The General Data Protection Regulation and California Consumer Privacy Act: The Economic Impact and Future of Data Privacy Regulations

Christopher Bret Alexander

Follow this and additional works at: https://lawecommons.luc.edu/lclr

Part of the Consumer Protection Law Commons

Recommended Citation
Christopher B. Alexander The General Data Protection Regulation and California Consumer Privacy Act: The Economic Impact and Future of Data Privacy Regulations, 32 Loy. Consumer L. Rev. 199 (). Available at: https://lawecommons.luc.edu/lclr/vol32/iss2/2

This Feature Article is brought to you for free and open access by LAW eCommons. It has been accepted for inclusion in Loyola Consumer Law Review by an authorized editor of LAW eCommons. For more information, please contact law-library@luc.edu.
THE GENERAL DATA PROTECTION REGULATION AND CALIFORNIA CONSUMER PRIVACY ACT:
THE ECONOMIC IMPACT AND FUTURE OF DATA PRIVACY REGULATIONS

Christopher Bret Alexander*

I. INTRODUCTION

The right to privacy in the United States, at least as compared to the European Union, has not adequately developed to meet the needs of consumers in the age of technology.\(^1\) Informational privacy, that is, protection not only from governments but also from businesses, is an important issue in the 21st century.\(^2\) The European Union recently

*Christopher Bret Alexander, M.B.A., J.D. Candidate, May 2020, Villanova Charles Widger School of Law. I would like to thank my Villanova Law Professor Doris DelTosto Brogan for her insightful, thought provoking and interactive lectures in my Data Privacy and Legal Ethics courses. I was very fortunate for the opportunity to learn, ask questions, and seek mentorship from such a profound legal scholar during my educational experience at Villanova University. Further, I dedicate this comment to my undergraduate and graduate Jesuit education at Saint Joseph's University. The Jesuit teachings fostered my personal development skills and inspired my professional leadership qualities. As such, I aspire to be a future agent of change and to be more like Saint Ignatius of Loyola, who went forth and “set the world on fire.”


\(^2\) See What does privacy mean?, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, https://iapp.org/about/what-is-privacy/ (last visited Feb. 20, 2020) (“Information privacy is the right to have some control over how your personal information is collected and used”).
implemented the General Data Protection Regulation ("GDPR")³ and, shortly thereafter, the state of California followed their lead on data privacy regulations with the passage of the California Consumer Privacy Act ("CCPA").⁴ Both of these data privacy laws strive to solidify the rights of consumers, but at a cost.⁵ The implication of new regulations on an unregulated and booming industry, like Big Data, will undoubtedly have serious ramifications on the economy.⁶ Businesses will need to spend a great deal of finite resources - time, effort, and money - in order to effectively and efficiently comply with the similar, but different laws.⁷ In the United States, states are debating their own data privacy regulations, similar to that of California's, which will undoubtedly make compliance even more complex and costly.⁸ In response to growing concerns of overregulation, Big Data


⁶ See generally Data Protection: What is the problem?, PRIVACY INTERNATIONAL, https://privacyinternational.org/learn/data-protection (last visited Feb. 20, 2020) ("As a result, innovations in policy and technology, private and public sector data practices, are largely left unregulated and unchecked, and this will have significant implications for rights of individuals, as well as for the development of the economies and societies.")


⁸ See Lauren Feiner, California's new privacy law could cost companies a total of $55 billion to get in compliance, CNBC (Oct. 5, 2019), https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-
companies are lobbying the federal government to intervene and preempt future state regulations. The growing possibility of federal legislation will likely lower compliance costs and maximize growth rates for businesses; however, lawmakers must appropriately balance the interests of businesses with the needs of consumers to ensure privacy rights are upheld.

II. BACKGROUND

Privacy is a complex theoretical concept to discuss and an even more complex concept to regulate in practice. The right to privacy has evolved to include informational privacy, which is one of the most pressing issues of the 21st century. The United Nations ("U.N."), United States ("U.S."), and European Union ("E.U.") are attempting to ensure regulations adequately address technological advances to protect the rights of consumers. First, the United Nations ratified the
Universal Declaration of Human Rights and recognized the right to privacy on the international level more than sixty years ago.14 Second, the United States does not have an explicitly defined right to privacy in the U.S. Constitution but informational privacy has been derived from many legal sources including Whalen v. Roe, a potential basis for future federal regulation as the state of California uses its economic and political power to implement the CCPA.15 Third, the European Union ratified the European Convention of Human Rights and recognized the right to privacy within its member states.16 The varying approaches to the right to privacy has generated different, but similar regulatory statutes out of California – the California Consumer Privacy Act – and out of the European Union – the General Data Protection Regulation.17 Both of these statutes, despite any differences, maintain an underlying goal of lawmakers and regulators to ultimately balance the rights of consumer with the interests of businesses.18

A. The Right to Privacy

The right to privacy is an individuals’ freedom to choose physical seclusion, autonomous decision making, and informational protection from other people, large corporations, and the government.19 Privacy is an inherently difficult concept to define, let alone regulate.20 Historically, privacy was limited to abstract ideas and

14 See infra notes 26-38 (reviewing U.N. efforts to pass data protections and regulations).
15 See infra notes 39-82 (reviewing U.S. efforts to pass data protections and regulations).
16 See infra notes 83-95 (reviewing E.U. efforts to pass data protections and regulations).
19 See Daniel J. Solove, Conceptualizing Privacy, 90 Cal. L. Rev. 1087 (2002). (discussing privacy as an evolving concept that is theoretically difficult to regulate).
20 See id. (emphasizing difficulties involving regulation of new concepts like data).
theoretical frameworks about "family, body, and home."\textsuperscript{21} Over time, as described by Daniel J. Solove, the concept of privacy has been extended beyond traditional social norms to be "shaped by culture and history."\textsuperscript{22} As the nature and role of privacy in society today continues to develop and progress, privacy law and the protections it affords must be examined in "specific contextual situations."\textsuperscript{23} Therefore, as technology advances and its potential uses or abuses continue to progress, the value of privacy cannot be underestimated.\textsuperscript{24} Fortunately, privacy law regulations in the European Union and United States are attempting to address the challenges of technological advances coupled with the concerns of informational privacy within their own respective legal frameworks.\textsuperscript{25}

1. The Right to Privacy and the United Nations

The United Nations, founded in 1945 as an international governing body, set forth a comprehensive "standard of achievements for all peoples and all nations," known as the Universal Declaration of Human Rights ("UDHR").\textsuperscript{26} The UDHR was not a legally-binding treaty, rather the UDHR was adopted simply to define "human rights and fundamental freedoms" as a founding document for the United Nations and a guiding document for the international community.\textsuperscript{27} Proclaimed in December 1948, the ratification encompassed a wide variety of rights from life and liberty to unions and voting.\textsuperscript{28} Article
12 of the UDHR pertained to privacy, stating "No one shall be subjected to arbitrary interference with [his or her] privacy, family, home or correspondence, nor to attacks upon [his or her] honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Article 12 was intended to be a broad interpretation of traditional privacy, including defamation protections, with the encouragement of government regulations to protect these privacy rights. Ultimately, the United Nations recognized the importance of privacy law and intended to provide a legal basis for government regulations intended to protect citizens against future privacy concerns.

Typically the United States does not ratify treaties with the United Nations that are legally "binding instruments under international law" because lawmakers would prefer to avoid any or all potential conflicts with domestic law, jurisdictional enforcement issues, and sovereignty worries that may arise. To illustrate the implications international law, a drug cartel leader named, Humberto Alvarez-Machain, allegedly murdered a United States Drug Enforcement Administration agent in 1985. At the time, the United States forcibly abducted Humberto after Mexico refused to assist the United States with extradition. Humberto was eventually found not guilty of the criminal charges and subsequently brought a civil lawsuit alleging his extradition, or lack thereof, was a violation of international law established in the UDHR. In 2004, the Supreme Court granted a writ of certiorari for Sosa v. Alvarez Machain and determined the UDHR was not applicable in this case. The Court's holding reinforced and solidified the United States perspective that the UDHR is not legally binding and "does not of its own force impose obligations

29 See id. at art. 12 (quoting importance of right to privacy).
30 See id. (describing application of traditional and future implications).
31 See UDHR supra notes 26-30 and accompanying text.
34 See id. (discussing issue and facts of case).
35 See id. at 700 (deriving power from Federal Tort Claim Act and Alien Tort Claim).
36 See id. (describing procedural history and application of law in court).
as a matter of international law." 37 The ruling spared U.S. lawmakers from additional sovereignty worries, but validated the need to rectify international disparities of law to uphold and protect, not impede, privacy rights in the United States. 38

2. The Right to Privacy and the United States

The right to privacy is not explicitly stated in the United States Constitution. 39 In the past, the Supreme Court has implicitly derived the right to privacy from the First, Third, and Fifth Amendment. 40 The First Amendment provides privacy of beliefs, as illustrated in Stanley v. Georgia when the Supreme Court held "[o]ur whole constitutional heritage rebels at the thought of giving government the power to control [people's] minds." 41 The Third Amendment provides privacy of the home, as illustrated in Griswold v. Connecticut when the Supreme Court held "[t]he Third Amendment, in its prohibition against the quartering of soldiers 'in any house' in time of peace without the consent of the owner, is another facet of that privacy." 42 The Fifth Amendment provides privileges against self-incrimination, as illustrated in Miranda v. Arizona when the Supreme Court held "[a]n individual's] right to remain silent unless he chooses to speak in the unfettered exercise of [his or her] own will." 43 Additional amendments like the Ninth Amendment, described as an "eloquent truism" about implied constitutional rights, and the Fourteenth Amendment, stating the "notions of liberty" in the Due Process Clause, also provide a basis for the "zone of privacy." 44 The Founding Fathers of America had tremendous foresight when compiling the U.S. Constitution, however, the "original intent" of the founders may be outweighed by the need

37 See id. at 735 (distinguishing that some countries do uphold UDHR as domestic law).
38 See id. (reinforcing need for additional uniform international regulations).
39 See generally U.S. CONST.
40 See infra notes 41-43 and accompanying text.
42 See U.S. CONST. amend. III; Griswold v. United States, 59 F.3d 1571 (11th Cir. 1995) (referencing Engblom v. Carey, 677 F.2d 957 (2d Cir. 1982)).
for a "living document" to further derive and justify constitutional rights.  

