, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, Oklahoma, Pennsylvania, Rhode Island, Texas, Vermont, Virginia, and Washington).

57. 815 ILL. COMP. STAT. 530/5 (2017).

58. VA. CODE ANN. § 59.1-571 (2021).

The only real similarity between these two is that "personal [data] information does not include . . . publicly available information."[59] It is clear that the United States will soon be facing the same challenges that the EU did before enacting the GDPR. If just the definition of "personal information" differs as in the example provided above, one can imagine how much else could differ between states. This could pose a significant problem for American consumers. Research indicates that more than half of consumers say they are already confused and understand either very little or nothing at all about the laws and regulations that are currently in place to protect their data privacy.[60] Further complication through differing data privacy regulations will not improve these statistics. Although this is certainly a problem for individual consumers, the problem is amplified for business owners. Differing state standards result in a higher administrative burden for businesses to stay informed in terms of their compliance obligations. It could also pose problems in terms of full and fair enforcement. One thing is for sure: it means job security for privacy lawyers and data privacy regulators!

II. APPLICATION OF PRIVACY REGULATIONS: COMPLIANCE

Businesses have an obligation to comply with the law, which means they must not only be aware of laws currently in place, but also those that are working their way through the legislature. Staying up to date on the latest regulations is easier said than done, but the task becomes even more difficult when there are differing standards across not only the United States, but across the world as well. In our increasingly globalized economy, businesses often operate in more than one state and more than one country. To do so, they must be familiar with and understand the differing standards amongst them. For purposes of this discussion, the two data protection provisions most relevant for companies and currently in effect are the CCPA and the GDPR. They differ in key ways, mainly with respect to their penalties for noncompliance, reach (who the law applies to and what kind of data is protected), and requirements for compliance. This section is dedicated to understanding the practical application of both the CCPA and GDPR, as they would apply to companies that conduct business in both jurisdictions, to demonstrate the challenges that are associated with compliance.

A. Understanding the Application of the CCPA and GDPR

Recognizing what it means to be noncompliant is fundamental to understanding what it means to be in compliance. Typically, noncompliance authorizes regulators to levy penalties such as monetary fines and injunctive or declaratory relief, which can be dangerous for companies of all sizes because it

59. 815 ILL. COMP. STAT. 530/5 (2017); VA. CODE ANN. § 59.1-571 (2021).

60. Brooke Auxier et al., *supra* note 4.

can result in extreme cost. When considering compliance with the GDPR, Article 83 provides that failure to comply can result in administrative fines that are to be determined in each "individual case [as] effective, proportionate and dissuasive."[61] These fines can range anywhere between the higher of either ten million euros or two percent of the total worldwide annual turnover of the preceding financial year; and the higher of either twenty million euros or four percent of the total worldwide annual turnover of the preceding financial year.[62] This suggests that penalties are supposed to be preemptive and prevent breaches of privacy from occurring in the first place. CCPA penalties, on the other hand, are reactionary and focus on the consequences of noncompliance. A violation of the CCPA can result in both civil penalties and private lawsuits by consumers for data breaches. After a business is notified that they are not in compliance, they have thirty days to cure any alleged noncompliance.[63] Failure to do so could result in an action brought by the California Attorney General for civil penalties ranging between $2,500 and $7,500 for *each violation* based on whether the violation was intentional or not.[64] If there is a data breach due to the company's failure to comply with the CCPA, individuals have the right to bring a private civil suit for the greater of damages between $100 and $750 per consumer per incident or actual damages.[65] The main change under Proposition 24 is the creation of the California Privacy Protection Agency ("CPPA") to implement and enforce California privacy regulations alongside the California Attorney General.[66] Fortunately for many companies, the CCPA originally barred the Attorney General from bringing an enforcement action until the sooner of six months after the final publication, or July 1, 2020.[67] It should be noted that the goal of the delayed effective date (January 1, 2023) for the CPRA is to provide companies additional time to figure out what they need to do to comply.[68] However, just because a company had a grace period to ensure they are in compliance with the CCPA or CPRA, does not mean that achieving compliance is easy or without cost.

61. Regulation 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), 2016 O.J. (L. 119) art. 83 [hereinafter GDPR].

62. *Id.* To put these figures in perspective, as of this writing, ten million euros is nearly twelve million dollars and twenty million euros is nearly twenty-four million dollars.

63. CAL. CIV. CODE § 1798.150 (2018). Note that this right to cure will be reduced when the CPRA goes into effect on January 1, 2023, as implementation of reasonable security procedures does not count. CAL. CIV. CODE § 1798.150 (2020).

64. CAL. CIV. CODE § 1798.155(b) (2018).

65. *Id.* § 1798.150(a).

