DePaul University
UNIVERSITY LIBRARIES

DePaul Business & Commercial Law Journal

Volume 21
Number 2 *Spring 2023 Symposium Edition: "Ethical Innovation in Our Changing World"*

Article 6

Federal Data Privacy Regulation: Do Not Expect an American GDPR

Matt Buckley
DePaul University College of Law

Federal Data Privacy Regulation: Do Not Expect an American GDPR

*Matt Buckley**

I. INTRODUCTION 147
II. GDPR & US STATE-BASED DATA PRIVACY 149
A. *EU's Approach to Data Privacy Regulations: GDPR* 149
1. Definitions and Scope of the GDPR 150
2. Consent and Lawful Data Collection 151
a. Principles Applicable to the Controller 151
b. Consent 151
c. Provision of Information 152
3. Rights of the Data Subjects 153
4. Controller's Obligations Regarding Data Security 154
a. Security of Processing 154
b. Data Protection Officer 154
c. Enforcement 155
B. *US Approach to Data Privacy Regulations* 155
1. California 156
a. Definitions and Scope of the CCPA 156
b. Lawful Data Collection and Right to Opt-Out 157
c. Rights of the Data Subjects 158
d. Controller's Obligations Regarding Data Security 159
2. Virginia 160
a. Definitions and Scope of the VCDPA 160
b. Consent and Lawful Data Collection 161
c. Rights of the Data Subjects 161

* J.D. Candidate 2023, DePaul University College of Law; Publication Editor, DEPAUL BUSINESS & COMMERCIAL LAW JOURNAL. I would like to thank Professor Max Helveston, Lauren McKenzie, and the rest of the Editorial Board for their contributions and encouragement. I would also like to thank my girlfriend Kendall and parents Matt and Sheila for their unwavering support throughout the writing process. I was fortunate enough to have received the support of these individuals, along with many others who aided me in writing this note.

d. Controller's Obligations Regarding Data Security 161
3. Colorado 162
a. Definitions and Scope of the CPA 162
b. Consent and Lawful Data Collection 163
c. Rights of the Data Subjects 163
d. Controller's Obligations Regarding Data Security 163
4. Utah 164
a. Definitions and Scope of the GDPR 164
b. Consent and Lawful Data Collection 165
c. Rights of the Data Subjects 165
d. Controller's Obligations Regarding Data Security 165
C. *Comparing EU and US Approaches* 165
1. Comparing Definitions and Scope 166
2. Vast Differences in Approach to Consent and Lawful Data Collection 166
3. GDPR's Upper Hand on the Rights of the Data Subjects 166
4. Diverse Controller's Obligations for Data Security 167
5. Key Takeaways of the EU and US Approach to Data Privacy 168
III. EU AND US ACTIONS IN OTHER COMMERCIAL FIELDS DEMONSTRATE FUNDAMENTAL DIFFERENCES IN REGULATORY APPROACHES 168
A. *Antitrust* 168
B. *GMOs* 170
C. *ESG* 172
IV. HOW STRUCTURAL DIFFERENCES BETWEEN THE EU AND THE US COULD AFFECT FEDERAL REGULATION .. 174
A. *Differences in Legislative Philosophy* 174
B. *Political Influence* 176
C. *Differences in Regulatory Legal Cultures* 178
V. WHAT WILL FEDERAL REGULATION OF DATA PRIVACY LOOK LIKE? 179
A. *Differences Between the Current Data Protection and Privacy Regimes* 179
B. *Where We Are Heading* 180
VI. CONCLUSION 182

I. INTRODUCTION

It's happening to everyone, everywhere, all the time. In today's digital age, data collection, sharing, and usage have become critical concerns for individuals, businesses, and regulators worldwide. With personal information often included in this data, the potential for its misuse, destruction, or theft can result in devastating financial and personal harm.[1] As a result, consumers are becoming more aware of their data being collected, how it is being utilized, and their rights when their data is compromised.[2] Recent high-profile scandals at Google and Facebook have heightened such consumer awareness. Facebook was fined $5 billion for allowing Cambridge Analytica, a political consulting firm, to harvest the data of over 78 million unsuspecting users to aid its political consulting business.[3] Google was widely criticized for its failure to notify users of Google+ that their private data had been hacked.[4]