More specifically, the right to privacy is alluded to in the Fourth Amendment which states "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The Fourth Amendment provides fundamental assurances in establishing a "reasonable expectation of privacy" from the government, as illustrated in Katz v. United States. In Katz, the Court held searches and seizures for "people, not places" must be reasonable in nature. For the most part, current case law pertaining to privacy law focuses on protecting the rights of physical seclusion and autonomous decision making from government interference, rather than informational privacy. Going forward, lawmakers should extend the Fourth Amendment to protect and regulate the personal information of individuals not only from government but also businesses.

In addition to the Constitution of the United States, each of the fifty states also have their own individual constitutions. Constitutions in ten states, including the state of California, contain "explicit provisions concerning the right to privacy." The ten states

---

46 See U.S. CONST. amend. IV.
48 See id. at 351 (describing procedural history and application of law in court).
49 See supra note 41-48 (referencing majority of current case law) and infra note 57 (referencing decision in Whalen v. Roe that helped establish information privacy).
are anomalies, representing one fifth of the states, in the United States that arguably value an individuals’ right to privacy more than the others.\textsuperscript{53} The majority of state privacy protections mirror that of the Fourth Amendment in the United States Constitution, whereas a minority of states expand upon the scope of privacy protections with specific references to privacy.\textsuperscript{54} In particular, under Article I Section 1 of the California Constitution states “All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.”\textsuperscript{55} The passage of the CCPA, continuous data breaches, and changing popular opinion about data privacy will likely result in additional states amending constitutions and passing regulatory statutes to protect individuals’ privacy rights and interests.\textsuperscript{56}

3. Informational Privacy in \textit{Whalen v. Roe}

The basis for the right to informational privacy was suggested, but not specifically held to be constitutionally protected in \textit{Whalen v. Roe}.\textsuperscript{57} That case involved a 1972 New York Statute entitled the Controlled Substances Act (“CSA”)\textsuperscript{58} that required doctors to document and track designated “potentially harmful” prescription drugs, known as Schedule II drugs.\textsuperscript{59} At the time, the state of New
York was attempting to find alternative ways to remedy the drug abuse epidemic adversely affecting its population. Accordingly, the Act required doctors to fill out three copies of an official form with information including: the name of the prescribing doctor; the name of the dispensing pharmacy; the name and dosage of the prescription drug; and the name, address, and age of the patient. The doctor was required to file one of the three form copies with the New York Department of Health, which would store the information for a period of five years and guaranteed the information would be protected from public disclosure.

Litigation ensued, alleging the Act was an unconstitutional breach of an individuals' "zone of privacy" and violated on the "reasonable expectation of privacy" among doctor-patient relationships. The Supreme Court identified two different privacy interests — "the individual interest in avoiding disclosure of personal matters [and] the interest in independence in making certain kinds of important decisions." That being said, the Court held that "the New York program does not, on its face, pose a sufficiently grievous threat to either interest" as identified by Justice Stevens. Consequently, the Court determined the New York Controlled Substance Act was within the states' policing powers to address the drug epidemic and did not violate any rights or liberties constitutionally derived from the Fourth or Fourteenth Amendment.

The majority opinion recognized the "threat to privacy implicit in the accumulation of vast amounts of personal information," but the Court did not address the possibility of intentional or unintentional disclosure of data. The Court was primarily concerned with privacy interests of individuals if information was abused or improperly

---

63 See id. at 598 (referencing U.S. CONST. amend. XIV and IV).
64 See id. at 599-600 (identifying two different privacy interests).
65 See id. at 600 (deciding New York CSA was not unconstitutional).
67 See 429 U.S. 589 at 605 (disregarding differences in data collection types).
disclosed by the government, not private entities. Interestingly, Justice Brennan's concurrence was skeptical about the use of a central computer for storing data and worried about the potential for increasing the risk of data breaches. Moreover, Justice Stewart’s concurrence referenced *Katz* when the Court held “the Constitution affords protection against certain kinds of government intrusions into personal and private matters, [but] there is no ‘general constitutional right to privacy.'” In retrospect, *Whalen v. Roe* laid the foundation for a right to informational privacy in the form of statutory regulations for individuals not only from government, but also private entities.

4. The State of California as a Major Trendsetter

California is the largest economy in the United States and the fifth largest economy in the world. The $2.7 trillion economy is driven by its nearly 40 million residents who contribute to the states’ Gross Domestic Product (“GDP”) when they consume or use the goods and services from businesses, such as Big Data companies headquartered in Silicon Valley. The state of California has the largest population in the United States, as a result, the state has the opportunity to vote for 53 out of the total of 435 United States Representatives. Therefore, due to the large size of its population

---

68 See id. (focusing on government not business concerns).
69 See id. (noting difference between entities affected).
70 See *Whalen*, 429 U.S. 589 at 608. (referencing concurring decision).
75 See generally California Members of Congress, GOVTRACK, https://www.govtrack.us/congress/members/CA#representatives (last visited Feb. 20, 2020) (illustrating 12% Representatives in the U.S. Representative are from California).
and vast scale of the economy, California has the ability to significantly influence wide spread policy creation or alterations of other states privacy standards and generate much needed discussions about future data privacy legislation on the federal level.\textsuperscript{76}

In 1963 California became the first state to adopt the recovery theory of strict product liability, \textit{"a legal rule that says a seller, distributor or manufacture of a defective product is liable to a person injured by that product regardless of whether the defendant did everything possible to make sure the defect never happened."}\textsuperscript{77} In \textit{Greenman v. Yuba Power Products, Inc.}, the California Court ruled in favor of the injured plaintiff, or consumer, instead of the defendant, or business, on the basis of strict product liability.\textsuperscript{78} Following the ruling, the California state legislature and its respective administrative agencies enacted some of the strictest car and product safety regulations.\textsuperscript{79} The majority of states followed California’s lead and now recognize strict liability for defective products following the \textit{Greenman} decision.\textsuperscript{80} California has been and will continue to be a leader in the nation for consumer protection standards starting with strict liability.\textsuperscript{81} Thus, the California Consumer Privacy Act is expected to affect not only other states seeking to model their own data privacy regulations similar to that of California’s, but also impact


\textsuperscript{78}See \textit{Greenman v. Yuba Power Prods., Inc.}, 377 P.2d 897 (1963) (involving a lawsuit over a chain saw malfunction injury that resulted in California adopting strict liability).

\textsuperscript{79}See Snavely \textit{supra} note 76 (reaffirming continued efforts to heavily regulate); see also \textit{About Us}, CONSUMER FEDERATION OF CALIFORNIA, https://consumercal.org/about-cfc/about-us/ (last visited on Feb. 20, 2020) (discussing consumer rights in California).


\textsuperscript{81}See Snavely \textit{supra} note 76 (addressing California’s ability to lead on issues).
nearly every business that engages in interstate commerce with California.82

5. Right to Privacy and the European Union

The European Union and its citizens, unlike the United States and its citizens, reap the protection and benefits of an explicit right to privacy.83 In 1991, after years of coalition, the European Union was formally established with the Maastricht Treaty as an international confederation of member states similar to United States.84 Today, the European Union is a political and economic governing body that consists of twenty-seven member states with a unified Parliament, Central Bank, and other shared government entities.85 The source of European Union law is derived from treaties, each of which, all of the member states agree to implement and follow as a condition for membership.86 The treaties establish a basis for governance, which allows the European Union Parliament to pass regulations that must be ratified or uniformly altered by each of the member states’ own respective Parliaments.87 In recent years, the European Union has come under scrutiny for overregulation; however, European Union leaders argue the short term economic costs will lead to long term economic opportunities for businesses and emphasize the importance of managing unique personal identities and the safe use of new technologies.88

82 See Tim Day Harold Kim, U.S. Chamber Privacy Comments on California Consumer Privacy Act Rulemaking, U.S. CHAMBER OF COMMERCE (Mar. 8, 2019), (emphasizing effect on interstate commerce and economic prosperity that requires federal privacy law).
83 See infra note 90 (citing ECHR) and infra note 92 (citing FREU).
86 See id. (discussing source of binding law for all member states).
87 See id. (discussing European Parliamentary systems).
88 See Nic Fildes, Europe’s telecoms groups warn over regulation, FINANCIAL TIMES (Sept. 25, 2017), https://www.ft.com/content/6e55ad82-a1f4-11e7-b797-b61809486fe2 (indicating you can’t put a price on protecting rights).
89 See Nic Fildes, Europe’s telecoms groups warn over regulation, FINANCIAL TIMES (Sept. 25, 2017), https://www.ft.com/content/6e55ad82-a1f4-11e7-b797-b61809486fe2 (indicating you can’t put a price on protecting rights).
The European Union identifies two specific treaties used to derive privacy protections – the European Convention of Human Rights, as well as, the Lisbon Treaty and the Charter of Fundamental Rights of the European Union. In 1953, following the guidance of the United Nations and the ratification of the UDHR, the European Union implemented its own European Convention of Human Rights (“ECHR”). Under Article 8 of the ECHR, “everyone has the right to respect for [their] private and family life, his home and his correspondence,” subject to certain restrictions. More recently, the ratification of the Lisbon Treaty and Charter of Fundamental Rights of the European Union (“FREU”) in 2000 explicitly included not only the right to privacy, but the right to informational privacy concerning “the protection of personal data.” The explicit right to informational privacy as a fundamental right was arguably ahead of its time, even to this day, with substantial implications on the global economy and international legal community. The FREU undoubtedly fostered the development and passage of privacy regulations in the European Union, today in form of the GDPR. The European Union, much like the state of California, recognizes the right to privacy and legislates accordingly because it “prides itself on the extensive privacy protections it affords its citizens.”