66. CAL. CIV. CODE § 1798.199.10 (2020).

67. CAL. CIV. CODE § 1798.185(c) (2018).

68. It should be noted that the CPRA contains a look back period beginning January 1, 2022. CAL. CIV. CODE § 1798.130 (2020).

The risk of penalties for noncompliance clearly serves to encourage compliance, so the next step is determining how to avoid a failure to comply. This section gives a brief overview of some of those components. Under the CCPA, for-profit companies must comply if they conduct business in California and either: have annual gross revenue over twenty-five million dollars; annually buy, receive, sell, or share for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or derive fifty percent or more of annual revenue from selling consumers' personal information.[69] Note that the CCPA is not limited to businesses within the state of California, just those that *conduct business* there. In 2023, the CPRA will keep the twenty-five million dollar threshold, but raises the "annually buys, sells, or shares" threshold to 100,000 or more consumers or households.[70] It also adds "sharing" to the final threshold regarding fifty percent of revenue from sale of personal information.[71] Compare these quite specific levels to the generalized standard under the GDPR, which simply requires all companies to comply if they are located in the EU, offer goods or services to EU residents, or monitor the behavior of EU residents.[72] These thresholds are quite different, but similar in that neither regulation limits its application to entities with a physical presence in that jurisdiction.

Another key difference is in the kind of data that is protected. The GDPR protects the processing of all personal data,[73] while the CCPA has exceptions to the kinds of personal data that it protects, such as medical information and data that is already legally available to the general public.[74] The CPRA will go even further to create an entirely new category of "sensitive personal information" to expand on what was already included in personal information, bringing protection closer to the all-inclusive coverage under the GDPR.[75] In order for any company to comply with a data privacy regulation, it must be familiar with and have a solid understanding of the kind of data that it collects. Services are available to help companies understand their data practices, but this comes at a price.

As mentioned previously, the CCPA provides consumers with the right to know (specifically the right to request information) about what kind of data is being collected, how it is being stored, and what it is being used for.[76] A company must be able to promptly respond to those requests. The CCPA also requires that consumers receive notice in the form of disclosure at or before the

69. CAL. CIV. CODE § 1798.140(c)(1) (2018).
70. CAL. CIV. CODE § 1798.140(d)(1) (2020).
71. *Id.*
72. GDPR, *supra* note 61, at art. 3.
73. *Id.* at art. 2.
74. CAL. CIV. CODE § 1798.145(c) (2018).
75. CAL. CIV. CODE § 1798.140(ae) (2020); *id.* § 1798.140(v).
76. CAL. CIV. CODE § 1798.110 (2018).

point in which their data is being collected.[77] This disclosure should also provide an "opt-out" provision that allows the consumer to direct the company to refrain from selling their personal information.[78] Thus, under the CCPA, companies should have a comprehensive privacy disclosure somewhere on their website that is easily accessible to consumers so that they may choose to opt-out. This differs slightly from the GDPR, where the concept of "opt-in" is used to obtain "freely given, specific, [and] informed" consent from the consumer "signif[ying] agreement to the processing of personal data."[79] Finally, an important consideration that often goes unrealized is the need to develop a method to specifically protect an ogranization's security procedures and practices. The GDPR requires that companies recognize, isolate, mitigate, and respond to data breaches, and report them to regulators within seventy-two hours of becoming aware of the incident.[80] This is a substantial but essential undertaking. As mentioned previously, data breaches were devastating for businesses even prior to the enactment of either the GDPR or the CCPA. Now, there are clear and significant penalties in place to punish companies for failing to comply in an effort to prevent future data breaches.

B. Compliance Efforts: Case Studies

To demonstrate the challenges that individual businesses face with compliance, this Article considers a couple of case studies. The following section will examine the approaches that different sized companies took to achieve compliance. The first case study considers the experience of a large company, and the second considers the experience of a smaller business.

1. Amazon Web Services

The larger the company, the greater advantage it has in the world market. In terms of financial resources alone, large companies can hire experts, purchase elaborate software, and acquire nearly anything else they need to ensure that they are in compliance with the law. Amazon Web Services ("Amazon") has an estimated 25,000 employees and will be used to demonstrate the advantages that larger companies have in terms of compliance with data privacy regulations.[81] Amazon went above and beyond to ensure it was in compliance with the GDPR long before it went into effect. It had a service readiness audit conducted to see whether it had the appropriate measures in place and obtained ISO certifications

77. *Id.* § 1798.100.

78. *Id.* § 1798.120.

79. GDPR, *supra* note 61, at art. 4.

80. *Id.* at art. 33.