Despite growing consumer awareness, data collection remains a highly valuable commodity for companies; it allows them to monetize and sell that data or use it to better reach their target markets.[5] The Interactive Advertising Bureau estimated that US businesses spent over $22 billion acquiring and analyzing personal data.[6] As calls for data regulation increase, these companies have also expressed their own demands for data regulation. More, the tech industry has vigorously opposed private rights of action and is urging Congress to enact preemptory legislation.[7]

---

1. Max N. Helveston, *Reining in Commercial Exploitation of Consumer Data*, 123 Penn St. L. Rev. 667, 674–683 (2019); IBM Security Communications, *Cost of a data breach 2022: A million-dollar race to detect and respond*, IBM (July 22, 2022), https://newsroom.ibm.com/2022-07-27-IBM-Report-Consumers-Pay-the-Price-as-Data-Breach-Costs-Reach-All-Time-High; Ido Kilovaty, *Psychological Data Breach Harms*, 23 N.C. J. L. & Tech. 1, 18–19 (2021).

2. Lauren Davis, *The Impact of the California Consumer Privacy Act on Financial Institutions Across the Nation*, 24 N.C. Banking Inst. 499 (2020); Michael B. Jones, *Uncertain Standing: Normative Applications of Standing Doctrine Produce Unpredictable Jurisdictional Bars to Common Law Data Breach Claims*, 95 N.C. L. Rev. 201, 202 (2016).

3. Cathy Lee, *The Aftermath of Cambridge Analytica: A Primer on Online Consumer Data Privacy*, 48 AIPLA Q.J. 529, 531 (2020).

4. Joanna Kessler, *Data Protection in the Wake of the GDPR: California's Solution for Protecting "The World's Most Valuable Resource"*, 93 S. Cal. L. Rev. 99, 101 (2019).

5. Christopher Bret 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, 228 (2020).

6. State of Data 2022: Assessing the Industry's Awareness and Readiness for Changes in Measurement and Addressability, Interactive Advertising Bureau, 18 (2022), https://www.iab.com/wp-content/uploads/2022/02/IAB_State_of_Data_2022_Master.pdf. Edit for reports.

7. Anna Edgerton, *Tech Lobbyists Don't Want States to Let You Sue Over Privacy Violations*, Bloomberg (March 20, 2023), https://www.bloomberg.com/news/articles/2023-03-20/big-tech-lobbyists-are-fighting-strict-data-privacy-laws-state-by-state#xj4y7vzkg; Jordan Crenshaw, *Ameri-*

While governments were slow to react to the explosion of digital technology innovations, there has been a marked increase in government involvement in technology regulation, spurred in significant part by the enactment of the European Union's General Data Protection Regulation ("GDPR", "Regulation"). The GDPR came into effect in 2018 after being enacted in 2016. This new regulation has significantly altered the way data is collected and processed, granting individuals new rights over their personal data. Its impact has been felt globally and has even influenced similar data regulations in the United States.

In 2018, the California Legislature enacted the California Consumer Protection Act (CCPA) which created the US's first comprehensive data regulations with general applicability.[8] Since then, four more states have enacted bills dealing with comprehensive data regulation, and the numbers are expected to continue growing. In 2018 only two states considered comprehensive data protection laws but in 2022 that number had grown to twenty-nine.[9]

With the potential for more data regulation coming from other states, companies are finding it challenging to meet the disparate requirements of different data regulation acts.[10] This has increased pressure on Congress to pass legislation that provides a national standard for data protection and consumer data rights in response to the growing number of laws sprouting up nationwide.

This Note argues that we should expect to see federal action and preemption in the area of data regulation, but that we should not expect to see a GDPR-style regulation in the United States. Parts I and II discuss the GDPR and recent data regulations that have been passed in California, Virginia, Colorado, and Utah. Part III highlights some key differences between the US and Europe. Part IV focuses on other areas of regulation, such as Antitrust, GMOs, and ESG disclosure, and how the US and EU differ in their approach to government intervention to protect consumer rights. Part V argues that a federal data protection bill is likely to balance the US's preference for market self-regulation with the need to protect consumers from invasive data collection practices.

---

cans Need Clear Data Protections, U.S. Chamber of Commerce (January 26, 2023), https://www.uschamber.com/technology/americans-need-clear-data-protections.