89 See infra notes 90-95 and accompanying text.  
90 See generally EUROPEAN CONVENTION FOR THE PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS (1950) at art. 10 [hereinafter referred to as ECHR].  
91 See id. at art. 8(b) (stating “There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”).  
92 See generally CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION (2000) at art. 8 (“everyone has the right to the protection of personal data concerning him or her”) [hereinafter referred to as FREU].  
94 See id. (describing development of privacy rights in Europe).  
95 See Beata A. Safari, Intangible Privacy Rights: How Europe’s GDPR Will Set a New Global Standard for Personal Data Protection, 47 SETON HALL L. REV. 809
III. ANALYSIS

The analysis will consist of a brief, but comprehensive review of the General Data Protection Regulation and the California Consumer Privacy Act, their respective privacy protections and policy ramifications. The analysis will also review the implications of the GDPR on Brexit and the CCPA on federal preemption before analyzing the economic implications of regulations on the economy – for better or worse.

A. General Data Protection Regulation ("GDPR")

The GDPR is a legally binding law on the European Union and its economic counterparts. The GDPR repeals and replaces the guiding principles of Data Protective Directive with regulations to achieve and uphold the right to privacy in the European Union. The European Union Parliament intended to create a comprehensive approach to modern day privacy issues with a list of rights, procedures, remedies, and violation fines. The GDPR has led to significant changes with the intersection of law and business, including the right to breach notifications, right to access, right to be forgotten, right to data portability, and data protection officers. Today, the European Union is willing to work with the United Kingdom during its transitional "Brexit" phase to mitigate the potential cost of compliance for businesses and consumers.

1. GDPR Background – Data Protective Directive and Safe Harbor Agreement

The GDPR repeals the Data Protective Directive 95/46/EC ("DPD") passed on October 24, 1995 when technology and its capabilities were still in the early stages of development. The DPD applied to entities located within the European Union and merely recommended guidance standards for companies to uphold rights (2017) ("difference between valuing liberty, for Americans, and dignity, for Europeans").

96 See generally GDPR, supra note 3 and accompanying text.
97 See infra notes 91-105 and accompanying text.
98 See infra notes 111-115 and accompanying text.
99 See infra notes 116-131 and accompanying text.
100 See infra notes 145-151 and accompanying text.
pertaining to an individual's personal information, as well as, the free circulation of data. Following the passage of DPD, the United States worked with the European Union to create the U.S.-E.U. Safe Harbor Agreement of 2000. The United States Department of Commerce worked with the European Union to ensure the seven principles of the framework were being adequately upheld by voluntarily participating companies, or companies could develop their own self-regulatory programs in accordance with the framework. Today, the framework is no longer a suggestion for companies doing business in the European Union or with its citizens, but legally enforceable principles incorporated into the GDPR.

In 2015, the U.S.-E.U. Safe Harbor Agreement of 2000 was overturned by the European Court of Justice "in the wake of the revelation of U.S. government surveillance programs following public of classified material by former N.S.A. contractor Edward Snowden." For over a year, there was uncertainty about the future of data protection until the United States and the European Union revised and replaced the Safe Harbor with the Privacy Shield of 2016. The Privacy Shield which was designed to ensure the E.U. sufficient data security while maintaining open transport for data and

---

102 See id. (illustrating a continuous need for balance).

103 See Safari, supra note 95 (noting timeline).

104 See id. (describing how United States and European Union officials work together to protect rights of citizens via non-legally binding international law recommendations).

105 See generally GDPR, the End of Safe Harbor, and What it Could all Mean for Businesses, NEFIBER, https://www.nefiber.com/blog/gdpr-changes-safe-harbor-mean-businesses/ (last visited Feb. 20, 2020) (listing seven principle: "(1) Notice: The purpose behind data collection and usage must be fully disclosed; (2) Choice: Opt-out opportunities must be provided to all individuals, and sensitive information must require an opt-in; (3) Onward Transfer: All future data transfers must follow Safe Harbor Privacy Principles or another comparable directive; (4) Security: Information must be adequately protected; (5) Data Integrity: All personal data gathered must be relevant, and the data's reliability should be verified; (6) Access: If an individual's personal information has been gathered, they must have the right to access and modify or remove inaccurate information; (7) Enforcement: The compliance of these rules by each organization must be feasible - with sanctions readily available to be handed out to those who do not follow through on their data privacy commitments").


107 See id. (noting uncertainty in regulatory compliance).
commerce for the United States. Similar to the Safe Harbor, the Privacy Shield focused on three main issues: handling Europeans personal data, U.S. government access to data, and protection of citizens’ rights in the European Union. The Privacy Shield complied with the DPD, not the GDPR and would no longer be relevant for international data regulations.

During this time period, the European Commission set out to "harmonize data privacy laws across Europe, protect and empower all E.U. citizens’ data privacy, and reshape the way organizations across the region approach data privacy" starting in 2012. After years of planning, the European Union Parliament voted and passed the GDPR in 2016. After two years of preparation for regulators and companies the GDPR was implemented on May 25, 2018 to ensure its data privacy regulations were “fit for the digital age.” At this time, the United States does not have plans to redo the Privacy Shield agreement with the European Union because the GDPR is legally binding authority, unlike the DPD recommendations that lacked

---

108 See Safari, supra note 95 (discussing the new and improved purpose of the Privacy Shield after the Safe Harbor); see also Martin Weis and Kristin Archick, US-EU Data Privacy: From Safe Harbor to Privacy Shield, CONGRESSIONAL RES. SERV. (May 19, 2016) (explaining Safe Harbor was null and void after the E.U. took issues with security surveillance concerns from U.S., agreement was redrafted and renamed Privacy Shield).

109 See Alvarez, supra note 106 (discussing safe harbor and subsequent privacy shield).

110 See Safari, supra note 95 (explaining distinctions between directions and regulation: "Directives are broad, goal driven pieces of legislation which provide guidelines for Member States implementation, but depend on the independent passage of a law in every Member States within a designated period of time. Regulation are narrow, specific pieces of legislation which become immediately enforceable - and binding - in every Member State without implementing a law in each State").

111 See generally GDPR, supra note 3 and accompanying text.


113 See id. (noting commentary).
jurisdictional authority. If companies do not comply with the GDPR there are hefty fines to pay.

2. GDPR Privacy Protections

The GDPR regulates a wide array of entities in order to protect individuals’ right to privacy. The GDPR regulates data controllers and data processors that process personal data within the European Union or process European Union data subjects’ personal data outside the European Union with the offering of goods and services. The GDPR has a far greater jurisdictional reach than the CCPA, essentially affecting all companies regardless of location who provide products or services to citizens of the European Union. The GDPR protects data subjects, who are identifiable persons to which personal data can relate. The GDPR provides equally broad protections as the CCPA with a less specific definition relating to data subjects.

The GDPR defines personal information, its potential uses, and its opt-in versus opt-out policy in a comprehensive way. The personal information covered under the GDPR is defined as any information relating to an identified or identifiable data subject. The GDPR exempts government records and does not include a household

---


117 See GDPR, supra note 3 at art. 24-43 (regulating controller and processor).

118 See GDPR, supra note 3 at art. 3 (describing territorial scope); contra CCPA supra note 4 at 1798.140 (defining businesses required to comply with consumer protections).

119 See GDPR, supra note 3 at art. 4(1) (defining personal data).

120 See id. (providing brief definition of data subject); contra CCPA, supra note 4 at 1798.140 (defining personal information and providing brief definition of consumer).

121 See id. (allowing for broad interpretation).

122 See id. (defining personal data).
or device specific caveat to personal information. Under the law, companies are allowed to use personal information that is pseudonymous or de-identified but are not allowed to use personal information that has been aggregated. The GDPR requires businesses to provide customers with detailed information about the data collected and its purposes. The GDPR does not provide a specific right to opt-out of the sale of personal information to third parties, rather it provides specific rights to opt-out of data collection of marketing purposes. The CCPA has a different policy on opt-in versus opt-out.

The GDPR provides that a business cannot discriminate against a data subject for exercising its rights, and there are no financial incentives for opt-in consent to using personal information like the CCPA. Any company found in violation of the privacy rights set forth in the GDPR does not have a time period to remedy the violation like under the CCPA. However, consumers may bring lawsuits seeking unspecified damages per data subject, per incident and the government €20 million euros or 4% of annual global revenue. Three of the most important rights under the GDPR, similar to that of the CCPA, are the right of disclosure of access, the right of data portability, and the right to deletion or erasure.