81. *AWS*, OWLER, https://www.owler.com/company/amazon-web-services [https://perma.cc/57UJ-BLL3].

in areas that were not even required by the GDPR. [82] In addition, it published a twenty-seven-page whitepaper report on its compliance with the GDPR to inform consumers about the measures that it had taken to ensure their privacy was secure.[83] In preparation for the CCPA, Amazon published a thirty-page whitepaper report on its compliance before it even went into effect.[84] This was a great strategy for Amazon, who chose to use the obligation to comply as leverage to demonstrate its dedication to its consumers. One author explained that "your ability to protect individuals will distinguish your company from competitors who have taken a passive approach or who ignore their responsibilities."[85]

However, it should be noted that Amazon's Vice President and Associate General Counsel Andrew DeVore claimed before the United States Senate that the GDPR "required us to divert significant resources to administrative and record-keeping tasks and away from inventing new features for customers and our core mission of providing better service, more selection, and lower prices."[86] He was not alone in his frustration, as Google's Chief Privacy Officer also offered written testimony estimating that "Google's workforce spent hundreds of years of human time" to bring the company into compliance with the GDPR.[87] In both cases, Amazon and Google expressed concern for small and medium sized companies that do not have the same resources. They demonstrated that compliance was not easy by describing the challenges that their respective companies faced. Even large companies that have claimed to be in compliance with the GDPR have been investigated for noncompliance, including Facebook, WhatsApp, Instagram, Twitter, LinkedIn, Apple, Google, Quantcast, Marriott,

82. 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, 334 (2019).

83. *Navigating GDPR Compliance on AWS,* AMAZON WEB SERVICES (Dec. 2020), https://d1.awsstatic.com/whitepapers/compliance/GDPR_Compliance_on_AWS.pdf [https://perma.cc/5ZLR-MWXE].

84. *Preparing for the California Consumer Privacy Act*, AMAZON WEB SERVICES (July 2019), https://d1.awsstatic.com/whitepapers/preparing-california-consumer-privacy-act.pdf [https://perma.cc/3XQR-J3WB].

85. Jordan Blanke, *Top Ten Reasons to be Optimistic About Privacy*, 55 IDAHO L. REV. 281, 302 (2019).

86. *Examining Safeguards for Consumer Data Privacy: Hearing Before the Senate Committee on Commerce, Science, and Transportation*, 115th Cong. (Sept. 26, 2018) (statement of Andrew DeVore, Vice President and Associate General Counsel, Amazon.com, Inc.), https://www.commerce.senate.gov/services/files/0F58A430-2037-4884-9B98-5FB3CA977838 [https://perma.cc/9EBA-VQ23].

87. *Examining Safeguards for Consumer Data Privacy: Hearing Before the Senate Committee on Commerce, Science, and Transportation*, 115th Cong. (Sept. 26, 2018) (written testimony of Keith Enright, Chief Privacy Officer, Google), https://www.commerce.senate.gov/services/files/5D32673E-D11D-4EE1-A7F3-8B03E407128D [https://perma.cc/3F2N-UWCQ].

and Verizon.[88] Since May of 2018, more than $417 million in fines have been imposed under the GDPR due to failure to comply resulting in data breaches.[89]

Both the CCPA and the GDPR reach large companies. These larger companies received a blessing in disguise by having to comply with the GDPR beginning in 2018 because much of the administrative burden required to comply with California's CCPA was already in the GDPR. The technical components are certainly not the exact same, but the point is that these companies did not have to start completely from scratch when the CCPA went into effect and could build upon the foundation that was already provided by the GDPR. Companies with significant resources, like Microsoft, can provide the same data privacy protection required by the GDPR to consumers worldwide.[90] By applying one standardized set of rules, Microsoft is avoiding the compliance nightmare in favor of efficiency and lowered compliance costs.[91] In that sense, large companies are better positioned to deal with increased regulations on data privacy simply due to their ability to afford and maintain compliance. Smaller companies, on the other hand, may be forced out of the market or business altogether by their inability to do so.

2. Evite

Smaller companies find themselves in a much less favorable position. They simply do not have the financial resources to hire experts or purchase elaborate software or other tools that they would need to ensure that they are in compliance with the law.[92] For instance, Evite has an estimated 269 employees and provides an example of how smaller businesses are burdened by the regulation.[93] It worked with two separate firms and spent more than one million dollars just to create a system that would help it understand its obligations under the CCPA and ultimately how to automatically comply with those regulations.[94] Evite's

88. U.S. INT'L TRADE COMM'N, ONE YEAR IN: GDPR FINES AND INVESTIGATIONS AGAINST U.S.-BASED FIRMS (Sept. 2019), https://www.usitc.gov/publications/332/executive_briefings/gdpr_enforcement.pdf [https://perma.cc/K2RZ-6UFM].