8. Davis, *supra* note 3, at 503–504.

9. Anokhy Desai, *The Growth of State Privacy Legislation*, International Association of Privacy Professionals (September 2022), https://iapp.org/media/pdf/resource_center/growth_of_state_privacy_infographic.pdf.

10. Edgerton, *supra* note 8.

II. GDPR & US STATE-BASED DATA PRIVACY

A. *EU's Approach to Data Privacy Regulations: GDPR*

Data protection and regulations have been revolutionized by the GDPR, which has been enacted in modified forms throughout the world. Initially proposed by the European Commission in January 2012, the GDPR underwent revisions during the consultation period before final approval by the EU Parliament in April 2016.[11] The GDPR repealed the Data Protective Directive 95/46/EC, which was created when the digital age was in its infancy. It came into effect in May 2018.[12]

Under EU law, there is an important difference between a regulation and a directive. Directives are more goal driven and offer guidelines and recommendations for member states but are not required to be implemented. On the other hand, regulations aim to influence and rectify specific issues affecting the EU with detailed legislation. Unlike directives, regulations do not require the passage of separate laws in the member-states and are immediately binding and enforceable.[13]

The EU takes pride in the privacy protections it provides to its citizens. This is indicated in Article 8 of the European Union Charter on Fundamental Rights, which states "[e]veryone has the right to the protection of personal data concerning him or her."[14] Additionally, it protects persons during the processing of their data "for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."[15] This language, approved in 2000, gave the impetus for the eventual passage of the GDPR which explains why the EU has enacted such broad data regulations.

The GDPR has two main goals. First is the "protection of natural persons with regard to the processing of personal data."[16] Second is the protection of the free movement of data which "shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."[17]

---

11. Alexander, *supra* note 6, at 215.

12. *Id.*

13. 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, 820–821 (2017).

14. Charter of Fundamental Rights of the European Union art. 8, 2016 O.J. C 202/389, at 395.

15. *Id.*

16. Regulation 2016/679/EC of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L 119/1.

17. *Id.*

1. Definitions and Scope of the GDPR

The GDPR aims to protect personal data and defines the term to mean any information that is currently or able to identify a natural person. Such identifiable information includes "a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[18]

In addition, the GDPR provides extra protection to what it calls "special categories" of personal data. These include race and ethnicity, political opinions, religious or philosophical beliefs, biometric data, healthcare data, or data concerning someone's sex life or sexual orientation.[19] Processing of these categories is prohibited unless certain requirements are met, such as "explicit consent."[20]

The GDPR applies to both automated and non-automated processing of personal data "which form part of a filing system or are intended to form part of a filing system."[21] However, these regulations do not apply to the collection of anonymous data.[22]

When personal data is monitored on the internet to create a profile and "particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors, and attitudes" it is considered processing activity.[23] It is important to note that if this occurs for a natural person in the EU, data collectors, also known as "controllers", must follow the regulation regardless of whether the processing occurs in the EU.[24]

Application of the GDPR is not limited to EU citizens but includes any natural person within the EU.[25] It also applies to controllers not established in the EU where (i) the data controller is offering goods or services (whether or not payment is required) or (ii) the controller or processor is monitoring the behavior of the data subject where that behavior takes place within the EU.[26] It is important to note that this means the Regulation applies to non-profits and government entities. The GDPR does not apply to data processing concerning legal persons or undertakings established as legal persons.[27]

---

18. Parliament and Council Regulation 2016/679, art. 4, 2016 O.J. (L 119) 1 (EC).
19. Parliament and Council Regulation 2016/679, art. 9, 2016 O.J. (L 119) 1, 38 (EC).
20. *Id.*
21. Parliament and Council Regulation 2016/679, art. 2, 2016 O.J. (L 119) 1, 32 (EC).
22. Parliament and Council Regulation 2016/679, recital 26, 2016 O.J. (L 119) 1, 5 (EC).
23. Parliament and Council Regulation 2016/679, recital 24, 2016 O.J. (L 119) 1, 5 (EC).
24. Parliament and Council Regulation 2016/679, recital 22, 2016 O.J. (L 119) 1, 4 (EC).
25. Parliament and Council Regulation 2016/679, art. 3, 2016 O.J. (L 119) 1, 32 (EC).
26. Parliament and Council Regulation 2016/679, art. 3, 2016 O.J. (L 119) 1, 33 (EC).
27. Parliament and Council Regulation 2016/679, recital 14, 2016 O.J. (L 119) 1, 3 (EC).