3. The Data Protection Officer: A Means to an End

Under Article 37 of the GDPR, a company must designate a Data Protection Officer ("DPO") responsible for the company’s strategic data protection initiatives and implementation of compliance requirements. Entities subject to the GDPR regulations, as

123 See GDPR, supra note 3 at art. 86-91 (describing provisions relating to specific processing situations, including exception for aggregated statistical data).
124 See id. (permitting aggregation of data for businesses); contra GDPR, supra note 3 at art. 11 (describing processing which does not require identification).
125 See GDPR, supra note 3 at art. 12-23 (regulating rights of data subject).
126 See GDPR, supra note 3 at art. 21 (describing right to object).
127 See id., see also CCPA, supra note 4 at 1798.120 (defining right to opt-out).
128 See GDPR, supra note 3 at art. 12-23 (prohibiting discrimination if exercise any or all rights); contra CCPA, supra note 4 at 1798.125(b) (allowing financial incentives).
129 See GDPR, supra note 3 at art. 77-84 (describing remedies, liability, and penalties).
130 See id. (elaborating on specific processes and remedies).
131 See infra notes 216-231 and accompanying text.
132 See GDPR, supra note 3 at art. 37 (describing designation of data protection officer).
described above, are required to hire a DPO if they are: (1) public authorities, (2) organizations that engage in large systemic monitoring, or (3) organizations that engage in large scale processing of sensitive personal data. The GDPR does not recommend any hiring credentials other than "expert knowledge of data protection law and practices." The new position has left many companies scrambling to find qualified individuals with little to no guidance on the job description and credentials. Article 39 of the GDPR attempted to clarify the role of a DPO by providing a non-exhaustive list of five important tasks or responsibilities, including but not limited to: (1) advise the company and its employees on pertinent data protection provisions, (2) monitor compliance with the law, (3) facilitate data protection impact assessments when required, (4) cooperate with regulators, and (5) serve as a main contact for the European Union supervisory authority. Articles 37 and 39 of the GDPR require the designation of a DPO, the first of many compliance costs, just to begin implementing and enforcing private protections within the covered entities.

As a result of the GDPR, the International Association of Privacy Professionals ("IAPP") estimates the DPO requirement of the GDPR alone will require companies to hire more than 28,000 DPO’s in the European Union and as many as 75,000 DPO’s around the world. The demand for compliance positions is expected to be extremely high in Big Data and five data-rich industries - technology, digital marketing, finance, healthcare, and retail. The new DPO position will be similar to that of a Chief Information Officer

133 See id. (detailing requirements for compliance not requirements for hire).
134 See GDPR, supra note 3 at art. 39. (describing tasks of data protection officer).
136 See GDPR, supra note 3 at art. 39. (detailing potential list of tasks).
137 See supra note 132-136 and accompanying text.
138 See Rodriguez, supra note 135 (noting companies are struggling to find supply to meet demand in order to comply with GDPR, may need to share or outsource).
139 See Rodriguez, supra note 135 (identifying data driven businesses).
Technically, the GDPR only requires an additional executive or manager position in the form of a DPO, but large companies will likely need to create or dedicate entire departments in order to comply with the duties and obligation imposed by the regulations. On the other hand, the CCPA does not require the appointment of a DPO, but in order to comply large companies, will likely need to allocate resources accordingly as well. Right now the median DPO salary in the United States is nearly $150,000; therefore, in order to meet demand companies affected by the GDPR are offering starting salaries of €71,584 in the European Union for GDPR-related compliance jobs. Overall, the expenses associated with added compliance salaries, new operational processes, and more technology infrastructure will increase the costs of doing business for affected companies as a “means to an end” for GDPR compliance.

4. The Implications of Brexit on Compliance

On June 24, 2016, the United Kingdom (“U.K.”) voted to leave the European Union in a referendum called “Brexit.” At the time,
GDPR compliance was the least of the Britain’s worries, but now as Britain plans to leave the European Union, the European Union Withdrawal Bill of 2018 will make the GDPR “Brexit proof.” The British government is committed to maintaining consistency in as many laws as possible for businesses during this transitional period, especially if Britain continues to do business as usual with the European mainland. The U.K. government is aware of the administrative burden regulations impose on businesses and would like to minimize the impact. In order to minimize the impact, Britain has passed its own Data Protection Act (“DPA”) to modernize data protections via its own domestic law. The DPA will comply with the GDPR and extend the regulatory framework to include additional data processing regulations. Going forward, the U.K. will be


148 See Analysis of the potential economic impact of GDPR – October 2017. LONDON ECONOMICS (Oct. 30, 2017), https://londoneconomics.co.uk/blog/publication/analysis-potential-economic-impact-gdpr-october-2017/ (analyzing potential economic impact and forecasting “profits to data analytics could decrease by up to £41 mil in the U.K., while profits attributable to prospecting for customers could decrease by up to £114 mil”).


150 See generally Data Protection Act 2018: What is it and what does it mean for insurance?, DWF (May 30, 2018), http://insurance.dwf.co.uk/news-updates/2018/05/data-protection-act-2018-what-is-it-and-what-does-it-mean-for-insurance/ (explaining DPA will comply with GDPR, but exempts certain inherently data oriented entities or function, i.e. “Unless explicitly stated or a substantial public interest and be satisfied for fraud prevention, insurance, criminal records, legal proceedings, automated decision making and profiling, and compensation...
responsible for its own legislation and companies will need to comply with both the GDPR and DPA if any legal discrepancies exist.\footnote{See \textit{generally} ePrivacy Directive, \textit{EUROPEAN DATA PROTECTION SUPERVISOR} https://edps.europa.eu/data-protection/our-work/subjects/eprivacy-directive\_en (last updated Feb. 20, 2020) (noting Privacy and Electronic Communications Directive 2002/58/EC, also known as ePrivacy Directive, involving privacy rights and electronic communication may soon be E.U. law like GDPR and involve additional compliance).}

\section*{B. Congressional Input on the GDPR}

On May 24, 2018, a day before the GDPR of the European Union took effect, four U.S. senators - Senator Edward Markey (D-MA), Bernard Sanders (I-VT), Richard Durbin (D-IL), and Richard Blumenthal (D-CT) – introduced a resolution, not a bill, encouraging entities covered by the GDPR in the E.U. to provide the same privacy protections to the citizens of the United States.\footnote{See \textit{generally} Resolution: Encouraging companies to apply privacy protection included in the GDPR of the European Union to citizens of the United States, 115\textsuperscript{TH} CONG. 2\textsuperscript{ND} SESSION, https://www.markey.senate.gov/imo/media/doc/GDPR\%20Resolution\%20.pdf} Even though the GDPR is not the law of the United States, the U.S. Senators recommended entities consider two important implications: 

\begin{quote}
(1) data processors have a legal basis for processing the data of users; and
(2) opt-in freely given, specific, informed, and unambiguous consent from users is a primary legal basis.
\end{quote}

The encouragement to provide the same legal protections \textit{"consistent with existing laws and rights in the United States, including the First Amendment"} has fallen on deaf ears because businesses are not incentivized to spend money complying with a law not required.\footnote{See \textit{id.} (ensuring legal compliance).} The resolution was merely political banter at the time; however, following the passage of the CCPA serious discussions in Washington, D.C. are taking place for a federal data privacy law to preempt the states and coexist with the GDPR.\footnote{See Elizabeth Schulze, \textit{The US wants to copy Europe’s strict data privacy law – but only some of it}, CNBC (May 23, 2019), https://www.cnbc.com/2019/05/23/gdpr-one-year-on-ceos-politicians-push-for-us-federal-privacy-law.html; see also Peter M. Lefkowitz, \textit{Why America needs a Thoughtful Federal Privacy Law}, N.Y.T. (June 25, 2019), https://www.nytimes.com/2019/06/25/opinion/congress-privacy-law.html}
The CCPA was a grassroots initiative created to demand the state of California protect the privacy rights of California residents from intrusive business practices not otherwise explicitly prohibited under the law.\textsuperscript{156} The CCPA was the first comprehensive data privacy regulation in the United States intended to provide consumers with a data privacy framework involving transparency, control, and accountability.\textsuperscript{157} The CCPA has led to significant changes with the intersection of law and business; including the right to breach notifications, right to access, right to be forgotten, right to opt out from having your information sold, and right to receive equal service if you opt out.\textsuperscript{158} Today, since enacting the CCPA, California has inspired other states to pass similar regulations and compelled the federal government to discuss preempting the law.\textsuperscript{159}

1. CCPA Background – Shine the Light Law and Initiative Referendum

The CCPA is not the first law in California to address privacy concerns, rather the Shine the Light Law passed in 2003 was intended to provide individuals the ability "to opt of out of information sharing or make a detailed disclosure of how personal information was shared for direct marketing purposes."\textsuperscript{160} Dissatisfied with the reach of the law, a privacy activist group named Californians for Consumer Privacy advocated for stricter and broader regulations.\textsuperscript{161} With the help of Alastair MacTaggert, a wealthy real estate developer, Risk Arney, a corporate finance executive, and Mary Ross, a former CIA and House Intelligence Committee informant, the privacy activist group was able to compile and write the CCPA.\textsuperscript{162} The CCPA was set for a statewide

\textsuperscript{156}See generally CCPA, supra note 4 and accompanying text.
\textsuperscript{157}See infra notes 160-173 and accompanying text.
\textsuperscript{158}See infra notes 174-190 and accompanying text.
\textsuperscript{159}See infra note 221-231 and accompanying text.
\textsuperscript{160}See generally California S.B. 27 (2005), available at https://www.epic.org/privacy/profiling/sb27.html (last visited Feb. 20, 2020) (noting limited scope; marketing focus; required disclosure of information-sharing practices; exempted small businesses with less than 20 employees and federal institutions).
\textsuperscript{161}See supra note 150 (discussing global privacy activism affecting laws).
\textsuperscript{162}See Ben Adler, California Passes Strict Internet Privacy Law with Implications for the Country, NPR (June 29, 2018), https://jezebel.com/how-a-woman-disappears-from-the-history-books-1828393645 (hypothesizing potential ramification of one state on others).
referendum, a legislative initiative directly proposed to Californian voters, on the November 2018 election ballot.\textsuperscript{163} According to legislators, technology companies, and lobbyists the original initiative was well intentioned, but deeply flawed.\textsuperscript{164} To avoid any political ramifications of the bill, politicians agreed to a compromise and passed a modified version of the initiative on June 28, 2018 in exchange for the withdrawal of the Californians for Consumer Privacy referendum barring any major amendments.\textsuperscript{165} Generally speaking, Californians for Consumer Privacy deemed the referendum and subsequent law a success for privacy rights.\textsuperscript{166}

The original CCPA initiative was based on three main principles – transparency, control, and accountability – and the enacted law encompasses all of these objectives in some way.\textsuperscript{167} First, the group wanted more transparency about what personal information companies collect about us, our children, and our devices, and who they are selling it to.\textsuperscript{168} Second, the group wanted to give consumers the ability “to tell companies not to sell their personal information” and ensure companies shouldn’t be able to retaliate against consumers who exercise this choice.\textsuperscript{169} Third, the group wanted to hold companies more accountable if they fail to take good care of your personal

\textsuperscript{163} See id. (describing legislative referendum history).