89. *Id.*

90. Voss & Houser, *supra* note 82, at 335.

91. *Id.*

92. It is important to note that finding data related to compliance for small companies was nearly impossible. The results of California's Standardized Regulatory Impact Assessment were based on a TrustArc survey that was only sent to businesses with 500 employees or more, which means that the report used to evaluate the impact of the CCPA has virtually no data on 99% of California businesses (those with fewer than 500 employees). BERKELEY ECON. ADVISING & RSCH., STANDARDIZED REGULATORY IMPACT ASSESSMENT: CALIFORNIA CONSUMER PRIVACY ACT OF 2018 REGULATIONS 10 (Aug. 2019), http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf [https://perma.cc/F6Z8-6T9E] [hereinafter 2019 REGULATORY IMPACT ASSESSMENT].

93. *Evite*, OWLER, https://www.owler.com/company/evite [https://perma.cc/X3HX-8PDC].

94. Singer, *supra* note 42.

system is not nearly as advanced as those of tech giants like Apple, Facebook, Google, Microsoft, and Twitter, who all have automated services enabling users to download personal data already in place.[95] Evite's situation demonstrates the dilemma for small businesses, because while Evite clearly had the resources necessary to establish their own compliance method, businesses that are less well-resourced will effectively be crippled by these complicated and non-standardized regulations. The sustainability of small businesses operating at either the local, state, or national level will depend on their ability to comply with such broadly different standards.

The GDPR can reach small and medium sized companies that conduct business with EU residents. In contrast, the CCPA's thresholds don't facially reach small businesses, but simple math indicates that it would only take 137 consumers, households, or devices a day to currently reach the 50,000 threshold.[96] The CPRA's heightened threshold of 100,000 consumers or households may reduce the applicability to smaller companies, but it will not eliminate it altogether.[97] Thus, it is imperative that all small businesses familiarize themselves with the requirements of the CCPA and CPRA so they are not blindsided by a noncompliance fine or civil lawsuit.

There are a couple effective approaches that a smaller business could take, including compliance and avoidance. As discussed below, compliance is expensive and extremely complex which means it is often not feasible for small businesses.[98] As data privacy standards continue to expand, giving greater protection to consumers, one strategy for businesses may be that if they are forced to comply and meet the standards of one state regulation, they may as well pick the most comprehensive and devote their resources to complying with that one. For many companies that have already gone to great lengths to comply with the GDPR, they could follow in Microsoft's footsteps and implement those changes to all their users in the United States instead of just focusing on

95. *Id.*

96. CAL. CIV. CODE § 1798.140(c)(1) (2019). Take 50,000 and divide by 365, the number of days in a year.

97. CAL. CIV. CODE § 1798.140(d)(1) (2020).

98. Craig McAllister, *What About Small Businesses? The GDPR and its Consequences for Small U.S. Based Companies*, 12 BROOK. J. CORP. FIN. & COM. L. 187, 197 (2017). *See also* E-mail from Mark Grace, Great Clips Franchisee, to Privacy Regulations Inbox (Oct. 11, 2019, 9:45 AM), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-comments-45day.pdf [https://perma.cc/SBX3-UWHF] (discussing the challenges of being a franchisee to an out-of-state franchisor and likely subject to the CCPA even though business only has 200 employees, but unable to comply because contractually required to operate under the franchisor's databases. Essentially, the franchisee can collect data, but not control its use or delete it because that is left to the franchisor. Although national franchisors undertake compliance efforts with federal regulations, they are less concerned about state level regulations until they become widely adopted. So, in the meantime, the burden and liability of compliance will fall upon the franchisee, who is stuck in the middle).

California.[99] Additionally, if small businesses could locate detailed information about the compliance efforts made by larger companies, it could be easier and more efficient to piggyback off their resources, but it is unclear whether that is realistic. Another option for small businesses is the avoidance strategy, which has two distinct methods. The first method of avoidance will still result in noncompliance, because it means that companies claim ignorance. They do not do anything and just try to fly under the radar as if the new privacy standards do not apply to them (even though the companies realize that they probably do apply). Even knowing the risk of being hit with noncompliance penalties or lawsuits, it still might be worth the gamble for some companies depending on the level of enforcement in a given jurisdiction. For instance, consider the extremely limited budget for the California attorney general whose office is likely to only conduct three enforcement actions each year.[100] At the outset, commentators have argued that these actions will be against large companies, because the attorney general said, "the bigger the company, the bigger the problem . . . the bigger the case will be."[101] In that scenario, it might be feasible for smaller companies to fly under the radar for a while without getting caught and use the extra time to finalize their compliance efforts. It should be noted that the CPRA's creation of the CPPA implies that enforcement will soon become a priority and trying to fly under the radar might not be the right choice considering the penalties discussed above for getting caught. The second method of avoidance does not result in noncompliance and has been employed by many American news outlets, such as the Los Angeles Times, the Chicago Tribune, and even the St. Louis Post Dispatch.[102] Instead of pretending that the privacy standards do not apply, small companies can just pull out of the market wherever they would be forced to comply with regulations that are beyond their current means. For instance, if an individual visits the website of a small company while physically located in Europe, they might see a message similar to this one:

> Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism.[103]

99. Kim Lyons, *No One is Ready for California's New Consumer Privacy Law*, THE VERGE (Dec. 31, 2019), https://www.theverge.com/2019/12/31/21039228/california-ccpa-facebook-microsoft-gdpr-privacy-law-consumer-data-regulation [https://perma.cc/J6HM-VUDA].

100. Rachael Myrow, *California Rings in the New Year with a New Data Privacy Law*, NPR (Dec. 30, 2019, 9:00 AM), https://www.npr.org/2019/12/30/791190150/california-rings-in-the-new-year-with-a-new-data-privacy-law [https://perma.cc/XKA9-N4KC].

101. *Id.*

102. Voss & Houser, *supra* note 82, at 330.

103. *Id.* at 330-331.

Of course, this method negatively impacts consumers' access to businesses and the company's access to the market, but it might be the most practical approach for small businesses because it relieves their duty to comply.[104] Otherwise small businesses would be plagued by "compliance fatigue" based on the nearly impossible task of developing a system of compliance that can adequately encompass state data privacy requirements for all fifty United States and the EU.[105]

Both larger and smaller businesses undoubtedly face challenges with compliance. However, there are even smaller local and family-owned businesses that are also vulnerable because they simply cannot compete. They are not even on the same playing field, and the devastating effect of such onerous regulations on these businesses should be taken into consideration as well.

C. Barriers to Compliance

A study on compliance with the GDPR indicated that small businesses were reporting the lowest readiness level while companies with over 5,000 employees had the highest.[106] It found the most common barriers to compliance were the need to make comprehensive changes to business practices, unrealistic demands from regulators, lack of experts knowledgeable about the regulation itself or how to respond to data breaches, insufficient budget, and too little time.[107] Seventy-two percent of companies indicated that they would have to invest in new technologies and services as well as undertake significant assessments of their ability to comply with the regulation.[108] For some, this means adding new staff like a data protection officer, creating an accountability framework and reporting structures, adjusting relationships with vendors, allocating a specific budget for compliance, or even closing overseas operations.[109] Thirty-nine percent of companies had not allocated a budget for complying with the GDPR, but those who did found that their budget reached millions of dollars annually. [110] Compliance is not cheap and while some companies are able to spend millions

104. Allison Grande, *EU Privacy Law Not Good Model for US*, LAW360 (Feb. 26, 2019, 10:31 PM), https://www.law360.com/articles/1132937/eu-privacy-law-not-good-model-for-us-house-panel-told [https://perma.cc/Y2CW-U9NB].

105. Taylor Armerding, *Awash in Regulations Companies Struggle with Compliance*, FORBES (Aug. 30, 2019, 9:18 AM), https://www.forbes.com/sites/taylorarmerding/2019/08/30/awash-in-regulations-companies-struggle-with-compliance/#10acd383150e [https://perma.cc/WZ9H-95LH].

106. PONEMON INSTITUTE, THE RACE TO GDPR: A STUDY OF COMPANIES IN THE UNITED STATES & EUROPE 2 (Apr. 2018), https://iapp.org/media/pdf/resource_center/Ponemon_race-to-gdpr.pdf [https://perma.cc/SDW4-9BA9].

107. *Id.* at 43.

108. *Id.* at 19.

109. *Id.*

110. *Id.* at 53.

of dollars to comply, smaller companies are struggling to do so.[111] A small business survey in the EU found that over half of small businesses spent between €1,000 and €50,000 on compliance, yet some spent over €1,000,000.[112] Another survey conducted one year after the GDPR went into effect found that seventy-nine percent of global businesses said they were either failing to meet regulatory requirements, having trouble keeping up to date, or both.[113] That is *after* spending significant funds to hire consultants and obtain technology to comply.