2. Consent and Lawful Data Collection

a. Principles Applicable to the Controller

Data controllers and processors must comply with Article 5, a catch-all article used in enforcement actions. Recent actions by the member-state Data Protection Authorities (DPA) have cited this article the most.[28] Article 5 states that personal data should be processed in a lawful, fair, and transparent manner and must only be collected for explicit, specific, and legitimate purposes.[29] In addition, data collection must be limited and relevant to what is necessary for the purposes they were requested and kept in a form that identifies data subjects for only as long as necessary. Finally, such data must be processed to ensure "appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures."[30]

b. Consent

In Article 6, the GDRP addresses when it is lawful to process personal data. Consent is one way, but data can also be processed if, (i) both parties are carrying out a contract, (ii) it is necessary for the performance of a task carried out in the public interest under official authority, or (iii) when it is necessary for legal compliance or to protect the vital interests of the data subject.[31] The burden is on the controller to prove that it obtained consent from the data subject, and they must keep a record of this consent.[32] Such consent must be in a clear affirmative manner and be a "specific, informed and unambiguous indication of the data subject's agreement."[33] This could include ticking a box on a website, choosing different technical settings, or other conduct indicating the data subject consented to the gathering of the data. However, Article 6 makes clear that "[s]ilence, pre-ticked boxes, or inactivity should not [ ] constitute consent."[34] The data subject has the right to withdraw their consent at any time and "[i]t shall be as easy to withdraw as to give consent."[35] The controller's data collection activi-

28. Brian Daigle & Mahnaz Khan, *The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities*, 332 Journal of International Commerce and Economics 1, 8 (2020).

29. Parliament and Council Regulation 2016/679, art. 5, 2016 O.J. (L 119) 1, 35 (EC).

30. *Id.*

31. Parliament and Council Regulation 2016/679, art. 6, 2016 O.J. (L 119) 1, 35 (EC).

32. Parliament and Council Regulation 2016/679, rec. 42, 2016 O.J. (L 119) 1, 8 (EC).

33. Parliament and Council Regulation 2016/679, rec. 32, 2016 O.J. (L 119) 1, 6 (EC).

34. *Id.*

35. Parliament and Council Regulation 2016/679, art. 7, 2016 O.J. (L 119) 1, 37 (EC).

ties prior to withdrawal are unaffected. The data subject must be informed of its rights to withdraw consent prior to or at the time of consent.[36]

It is important to note that the GDPR has special rules if the data subject is a child. If the data subject is 15 years old or younger, only the parent or guardian of the child can give consent.[37] Member states can lower this age, but not below 13.[38] Controllers need to make reasonable efforts to verify proper consent when children's data is at issue "taking into consideration available technology."[39]

c. Provision of Information

The GDRP has specific regulations regarding the collection of data. When collecting data from a data subject, the controller must provide certain basic information such as the identity and contact details of the controller and its data protection officer. The controller must also inform the data subject of their rights to request rectification, erasure, restriction of processing, and data portability. Additionally, they must inform the person about the existence of automated decision-making. If such processes are used, the data controller must provide "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[40]

The controller must provide specific information about why the data is being processed, the legal basis for doing so, and any recipients or categories of recipients of the data. They must also specify how long the data will be stored, the criteria used to decide this, and "whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract."[41]

Originally consenting does not relieve the controller from providing the data subject with their information if requested later. The controller must deliver the information in a clear manner and within one month of receiving the request except in certain situations. If the controller chooses not to fulfill the request, it must inform the data subject within one month and advise them of their right to lodge a complaint with a DPA.[42]

---

36. *Id.*
37. Parliament and Council Regulation 2016/679, art. 8, 2016 O.J. (L 119) 1, 37 (EC).
38. *Id.*
39. Parliament and Council Regulation 2016/679, art. 8, 2016 O.J. (L 119) 1, 38 (EC).
40. Parliament and Council Regulation 2016/679, art. 13, 2016 O.J. (L 119) 1, 40 (EC).
41. *Id.*
42. Parliament and Council Regulation 2016/679, art. 12, 2016 O.J. (L 119) 1, 39 (EC).