\textsuperscript{164} See generally Nefi Acost, et al, \textit{The California Consumer Privacy Act: 3 Early Questions}, LAW 360 (July 2, 2018), (alleging flaws of referendum include: “statutory damages provision for any violation of the CCPA’s new duties, a new whistleblower and private attorney general enforcement system and a provision prohibiting further amendments to the initiative without 70 percent approval in the Legislature”).

\textsuperscript{165} See id. (explaining technology companies wanted to mitigate impact of the initiative with control of lawmakers to amend legislation, unlike qualified ballot initiatives).


\textsuperscript{167} See generally About the California Consumer Privacy Act, CALIFORNIA CONSUMER PRIVACY ACT, https://www.caprivacy.org/about (last visited Feb. 20, 2020).


information after multiple, massive data breaches.\textsuperscript{170} The group laid out ten specific requirements to protect the consumer’s right to privacy, but not all of the provisions were included in the final bill, or enacted law.\textsuperscript{171} As previously stated, California’s CCPA did not extend privacy rights as far as the GDPR due to political pressures of Big Data companies, a lack of debate and hasty passage, and different legal regime.\textsuperscript{172} As a byproduct of the hasty passage there are some ambiguities or “drafting defects” that will lead to confusion – “[w]hat will plaintiffs have to show to recover statutory damages,” “[w]hat obligation does the CCPA impose on covered business to make California residents’ data portable,” and “[h]ow much flexibility will businesses have in responding to request to be forgotten” – and subsequent litigation will surely ensue for lawyers, courts, and regulators to work through.\textsuperscript{173}


\textsuperscript{171} See supra note 163 (attempting to give consumers the ability to control their personal information, including: “(1) Right to know ALL data collected by a business on you, twice a year, free of charge; (2) Right to say NO to the sale of your information; (3) Information Security: Right to sue companies who collected your data, where that data was stolen or disclosed pursuant to an unauthorized data breach, if the company was careless or negligent about how it protected your data (i.e. if the data was unencrypted, un-redacted, or the company didn’t have reasonable security policies and procedures in place to protect it). Identity Theft needs to be curbed!; (4) Right to DELETE data you have posted; (5) Right not to be discriminated against if you tell a company not to sell your personal information; (6) Right to be informed of what categories of data will be collected about you prior to its collection/at point of collection, and to be informed of any changes to this collection; (7) Mandated opt-in before sale of children’s information (under the age of 16); (8) Right to know the categories of third parties with whom your data is shared; (9) Right to know the categories of sources of information from whom your data was acquired; (10) Right to know the business or commercial purpose of collecting your information.”).

\textsuperscript{172} See Acost, supra note 164 (reviewing flawed legislative process).

\textsuperscript{173} See Acost, supra note 164 (explaining possibility California legislature may pass technical fixes or substantial amendments if lobbyist are able to persuade legislators to change law, while Attorney General also has discretion to interpret and avoid litigation).
The CCPA regulates a wide array of entities in order to protect individuals’ rights to privacy. The CCPA regulates for-profit businesses that meet one of the three requirements: (1) has a gross revenue greater than $25 million, (2) buys, receives, sells, or shares the personal information of more than 50,000 consumers, households, or devices, and (3) “derives 50 percent or more of its annual revenues from selling consumers’ personal information.” The CCPA has far less jurisdictional reach than the GDPR, essentially affecting all companies engaged in interstate commerce within the state of California. The CCPA protects California residents, who are domiciled in the state, and consumers, who include customers of household goods and services, employees, and business-to-business transactions. The CCPA provides equally broad protections as the GDPR with more of a specific definition relating to consumers.

The CCPA defines personal information, its potential uses, and its opt-in versus opt-out policy in a comprehensive way. The personal information covered under the CCPA is defined as anything that can be identified, related to, described, is capable of being associated with, or may reasonably be linked, directly or indirectly with a consumer or household. The CCPA exempts government records and, unlike the GDPR, includes a household or device specific caveat to personal information. Under the law, companies are

---

175 See CCPA, supra note 4 at 1798.140 (defining businesses required to comply with consumer protections).
176 See id. (emphasizing 1798.140(b) number of households and its potential effect on interstate commerce); contra GDPR, supra note 3 at art. 3 (describing territorial scope).
177 See CCPA, supra note 4 at 1798.140 (defining personal information and providing brief definition of consumer, as well as citing § 17014 of Title 18 of California Code).
178 See id.; contra GDPR, supra note 3 at art. 4(1) (defining personal data).
179 See id. (allowing for broad interpretation).
180 See CCPA, supra note 4 at 1798.140 (o)(1) (elaborating on definitional caveats).
181 See CCPA, supra note 4 at 1798.140 (“publicly available means information that is lawfully made available from federal, state, or local government records”).
provided discretion to utilize personal information that is de-identified or aggregated. Additionally, one of the major rights afforded is notice for collection and notice of breaches. The CCPA requires businesses to inform customers what categories of personal information is being collected and why. If the reason for collection changes after consent is given, notice must be given, and consent can be withdrawn. The CCPA provides consumers the ability to opt-out of the sale of personal information to third parties and must include a “Do Not Sell My Personal Information” link on a website’s homepage.

The CCPA provides that a business cannot discrimination against a consumer for exercising their rights, however, a company can provide financial incentives for opt-in consent to using their personal information. Any company found in violation of the privacy rights set forth in the CCPA will have a 30-day period to remedy the violation. However, consumers may bring lawsuits seeking up to $750 per consumer per incident and the government can fine the company up to $7,500 per violation. Three of the most important rights under the CCPA, similar to that of the GDPR, are the right of disclosure of access, right of data portability, and right to deletion or erasure.

3. The Implication of Federal Preemption on Compliance

In 2017 alone, 42 state legislatures introduced 240 bills or resolutions related to cyber security and data privacy. Needless to
say, Big Data companies are worried about the possible ramifications of these laws on their businesses. Fear of uncertainty, companies that have been "largely untouched by regulators" are now lobbying the federal government to preempt the states with its own industry devised data privacy regime. On September 26, 2018, executives and representatives from six Big Data companies – Amazon, Apple, AT&T, Charter, Google and Twitter – testified to Congress urging lawmakers to preempt the CCPA and other state regulations with its own federal data privacy framework. The Big Data companies have warned that "inconsistent" or "conflicting" regulations would lead to detrimental "balkanization of services" for consumers both internationally and domestically. Big Data provides a strong argument that data privacy regulations on the federal level will be more efficient for both companies and consumers, so long as Congress reassures the American people that lobbying interests are minimized and consumer rights are a priority.

At the Congressional hearing, Big Data representatives recognized the importance of transparency and the right to privacy but were unable to agree on or articulate certain important regulatory issues. For instance, the representatives denied selling user data and didn’t want to talk about notice, consent, nor control. Moreover, on the debate of opt-in versus opt-out, the response was uniformly that
"the digital ecosystem is just too complicated for people to make meaningful choices about each piece of data and each company that gets to touch it." According to Google’s Chief Privacy Officer, Keith Enright, Google believes if companies required users to check a box for every processing option it would “degrade the service” and “disincentivize users from engaging.” These responses are the very reason for regulation in the first place.

Big Data companies are not typically interested in the privacy rights of consumers – it’s all about the monetizing information – and our government must put consumer rights ahead of corporations seeking to maximize profits with our data. Google testified that GDPR compliance has cost “billions of dollars” of infrastructure investment and “hundreds of years” of employee hours. There is a lot of money at stake for Big Data companies, for example, the CCPA referendum compelled companies like Facebook, Google, Comcast, AT&T, Verizon, Microsoft and Uber to contribute almost two million dollars to a Political Action Committee to oppose the CCPA initiative. According to the privacy group in favor of the CCPA, rumor had it that the PAC was willing to spend more than $100 million dollars to oppose the measure in the November election.

Thus, lawmakers should be weary of lobbying interest and gain input from privacy advocates, businesses, and regulators to ensure the privacy rights of individuals are upheld. Understandably, striking a

199 See id. (emphasizing need for all in approach to negotiate any issues).
200 See id. (discussing potential user-friendly options for opt-in versus opt-out options).
201 See infra notes 197-200 and accompanying text.
202 See Aleks Krotoski, Big Data age puts privacy in question as information becomes currency, GUARDIAN (Apr. 22, 2012), https://www.theguardian.com/technology/2012/apr/22/big-data-privacy-information-currency (“Exploiting Big Data’s opportunities will need a delicate balance between the right to knowledge and the right of the individual”).
203 See Bernstein, supra note 193 and accompanying text.
204 See id. (discussing opposition to the original initiatives from tech companies).
205 See id. (illustrating lobbying efforts on behalf tech companies like Google).
balance between privacy and business concerns is crucial too. Industry groups claim that small companies and startups are being forced out of Europe and warn that the same could happen in California. Moreover, not all of the executives at the Congressional hearings dismissed privacy rights. Damien Kieran, Twitter's Global DPO, believes “privacy is a fundamental right, not a privilege” and supports a “robust framework that balances the protection of individual’s rights and the preservation of the freedom to innovate.” In theory a self-regulated industry sounds ideal, but the federal government should intervene and hold companies accountable for constitutionally derived rights.