According to a survey conducted just ten months before the CCPA was set to go into effect, only fourteen percent of companies were compliant.[114] For many small businesses, the CCPA is the first comprehensive data privacy regulation that they have encountered, so these statistics are further reduced for companies that did not have to comply with the GDPR. Only six percent of those companies were compliant with the CCPA.[115] The Attorney General of California had a Standardized Regulatory Impact Assessment ("SRIA") prepared to measure the impact of the CCPA on California's businesses.[116] The SRIA concluded that the total cost of initial compliance would be approximately fifty-five billion dollars after breaking down the cost to businesses into four categories: legal, operational, technical, and business.[117] It assumed that businesses with less than twenty employees would incur initial compliance costs of $50,000, those with twenty to 100 employees would incur $100,000, those with 100 to 500 employees would incur $450,000, and those with more than 500 employees would incur two million dollars in costs.[118] The SRIA suggests that large businesses will have a competitive advantage because their resources allow for quick adjustments, while small businesses struggle to adapt at all (much less

111. Ivana Kottasova, *These Companies are Getting Killed by GDPR*, CNN BUSINESS (May 11, 2018, 6:39 AM), https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html [https://perma.cc/6DFK-NACY].

112. GDPR.EU, 2019 GDPR SMALL BUSINESS SURVEY (May 2019), https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf [https://perma.cc/V49X-Z8SD]. In US dollars, that range is (at current exchange rates) roughly between $1,186, $5,933, and $1,186,745.

113. Scott Augustin, *Businesses Struggling with GDPR After One Year, Says Thomson Reuters Survey*, THOMSON REUTERS (May 22, 2019), https://www.thomsonreuters.com/en/press-releases/2019/may/businesses-struggling-with-gdpr-after-one-year-says-thomson-reuters-survey.html [https://perma.cc/6XXR-7WGJ].

114. Press Release, TrustArc, Survey Reveals 88% of U.S. Companies Need Help Complying with California Consumer Privacy Act (CCPA) (Mar. 19, 2019), https://www.trustarc.com/press/survey-reveals-88-of-u-s-companies-need-help-complying-with-california-consumer-privacy-act-ccpa/ [https://perma.cc/FS39-BYMZ].

115. *Id.*

116. 2019 REGULATORY IMPACT ASSESSMENT, *supra* note 92, at 6. It is important to note that there were many businesses not located in California that would have fallen under the CCPA but were outside of the scope of SRIA and not included in this estimation. *Id.* at 21.

117. *Id.* at 10-11.

118. *Id.* at 11.

quickly).[119] Thus, small businesses are the ones facing a "disproportionately higher share of compliance costs."[120] Think about the efforts companies made to comply with the CCPA in California that will be sent back to the drawing board when the CPRA goes into effect. This setback is frustrating for companies, but it is just the beginning as this dilemma will be persistent so long as nothing is done to streamline the onslaught of new privacy regulations.

Having to comply with new data privacy standards can be onerous for businesses of all sizes, but especially for those that are smaller and have fewer resources. The smaller the business, the less likely that it will be able to keep up with the ever-changing regulations regarding data privacy. This is especially true when there are multiple differing regulations in the same area. The lesson here is that compliance with privacy standards can have a significant impact on businesses, but there is a way to minimize this impact while supporting increased privacy regulations—develop just one universal standard.

III. FUTURE DEVELOPMENT: CONSIDERATIONS FOR ONE UNIVERSAL REGULATION

The wide array of data privacy standards at the state, national, and international levels conflict with one another and result in confusion for both businesses and consumers alike. The ideal solution would be a multilateral treaty on data privacy that creates universal standards, like the GDPR. In the meantime, a federal privacy standard should be implemented in the United States to address the state of uncertainty. It is unclear whether the government is ready to develop a federal standard at all, much less one as expansive as the GDPR, so states will continue to use their power to adopt legislation of their own in the meantime. The EU saw the same patchwork legislation approach, which is why it adopted the GDPR as an all-encompassing alternative. Although the United States could face the same challenges and end up with the same result, action should be taken now to prevent harm to its businesses and consumers.

A. The Ultimate Solution is One Universal Regulation

Consumers do not want to lose trust in United States companies that process their personal data, but this trust will continue to erode as long as a state of uncertainty exists with regard to data privacy protections.[121] The United States needs nothing short of a federal equivalent of the GDPR. Although a federal standard could develop naturally over the next few decades as evidenced by the development of the GDPR in the EU, consumers and businesses in the United States need it as soon as possible. The best solution is to adopt a national standard mirroring the GDPR because many United States businesses are

119. *Id.* at 31.

120. 2019 REGULATORY IMPACT ASSESSMENT, *supra* note 92, at 31.