3. Rights of the Data Subjects

Under the GDRP, data subjects have the right to access their personal data and are expected to be able to exercise that right easily and at reasonable intervals.[43] This right is provided so that data subjects can be aware of and verify the lawfulness of the processing.[44]

The GDPR also grants a right to data subjects to rectify any inaccurate personal data and add a supplementary statement to incomplete personal data.[45] If there is a dispute regarding the accuracy of their information, data subjects also have the right to restrict the processing of their personal data.[46] The GDPR outlines several ways to restrict processing including "temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website."[47]

Another right that the GDPR provides is a right to be "forgotten" where a data subject has his or her personal data erased and no longer processed. This right applies when the data is no longer needed for its original purposes for which they were collected or processed, the data subject has withdrawn their consent, or objects to the processing of their data, or "where the processing of his or her personal data does not otherwise comply with [the GDRP]."[48]

Similar to the right to be forgotten is the right to erasure. This gives the data subject the right to obtain "the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay."[49] Here, the controller has the obligation to inform other controllers and processors that the data subject has requested the erasure of their personal data.[50] Whether a controller has taken reasonable steps depends on the available technology and the cost of implementation.[51]

Finally, the data subject also has the right to have their data given to them "in a structured, commonly used and machine-readable format."[52] This includes the right to request that the controller transmit

43. Parliament and Council Regulation 2016/679, art. 15, 2016 O.J. (L 119) 1, 43 (EC).
44. Parliament and Council Regulation 2016/679, recital 63, 2016 O.J. (L 119) 1, 12 (EC).
45. Parliament and Council Regulation 2016/679, art. 16, 2016 O.J. (L 119) 1, 43 (EC).
46. Parliament and Council Regulation 2016/679, art. 18, 2016 O.J. (L 119) 1, 44 (EC).
47. Parliament and Council Regulation 2016/679, recital 67, 2016 O.J. (L 119) 1, 13 (EC).
48. Parliament and Council Regulation 2016/679, art. 17, 2016 O.J. (L 119) 1, 43 (EC).
49. Parliament and Council Regulation 2016/679, recital 66, 2016 O.J. (L 119) 1, 13 (EC).
50. *Id.*
51. *Id.*
52. Parliament and Council Regulation 2016/679, art. 20, 2016 O.J. (L 119) 1, 45 (EC).

their data without hindrance, and if technically feasible, transfer it directly to another controller.[53]

4. Controller's Obligations Regarding Data Security

a. Security of Processing

Under GDRP regulations, controllers have to consider the nature and purposes of the processing as well as the various risks to the rights and freedoms of natural persons.[54] The GDPR requires that risk be "evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk."[55] A Controller must implement appropriate measures to ensure a level of security appropriate to the risk.[56] European regulators and data controllers shall take into account the "state of the art, the costs of implementation, the nature and purposes of the processing, and the risk for the rights and freedoms of natural persons, controller, and processor."[57] Controllers need to account for the risk of destruction, loss, and unauthorized disclosure or access to personal data.[58] Pseudonymization and encryption are mentioned as a way to comply with the regulation.[59]

b. Data Protection Officer

The GDPR requires controllers to designate a Data Protection Officer (DPO) and provide their contact information to the public and the DPAs.[60] The DPO should be chosen based on their professional qualities and expert knowledge of data protection law and practices relevant to the controller's collection activities and protection required.[61] The DPO may be an employee of the controller, or they can be hired as an independent contractor.[62] While the DPO may have additional job responsibilities, the controller must ensure that such duties do not create a conflict of interest.[63]

In addition, the DPO must play a crucial role in safeguarding personal data and must have access to personal data, processing opera-

53. *Id.*
54. Parliament and Council Regulation 2016/679, art. 24, 2016 O.J. (L 119) 1, 47 (EC).
55. Parliament and Council Regulation 2016/679, recital 76, 2016 O.J. (L 119) 1, 15 (EC).
56. Parliament and Council Regulation 2016/679, art. 32, 2016 O.J. (L 119) 1, 51 (EC).
57. *Id.*
58. Parliament and Council Regulation 2016/679, recital 83, 2016 O.J. (L 119) 1, 16 (EC).
59. Parliament and Council Regulation 2016/679, recital 28, 2016 O.J. (L 119) 1, 5 (EC).
60. Parliament and Council Regulation 2016/679, art. 37, 2016 O.J. (L 119) 1, 55 (EC).
61. *Id.*
62. *Id.*
63. Parliament and Council Regulation 2016/679, recital 97, 2016 O.J. (L 119) 1, 18 (EC).