Data privacy regulation affects nearly every company because every company is a data company in some capacity or another. From the perspective of businesses, unchecked regulators are seen as a threat to company revenue in the form of higher operational expenses. Ultimately these expenses will result in higher costs for consumers passed on via product prices and service fees. Arguably in the context of data privacy, consumers want to maximize protections and businesses want to minimize costs, thus comprehensive and uniform federal legislation not individual state regulations would be most

---

207 See id. (noting stakeholder various interests).
208 See Bernstein, supra note 193 and accompanying text.
209 See Bernstein, supra note 193 and accompanying text.
212 See supra note 5-6 and accompanying text.
effective and efficient.\textsuperscript{214} In order to combat the growing possibility of individual state regulations, Big Data companies are willing to spend millions of dollars to lobby lawmakers and their constituents to ensure the monetization of personal information is protected and compliance does not disrupt their financial operations.\textsuperscript{215}

\textbf{D. Compare and Contrast GDPR v. CCPA}

The GDPR and CCPA are equally challenging but impose different duties and obligations.\textsuperscript{216} Therefore, companies that are now compliant with the GDPR data privacy framework will not be compliant with the CCPA data privacy framework and should plan accordingly.\textsuperscript{217} It is undisputed the GDPR creates more data privacy rights with broader implications to the business community than the CCPA.\textsuperscript{218} For instance, there are some "GDPR data subject rights that have no equivalent under CCPA," such as the right to object, the right to restriction, and the right not to be subject to automated decision-making.\textsuperscript{219} That being said, the three rights that are broadly comparable between the two regimes are access, erasure, and portability; however,

\begin{footnotesize}
\begin{enumerate}
\item See Pearl Cohen Zedek Latzer Baratz, \textit{Stakeholders in the U.S. advocating for a federal privacy law}, LEXOLOGY (Mar. 3, 2019), https://www.lexology.com/library/detail.aspx?g=57e80f50-d31c-4bd0-ab2a-b04dcf729ce0 (presenting desire of majority stakeholders for federal law and their lobbying efforts in Washington D.C. to accomplish such a goal for their interests).
\item See \textit{id.} (describing plans to sway political process for business convenience).
\item See \textit{infra} note 221-231 and accompanying text.
\item See Carol A.F. Umhoefer, \textit{CCPA vs. GDPR: the same, only different}, DLA Piper (Apr. 11, 2019) https://www.dlapiper.com/en/us/insights/publications/2019/04/ipt-news-q1-2019/ccpa-vs-gdpr/ ("Businesses that have undertaken GDPR compliance will have an advantage in addressing CCPA, but those efforts alone won’t suffice").
\item See Navdeep K. Singh, \textit{What You need to Know about the CCPA and the European Union’s GDPR}, A.B.A. (Feb. 26, 2020), https://www.americanbar.org/groups/litigation/committees/minority-trial-lawyer/practice/2020/what-you-need-to-know-about-the-ccpa-and-the-european-unions-gdpr/ ("In terms of coverage, the GDPR is broader in scope than the CCPA, and encompasses private companies, non-profit organizations, and public bodies and institutions; in contrast the CCPA is largely confined to for-profit businesses of a threshold size in terms of revenue and scale of operations").
\end{enumerate}
\end{footnotesize}
the laws differ with regards to the right to erasure, right opt in versus opt out, requiring a DPO, and enabling class action lawsuits.\footnote{220}{See Laura Jehl and Alan Friel, CCPA and GDPR Comparison Chart, BAKER HOSTETLER LLP, https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf (last updated Feb. 20, 2020) (providing overview comparison table).}

First, the right to be forgotten or the right to erasure and its procedural application differs under the GDPR and CCPA.\footnote{221}{See supra notes 222-223 and accompanying text.} Under the GDPR, the data subject must satisfy a condition for the data to be erased, and the controller must then erase the data, unless an exemption applies.\footnote{222}{See id. (distinguishing laws); see also CCPA, supra note 4, at 1789.105} Under the CCPA, the consumer doesn’t have to satisfy any conditions, but a finite and specific list of exemption exist under which the request can be refused.\footnote{223}{See infra notes 225-226 and accompanying text.} Second, the right to opt in versus opt out is different.\footnote{224}{See infra notes 225-226 and accompanying text.} The GDPR requires consumers to opt in to allow the data to be processed, whereas the CCPA requires consumers to opt out of allowing companies to sell their information.\footnote{225}{See id. (distinguishing laws).} The differences between opting in and opting out require companies to adjust every aspect of data collection.\footnote{226}{See id. (distinguishing laws).} Third, the CCPA does not require a DPO like the GDPR, though it does mandate that businesses train employees involved in compliance and responding to customer inquiries about the CCPA.\footnote{227}{See GDPR, supra note 3 at art. 37; see also CCPA, supra note 4 at 1798.150 (distinguishing laws).} Fourth, both laws create a cause of action for class action lawsuits to claim minimum statutory damages for data breaches and allows the state to impose fines for violations.\footnote{228}{See id. (distinguishing laws).} The class action and violation amounts differ, but the risk of non-compliance can be extremely high.\footnote{229}{See id.} For both laws, the jurisdictional reach has yet to be seen as it extends beyond domestic and international border.\footnote{230}{See Special Coverage: Broader Implications of California’s Sweeping Online Data Privacy Statue, LEXIS NEXIS (Sept. 12, 2018), https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/posts/special-coverage-broader-implications-of-california-39-s-sweeping-online-data-privacy-statute (discussing jurisdictional hurdle if California or E.U., cannot enforce regulations to non-CA businesses or non-EU businesses, then companies within their jurisdiction will hurt compared to competition).}
Essentially, any business involved in commerce could be subject to compliance regulations—whether these regulations will be enforced is yet to be seen.\textsuperscript{231}

\textbf{E. Economic Implication of Data Privacy Regulations on Big Data}

Big Data has gone relatively unregulated since its inception, resulting in an economic boom for technology companies and products or services they provide to nearly every company engaged in business.\textsuperscript{232} Companies utilizing business data and analytics have increased their operational efficiency and in turn their profitability.\textsuperscript{233} Data privacy regulations will affect the growth projection of Big Data in the short term, but the necessary evil of regulation will result in long term gains for companies and most importantly the protection of consumer rights.\textsuperscript{234} Companies will have a difficult time adapting to changing legal frameworks, but companies can mitigate their risk of non-compliance by purchasing data loss liability insurance until data privacy processes are fully implemented to avoid the potential for violation fines.\textsuperscript{235} The economic implications of compliance are executive management or board-level priorities and should be treated as such.\textsuperscript{236}

1. The Potential Economic Benefit of Unregulated Big Data

Big Data is buzzword that references “the dramatic rise of statistical and computational technology that allows for collection and analysis of data on everything.”\textsuperscript{237} Accordingly, data-driven growth has helped businesses minimize their utilization gap and maximize their incremental revenue.\textsuperscript{238} The vast amount of data collected today

\textsuperscript{231} See id. (emphasizing uncertainty in marketplace).
\textsuperscript{232} See infra notes 237-241 and accompanying text.
\textsuperscript{233} See infra notes 242-252 and accompanying text.
\textsuperscript{234} See infra notes 253-266 and accompanying text.
\textsuperscript{235} See infra notes 269-273 and accompanying text.
\textsuperscript{236} See infra notes 267-268 and accompanying text.
is useless without analysis and insight to help the decision-making processes generate a competitive edge in an increasingly competitive environment.\textsuperscript{239} Many companies that are shifting from data-driven to insights-driven analysis are growing on average “more than 30% annually and are on track to earn $1.8 trillion by 2021. Such companies will be growing 8-10 times faster than their non-insights-driven rivals, through 2021.”\textsuperscript{240} Big Data has big potential for businesses, big challenges for regulators, and big impacts for the economy.\textsuperscript{241}

The GDPR, CCPA, and the possibility of additional regulations now have more and more companies concerned about data privacy and security concerns.\textsuperscript{242} To remedy business concerns, new services and products will need to meet the demands for processing and handling data in light of recent regulations in a variety of different jurisdictions.\textsuperscript{243} The prominent players in Big Data - Amazon, Google, IBM, Microsoft, Oracle, Dell, Hitachi, VMware, HP, and Teradata - are complying with the law and continuing to generate large amounts of profit from data as if it were business as usual.\textsuperscript{244} It can be difficult


\textsuperscript{240} See Jeremy Harvey, Going from Big Data to Big Insights to Big Revenue, WICKET LABS (Sept. 4, 2018), https://www.wicketlabs.com/wicket-blog/going-big-data-big-insights-big-revenue/ (emphasizing data use increases profits and improves operations).


\textsuperscript{242} See id. (describing a recent study, respondents from companies reported “the top three barriers to more effective use of data and analytics are: 1. Data privacy and security concerns (as reported by 49% of respondents 2. Data access is limited across the organization (33%) 3. Current solution is too complicated (28%)”).