121. McAllister, *supra* note 98, at 203.

already required to comply with it.[122] The California SRIA indicates that most large businesses are already compliant with the GDPR, and thus would not have to reinvent the wheel to comply with new federal legislation.[123] By adopting a national standard that mirrors the GDPR, there will undoubtedly be a short term negative impact on businesses that have yet to comply with the GDPR as they try to catch up. While there are plenty of businesses that are not yet required to comply with a comprehensive data privacy regulatory scheme such as the CCPA or the GDPR, the keyword is *yet*. There is no denying that it is only a matter of time before they have no choice. Creating this standard will have long term benefits such as the United States maintaining a competitive advantage over countries that have not adopted comprehensive data privacy regulations, because the current trend among nations is to adopt such comprehensive schemes. It is not a question of whether privacy regulations are coming, the question is when. Also, the new standard would not go in effect overnight; many privacy regulations include a grace period to give businesses some time to figure out their obligations. A national data privacy standard would ease domestic trade within the United States as well as non-domestic trade because there would be only one universal set of requirements for all businesses and industries to comply with.[124] The longer it takes for the United States to take affirmative steps in this direction, the greater the likelihood of a weaker federal law because there will be even more conflicting state standards to address.[125] Furthermore, the fact that countries all over the world are developing their own robust standards, with which United States businesses might have to comply, means time is certainly of the essence, as privacy concerns linger for consumers and businesses struggle to comply with onerous demands from differing regulations.

B. Obstacles: The Effect of Partisan Politics

Just like any political issue, there has been support and pushback from both sides. Although one might not expect this to be a partisan issue, coming up with a solution may very well be.[126] There have been numerous attempts within the last decade to pass federal privacy regulations, but none have been successful.[127] Take the Consumer Privacy Bill of Rights, for example, put forth by the Obama

122. Joanna Kessler, Note, *Data Protection in the Wake of the GDPR: California's Solution for Protecting "The World's Most Valuable Resource",* 93 S. CAL. L. REV. 99, 125 (2019).

123. 2019 REGULATORY IMPACT ASSESSMENT, *supra* note 92, at 31.

124. Humerick, *supra* note 2, at 125.

125. Carsten Rhod Gregersen, *The US Is Leaving Data Privacy to the States and That's a Problem*, BRINK (Aug. 20, 2019), https://www.brinknews.com/the-us-is-leaving-data-privacy-to-the-states-and-thats-a-problem/ [https://perma.cc/Y7ZL-F76U].

126. John McKinnon, *Partisan Rift Threatens Federal Data Privacy Efforts*, WALL ST. J. (Feb. 17, 2019), https://www.wsj.com/articles/partisan-rift-threatens-federal-data-privacy-law-11550422831 [https://perma.cc/8DGY-4ZS6].

127. Humerick, *supra* note 2, at 110.

administration in 2012.[128] No progress was made because opponents argued that this would "stifle industry innovation" and proposed self-regulation as an alternative.[129] Large technology companies such as Apple and Facebook have started to push for a national standard similar to that of the GDPR to override the comprehensive state regulations, but opponents are pushing back because they don't want a federal standard that will just be a watered-down version of what the states are working so hard to create.[130] These opponents seem to prefer waiting out the long game, as we saw with the development of the EU's data privacy regulation, which allowed countries to build robust protections and work together towards a meaningful compromise. The Trump administration resisted both bipartisan attempts and EU pressure to develop a national cyber policy similar to the GDPR citing, in part, that they were viewed as foreign mandates.[131] However, there are millions of dollars being spent in lobbying for a federal standard.[132] The state of Arizona introduced a House Concurrent Resolution that said "a single federal standard for comprehensive consumer data privacy regulation is preferable to a state-by-state approach," but it died in chamber.[133] In September of 2020, both parties introduced federal data privacy legislation: the Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act ("SAFE DATA") and the Consumer Online Privacy Rights Act ("COPRA").[134] Even if these particular acts fail, their introduction alone suggests that hope is on the horizon that, if Congress is able to prioritize data privacy, federal legislation could be put in place during the Biden administration. If the United States gets on board with developing a comprehensive regulation, there could be encouragement from international bodies to collaborate on a truly universal regulation. There are problems inherent with this process at the international level as well, but there is an overwhelming sense that humans have some sort of right to privacy. What that may look like may differ across the world, but certainly there is a baseline that could be established for everyone.

128. Lily Li, *American Privacy Laws in a Global Context: Predictions for 2018*, 60 ORANGE COUNTY LAWYER 31, 32 (2018).

129. *Id.*

130. McKinnon, *supra* note 126.

131. Rustad & Koenig, *supra* note 46, at 453.

132. *Id.*

133. H.C.R. 2013, 54th Leg., Second Reg. Sess. (Az. 2020).

134. *Election 2020: Looking Forward to What a Biden Presidency May Mean for Data Privacy and Data Privacy Litigation*, NAT'L L. REV. (Nov. 12, 2020), https://www.natlawreview.com/article/election-2020-looking-forward-to-what-biden-presidency-may-mean-data-privacy-and [https://perma.cc/5ETS-SG88].