\textsuperscript{243} See Federal TM Ser. No. 88122323 (emphasizing the need for privacy assessments, regulatory compliance, and data management services for private entities and what that means lawyers, managers, and IT professionals as more work becomes readily available).

to comprehend the quantity of data companies are processing, for example, Google alone processes 2.4 million web searches per minute and Amazon generates a staggering $258,751.90 in sales and service fees per minute.\footnote{245} In general, companies that maximize their use of data analytics in the decision making process generate 12% more revenue than those who do not, and regulations limiting data use in any way will be problematic for these business.\footnote{246} Unfortunately, it is difficult to determine the actual amount of revenue companies generate from the sale of personal information and the extent of Big Data.\footnote{247}

The International Data Corporation ("IDC") recently released their semi-annual report and forecasted "worldwide revenues for Big Data and business analytics solutions will reach $260 billion in 2022 with a compound growth rate ("CAGR") of 11.9% over the 2017-2022 forecast period."\footnote{248} Currently, the five industries that are making the largest investments are "banking, discrete manufacturing, process manufacturing, professional services, and federal/central


\footnote{246} See Using Data to Maximize Value, BOSTON CONSULTING GROUP (Feb. 13, 2010), https://www.bcg.com/de-de/capabilities/big-data-advanced-analytics/maximizing-value.aspx; see also Taylor Armerding, Awash in Regulations, Companies Struggle With Compliance, FORBES (Aug. 30, 2019), https://www.forbes.com/sites/taylorarmerding/2019/08/30/awash-in-regulations-companies-struggle-with-compliance/#6d40b709150e ("compliance is complicated and expensive. Four year ago, experts were talking about “compliance fatigue,” given the number of standards and regulations organizations had to follow regarding the collection, sharing, and security of data.")

\footnote{247} See Matthews, supra note 240 ("it’s better to look at the revenue flowing in for the company which is directly tied to data handling and storage" since data not disclosed).

\footnote{248} See generally Revenues for Big Data and Business Analytics Solutions Forecast, IDC (Aug. 15, 2018), https://www.idc.com/getdoc.jsp?containerId=prUS44215218
2020] The General Data Protection Regulation and CCPA

government." The industries that will receive the largest revenue growth in return for their investment are "retail (13.5% CAGR), banking (13.2% CAGR), and professional services (12.9% CAGR)." The IDC report recognized the United States is "by far the largest geographic market," followed by Western Europe and the Asia-Pacific region. It is important to note that it is unclear whether the IDC report accounted for the potential adverse impact of data privacy regulations into consideration with these future growth projections.

2. Impact of Regulations on Growth

The cost of regulation in general is difficult to calculate, as there are very few unbiased studies about regulation and growth. That being said, one study estimates the cost of regulation in 2008 was $1.75 trillion. In the same year, total expenditures by the U.S. government were $2.9 trillion and 38% of the total was allocated for regulation expenditures. Regulations cost time, money, and effort since all businesses must comply with regulations on the international, federal, state, and local level. To put the cost of regulation into perspective, a recent journal estimated that federal regulations "reduced economic

249 See id. (listing industries that make up half worldwide BDA revenues at $81 billion).
250 See id. (providing industry revenue growth); see also Ricky Wayman, Compound Annual Growth Rate: What You Should Know, INVESTOPEDIA (Sep. 24, 2019), https://www.investopedia.com/investing/compound-annual-growth-rate-what-you-should-know/ (defining CAGR as the mean annual growth rate of an investment over a specified period of time longer than one year).
251 See supra note 248 and accompanying text (noting that United States is undoubtedly a geographic leader, but the market is expected to shift its momentum in favor of Asia).
252 See supra note 248 and accompanying text (discussing underlying numbers).
255 See id. (noting concerns of compliance from different government levels).
growth by about 2 percent per year between 1949 and 2005.” \(^{256}\) According to the journal, “if federal regulations were still at levels seen in the year 1949, current GDP would be $38.8 trillion higher.” \(^{257}\) If true, the claim is staggering, but Big Data has been able to grow unchecked and unregulated since its inception. \(^{258}\) Despite the economic benefits of Big Data for businesses – cost reductions, products development, service improvements, targeted marketing, operations optimization, and faster innovation in general – regulations are a ‘necessary evil’ to protect the rights of consumers. \(^{259}\) Historically, the United States government has balanced the interest of businesses and consumers – “business has both prospered and suffered as a consequence of government action [concurrently] consumers have been protected from exploitive business practices [via the] same government rules and regulations.” \(^{260}\) Large companies, unlike small companies, can absorb the cost of regulations by increasing their cost of business passed onto the consumers in inconspicuous price increases. \(^{261}\) The problem is that small businesses are the heart of America’s economy. \(^{262}\) Regulation adversely affects


\(^{257}\) See id. (emphasizing potential ramification of regulations of GDP).

\(^{258}\) See supra note 6 and accompanying text.


\(^{261}\) See id. (illustrating differences in how businesses handle regulation).

\(^{262}\) See generally Michael Hendrix, *Regulations Impact Small Business and the Heart of America’s Economy*, U.S. CHAMBER OF COMMERCE FOUNDATION (Mar. 14, 2017), https://www.uschamberfoundation.org/blog/post/regulations-impact-small-business-and-heart-americas-economy (describing majority of businesses are small); *see also* Geoffrey James, *Government Regulation is Good for Business*, CBS NEWS (Oct. 25, 2010), https://www.cbsnews.com/news/government-regulation-is-good-for-business/ (noting that according to the U.S. Small Business Administration (SBA), “99 percent of all independent enterprises in the country employ fewer than 500 people” by contrast “47.7 million Americans work for firms with 500 or more employees.”); *see also* Small Business and the Corporation: Chapter 4, U.S. DEP’T
small businesses more than large companies because regulatory compliance exerts a disproportionate burden on fixed costs. Higher fixed costs leads to less competitive prices against foreign companies and generate a level of uncertainty in the marketplace, both of which leads to reductions in investment and hiring. Due to these unintended consequences of regulations the CCPA, unlike the GDPR, takes into consideration the impact of data privacy regulations on small businesses and essentially exempts them based on the criteria for covered entities. By and large, regulatory accumulation “slows down economic growth,” however regulations do provide critical consumer benefits.

3. Data Insurance

The uncertain implications of data privacy regulations will have a significant impact on the operations of almost every company engaged in commerce. Therefore, GDPR and CCPA compliance should be a “board-level priority” in order to comply with the regulations and prevent financial consequences associated with

---

263 See id. (providing additional arguments against fixed costs).


265 See generally Sammi Caramella, California’s Own GDPR, How CCPA Will Affect Small Business, BUSINESS NEWS DAILY (July 23, 2018), https://www.businessnewsdaily.com/10960-ccpa-small-business-impact.html (describing that CCPA exempts companies making less than $25 million, while average revenue for small business is less and largely excluded, i.e. “businesses with 20 to 99 employees generate average revenue of $7,124,000.” However, all businesses should try to comply).

266 See McLaughlin, supra note 256 (discussing negative impact of regulations); see also Geoffrey James, Government Regulation is Good for Business, CBS NEWS (Oct. 25, 2010), https://www.cbsnews.com/news/government-regulation-is-good-for-business/ (discussing positive economic impact of regulations, “No government regulation = good for big business, bad for small business; Most government regulation = good for big business, bad for small business; Some government regulation = bad for big business, good for small business.”).

violations. Specifically, companies will need to immediately reevaluate their insurance policies to determine if coverage will mitigate any or all of the risks related to the heightened regulatory focus. Data insurance is vital to protect against costly and complex data breaches that happen more often than not, but not all insurance policies are created equal. For instance, some of the better and more costly insurance plans provide outsourced services to lessen the financial and reputation impact of privacy breaches and violations to companies, including: “expert legal, technical, compliance, and public relations services; victim notification and call center services, regulatory penalties or lawsuits, forensic investigation, and ongoing credit and data monitoring.”

It is yet to be determined whether or not insurance companies will cover the hefty fines associated with regulations violations - 4% of worldwide revenue or €20 million with the GDPR or $750 per person with the CCPA - or if the terms and conditions will exclude or limit such coverage. If insurance covers

---


270 See id.


272 See Alan Friel, SB-1121 Does Not Fix the CA Consumer Privacy Act, But Would Delay Enforcement, DATA PRIVACY MONITOR (Aug. 27, 2018), https://www.dataprivacymonitor.com/state-legislation/sb-1121-does-not-fix-the-ca-consumer-privacy-act-but-would-delay-enforcement/ (noting CCPA and GDPR are exempting some inherently data oriented companies like insurance companies and health care providers, but additional “11th hour” amendments or exemptions will likely follow).

238
these hefty fines and other regulation requirements, premiums associated with data insurance will surely rise.\textsuperscript{273}

\textbf{F. Regulatory Developments on the Federal Level}

The development of privacy law in the United States, starting with California’s CCPA, stems from the failure of businesses to self-regulate by neglecting basic consumer rights time and again.\textsuperscript{274} The passage of the CCPA may lead to costly individual state regulations and could potentially be detrimental to economic efficiency.\textsuperscript{275} Thus, technology companies have lobbied the federal government to preempt the states with the implementation of federal legislation governing data privacy rights.\textsuperscript{276} If legislation is implemented it will likely be administered by the Federal Trade Commission, an agency that has already taken action against data privacy breaches on its own accord.\textsuperscript{277} Federal data regulations are nothing new, President Obama attempted to pass a consumer protection bill but the political pressure was not available.\textsuperscript{278} Today, President Trump is attempting pass data regulations but it is unlikely it will accomplish anything especially in the form of an Executive Order.\textsuperscript{279} Ultimately, if Congress is unwilling to act, a possible legal alternative is an industry or judicially-created fiduciary duty.\textsuperscript{280}

\textbf{1. The Privacy Act of 1974 and The Federal Trade Commission Authority}

Congress passed the Privacy Act of 1974, and subsequently supplemented the law with the Privacy Act of 1980, establishing a "code of fair information practices that governs ... information about


\textsuperscript{274} See Adams, supra note 210 and accompanying text.

\textsuperscript{275} See supra note 232-266 and accompanying text.

\textsuperscript{276} See Bernstein, supra note 193 and accompanying text.

\textsuperscript{277} See supra note 281-287 and accompanying text.

\textsuperscript{278} See infra note 288-293 and accompanying text.

\textsuperscript{279} See infra note 294-300 and accompanying text.

\textsuperscript{280} See infra note 301-307 and accompanying text.
individuals ... by federal agencies."²⁸¹ Both of these Acts simply put into place operational processes for the federal government, neither of these Acts protected consumers from businesses nor enabled a private cause of action for litigation to defend the right to privacy.²⁸² However, under 15 USC §45, Section 5(a), the Federal Trade Commission ("FTC") has the authority to regulate "unfair or deceptive acts or practices in or affecting commerce."²⁸³ In 2016, the FTC used the "flexibility and breadth" of its authority to extend "its regulatory reach to the e-commerce impact of big data."²⁸⁴ The Commission argued "a material statement or omission that is likely to mislead a consumer acting reasonably under the circumstances" covers technological data concerns and initiated more than 100 privacy and data security enforcement actions.²⁸⁵ If Congress is unwilling to enact legislation to protect consumers, the FTC may be directed to enact more regulations within the current legal regime from the Executive Branch.²⁸⁶ On the other hand, if Congress is willing to enact legislation to help protect consumers, the FTC will likely be the federal agency to implement such consumer regulations.²⁸⁷


²⁸² See id. (discussing government not business impact).


²⁸⁵ See id. (summarizing commission findings on privacy law concerns).

²⁸⁶ See id. ("If a company violates a material promise—whether that promise is to refrain from sharing data with third parties, to provide consumers choices about sharing, or to safeguard consumers’ personal information—it will likely be engaged in a deceptive practice," it noted. Furthermore, "Companies that maintain big data on consumers should take care to reasonably secure that data commensurate with the amount and sensitivity of the data at issue, the size and complexity of the company’s operations, and the cost of available security measures.").

²⁸⁷ See id. ("The FTC has provided guidance on collecting, using, and protecting the privacy of consumers, but focus on proper disclosures, keeping promises, and maintaining adequate security.").
2. President Obama and the Consumer Privacy Bill of Rights

Past presidential administrations have discussed the need for privacy regulations, but few have been able to make any substantial policy changes outside of the Oval Office.\footnote{See Mulligan, supra note 281 and accompanying text.} Under President Obama, the White House announced "a comprehensive review of the way that big data will affect the way we live and work; the relationship between government and citizens; and how public and private sectors can spur innovation and maximize the opportunities and free flow of this information while minimizing the risks to privacy."\footnote{See generally Big Data and the Future of Privacy, ELECTRONIC PRIVACY INFORMATION CENTER, https://www.epic.org/privacy/big-data/ (last visited Feb. 20, 2020) (recognizing national legislation needed but not formulated to extend protection).} The Obama administration released the Consumer Privacy Bill of Rights ("CPBR") in 2012 and sought feedback from privacy advocates and Big Data companies alike.\footnote{See id. (surveying sought feedback on the following: "(1) What potential harms arise from big data collection and how are these risks currently addressed?, (2) What are the legal frameworks currently governing big data, and are they adequate?, (3) How could companies and government agencies be more transparent in the use of big data, for example, by publishing algorithms?, (4) What technical measures could promote the benefits of big data while minimizing the privacy risks?, (5) What experience have other countries had trying to address the challenges of big data?, (6) What future trends concerning big data could inform the current debate?").} Within the framework for protecting privacy and promoting innovation it included the following principles – individual control, transparency, respect for content, security, access and accuracy, focused collection, and accountability.\footnote{See id. (listing principles enshrined in mock framework).} Unfortunately, the CPBR was unable to gain bipartisan support on Capitol Hill, but it emphasized and set the precedent that data privacy regulations are a presidential-level issue.\footnote{See Mickey Meece, President Obama's Consumer Privacy Bill of Rights, FORBES (Feb, 23, 2012), https://www.forbes.com/sites/mickeymeece/2012/02/23/president-obamas-consumer-privacy-bill-of-rights/#259cb65789ba ("...he says he expects any bill to generate "vehement opposition from lobbyists on Capitol Hill, who represent these large online companies with tremendous financial clout...It will be interesting to see if the bill will be watered down by Congress, added Hayes, a professor at Pace").} In a speech, President Obama stated that "even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion
that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever.”

3. President Trump and a Potential Executive Order on Data Privacy

As of 2017, the Trump administration had interest in working toward a proactive, rather than reactive, approach to consumer privacy regulations via legislation, agency regulations, or Executive Orders. The Trump administration’s plan hopes to modernize federal law in order to “spur greater domestic and even global regulatory harmony.” Given the pro-business and deregulation agenda, it is uncertain whether any regulations proposed by the current administration will actually expand protections for consumers’ data or just make it easier for corporations to continue exploiting consumer data and consumer rights. All in all, a federal regulatory initiative will be complex and difficult to pass given the varying special interests groups and partisan politics in Washington D.C. today. It will be impossible for federal regulations to be “all things, to all people” but difficult decisions and bipartisan compromises will have to be made to address the rapid, ever-changing advances in technology. Federal regulations will disrupt the economy, but differing international standards and state law conflicts will involve an even bigger economic impact if not addressed sooner than later. The need for regulations

295 See id. (deeming President Trump and his administration’s data regulation ideas as an “ambitious proposal” and “laudable goal”).
296 See id. (describing Executive Order 12866, or “Reducing Regulation and Controlling Regulatory Costs,” requires repeal of two old regulations for each new regulation).
298 See id. (discussing need for compromise).
299 See David McCabe, Congress and Trump Agreed they want a National Privacy Law. It is nowhere in Sight, N.Y.T. (Oct. 1, 2019), 242
is a priority now more than ever because if companies continue to go unchecked, not only will they have the ability to use personal information to make informed business decisions but will also have the ability to “manipulate users, push agenda, or discriminate surreptitiously” against consumers.  

4. A Fiduciary Duty as a Hypothetical Solution

The imposition of a fiduciary duty, a legal or ethical relationship of trust, between consumers and service providers may help reduce “information asymmetries” and ensure personal information is used in ways “consistent with users’ expectations.” A fiduciary duty does not currently exist in the United States, but the CCPA has taken steps to “level the playing field.” At this point, there are only two ways to develop a fiduciary duty – “one involving legal changes and the other involving industry changes.” Given Big Data’s lack of self-regulation and unwillingness to embrace industry regulations, legal changes involving statutes and a fiduciary duty could be an alternative to develop privacy rights. In essence, implementing a fiduciary duty in addition to statutory regulations, will ensure “that the era of Big Data does not necessarily mean the end of personal privacy.” Private action and public enforcement will help further individual protections of fundamental privacy rights. That being said, to the dismay of privacy activists “some people may find the tradeoff of privacy for convenience worthwhile, or come to accept this diminution of privacy as inevitable, and perhaps not.”


301 See id. at 19 (noting absence of fiduciary duty in United States).
302 See id. at 48 (referencing CCPA).
303 See id. at 47 (describing path).
304 See id. (noting that in order to legally develop a fiduciary duty there would need to be “(1) a federal statute that impose the duty on service providers, and (2) enforcement in courts.” A federal statute should generally describe covered entities and duty, but allow courts to determine what a “reasonable user” should expect. A law will have to continue to develop and adapt with technology advances and way we interact with it does too.).
305 See id. at 49 (noting possibility of coexistence or fiduciary duty and regulations).
306 See id. (strengthening argument of joint enforcement).
307 See id. (citing Justice Sotomayor).
Progress for the sake of progress should be discouraged, at some point lawmakers need to stop and regulate Big Data before the federal government loses control of the data revolution all together. Any new local, state, or federal data protection law will have intended and unintended consequences. Now is the time for Congress to act since states, lobbyists, and consumers are seeking guidance on data regulations. According to the World Economic Forum, 83% of Americans want tougher regulations for data privacy, and executives from six technology companies are advocating for intervention.\(^3\) The global regulatory environment toward Big Data is not accelerating, it is just catching up, and businesses are rightfully worried about the economic impact.\(^3\) The “tsunami of activity” involving Big Data could cause business to suffer from regulation fatigue, especially since additional legislation and increase litigation is inevitable.\(^3\) Congress needs to act swiftly to implement a federal regulatory framework for data that balance the interests of pro-privacy advocates and pro-business lobbyists. A uniform, comprehensive regulation on the national level will protect the right to privacy and mitigate the impact to businesses in the wake of the General Data Protection Regulation in the European Union and California Consumer Privacy Act in the state of California.\(^3\) The economy will eventually recover and adapt to


\(^{309}\) See John Burn-Murdoch, Data protection law is in danger of lagging behind technological change, GUARDIAN (Apr. 12, 2013), https://www.theguardian.com/news/datablog/2013/apr/12/data-protection-law-lagging-behind-technology ("Laws is always going to be playing catch up to technology").


\(^{311}\) See Mitchell Noordyke, US State Comprehensive Privacy Law Comparison, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, https://iapp.org/resources/article/state-comparison-table/ (last updated Feb. 20, 2020) (providing overview of state by state data privacy protections and emphasizing need for uniform federal law to prevent additional state laws leading to increasing or conflicting compliance costs); see also Joseph J. Lazzarotti, Maine and Nevada Sign
new regulatory regimes, however, the right to privacy cannot be restored and upheld if not protected by a much needed regulatory regime.