C. Consequences of Failure to Develop a Universal Regulation

If the United States does not establish a federal standard for data privacy, there will be consequences for consumers, businesses, and the global economy. As previously discussed, differing privacy standards result in extreme costs associated with compliance and there is no doubt that the increased operational costs for businesses will be passed directly on to consumers. The SRIA explained that in addition to the cost of compliance, these regulations will result in reduced productivity for businesses.[135] As mentioned previously, the technological advancement of direct marketing allows for personal data to be used for targeted advertisements which in turn leads to sales. According to the SRIA, the average revenue per user for search, banner, and video advertisements are $136.71 on desktop computers and $266 on mobile devices.[136] In California alone there are 30.9 million desktop users and 31.7 million mobile device users, suggesting the value of advertisements in California is over $12 billion annually.[137] This means that the value of personal data that would fall under all of the data privacy regulations is substantial. Without the ability to use this data, businesses will struggle to compete. In the study on the GDPR, sixty percent of businesses said that the GDPR would significantly change their business model regarding the collection, use, and protection of personal information.[138] Accordingly, seventy-one percent of businesses said that failure to comply with the GDPR would result in a detrimental impact on their ability to conduct business.[139] If a small company is forced out of business because it is unable to comply with privacy standards, consumers will be forced to take their business elsewhere (including to the larger companies that may charge more for the same product or service, simply because they can).

Despite increased costs and reduced revenue for businesses, the overall impact on the market and economy is unknown. The concern is that while the rest of the world is adopting privacy approaches like the GDPR, the United States is falling behind.[140] As discussed earlier, a multitude of countries have legislation in place regarding data privacy.[141] Until the United States institutes a federal regulation on par with the GDPR, it will suffer a disadvantage by not requiring its businesses to use data commercially in accordance with international legal standards, while other countries around the world do. That is the ultimate cost, as the disadvantage could result in the United States losing its place in the international market and could have negative repercussions for both

135. 2019 REGULATORY IMPACT ASSESSMENT, *supra* note 76, at 12.
136. *Id.* at 14.
137. *Id.* at 14-15.
138. PONEMON INSTITUTE, *supra* note 89, at 3.
139. *Id.*
140. Humerick, *supra* note 2, at 111.
141. UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, *supra* note 12.

the national and international economies. Thus, the United States should feel the pressure to make meaningful adjustments to preserve its competitive edge in the international market. Companies are starting to get serious about data privacy, which means that change is coming. If the United States does not put forth its own efforts to change, the consequences will be both unavoidable and detrimental to businesses and consumers alike.

CONCLUSION

Given the current climate of piecemeal data privacy regulations in the United States, consumers and businesses are left to navigate a confusing legal environment with rules that are difficult to comply with, much less enforce.[142] The GDPR has created a "worldwide gold standard" for data privacy.[143] If the United States wants to maintain its status as a global competitor in the international market, the best way to do that is to apply the strongest protection standards so that it does not fall behind. Until a federal standard is developed in the United States, there will continue to be an influx of comprehensive data privacy regulations at the state level. Some believe that data privacy regulations are "establishing a digital bill of rights for the individual,"[144] and others believe that this movement will be "the start of the 'roaring 20s' in the privacy realm."[145] Whichever way you look at it, recent regulations such as the EU's GDPR and California's CCPA and CPRA are leaving their mark on both the market and the economy. This means that data privacy protection in the digital era will never be the same because we are now "putting people first in the Age of the Internet."[146]

TIFFANY LIGHT*

142. Carsten Rhod Gregersen, *supra* note 108.

143. Rustad & Koenig, *supra* note 46, at 453.

144. Colin Fraser, *Phil Maynard Tealium CLO Discusses Compliance with Privacy Laws*, 60 ORANGE COUNTY LAWYER 26, 27 (May 2018).

145. Liisa Thomas, *3 Privacy Law Predictions for The New Year*, LAW360 (Jan. 1, 2020, 11:56 AM), https://www.law360.com/articles/1229279/3-privacy-law-predictions-for-the-new-year [https://perma.cc/6FWU-KUCV].

146. Press Release, Xavier Becerra, *supra* note 1.

* J.D., May 2021, Saint Louis University School of Law. I would like to thank Professors Erika Cohn and Matthew Bodie for their guidance and support throughout the drafting stage. I would also like to thank Michael McMahon and the rest of the Saint Louis University Law Journal staff that helped transform this Article.