tions, and any resources necessary to comply with GDPR regulations.[64] In doing so the DPO, (1) shall not be fired or reprimanded for performing their duties, (2) must report to the highest level of management of the controller, and (3) maintain independence.[65] The DPO is responsible for monitoring compliance, advising the controller of their GDRP obligations, and cooperating with the supervisory authorities.[66]

c. Enforcement

National data protection authorities enforce the GDPR in each EU member state.[67] These authorities are empowered to investigate complaints, conduct audits, and impose fines for non-compliance with GDPR rules.[68] If a data subject believes that their rights have been violated, they can file a complaint with their relevant data protection authority.[69]

Further, data protection authorities have the power to investigate complaints and initiate their own investigations into potential GDPR violations. They can also conduct audits of organizations to ensure compliance with GDPR rules.[70] If a violation is found under the GDPR, the DPAs can levy fines for non-compliance which reach up to _20 million or 4% of a company's global annual revenue, whichever is higher.[71] The exact amount of the fine depends on the severity and duration of the violation, as well as other factors.[72]

B. *US Approach to Data Privacy Regulations*

In contrast to the European Union, the United States does not have an overarching data privacy law.[73] Instead, there is a collection of federal laws that target specific types of data, with state data laws that vary in scope and impact on companies operating in those jurisdictions.[74] As a result, there is a patchwork of regulations that businesses and other entities must comply with. This section will examine the

64. Parliament and Council Regulation 2016/679, art. 38, 2016 O.J. (L 119) 1, 56 (EC).
65. *Id.*
66. *Id.*
67. Parliament and Council Regulation 2016/679, art. 51, 2016 O.J. (L 119) 1, 65 (EC)
68. *Id.*
69. Parliament and Council Regulation 2016/679, art. 77, 2016 O.J. (L 119) 1, 80 (EC)
70. Parliament and Council Regulation 2016/679, art. 58, 2016 O.J. (L 119) 1, 69 (EC)
71. Parliament and Council Regulation 2016/679, art. 83, 2016 O.J. (L 119) 1, 82–83 (EC)
72. *Id.*
73. Helveston, *supra* note 2.
74. Id.

data privacy laws in California, Virginia, Colorado, and Utah and compare them to each other and the GDPR.

1. California

The California Consumer Protection Act (CCPA) was enacted in response to the passage of the GDPR, but ironically, it came into existence in almost opposite circumstances. The CCPA's passage began with the efforts of a grassroots advocacy group called Californians for Consumer Privacy (CCP). With the support of wealthy backers, the CCP wrote a comprehensive data privacy bill and secured enough signatures to have their initiative placed on the ballot for a state-wide referendum.[75]

California legislators felt this initiative was too consumer friendly and did not strike the right balance between consumer protection and business innovation.[76] Tech industry leaders described it as a potential disaster for Californians.[77] In order to address fears from the tech industry and prevent the passage of a bill without their input, legislators, and proponents of the ballot measure reached a compromise.[78] This resulted in a modified version of the CCP initiative being signed into law on June 28, 2018, known as the California Consumer Protection Act (CCPA).[79]

The CCPA was amended by the voters of California in November 2020 and the California Privacy Rights Act ("CPRA") went into effect in January 2023. For clarity's sake, I will refer to both bills in their final incarnation as the CCPA.

a. Definitions and Scope of the CCPA

The CCPA defines two separate categories for information. Personal Information includes identifiers such as name, IP address, email address, protected class characteristics, sensory, biometric, and geolocation data, personal history of purchasing decisions and interactions, cookies, employment-related information, and using this information to create a profile."[80] Whereas, sensitive personal information includes (1) a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or

75. Kessler, *supra* note 5, at 106
76. *Id.*; Lee, *supra* note 4, at 535–536
77. *Id.*
78. Kessler, *supra* note 5, at 106
79. Alexander, *supra* note 6, at 223
80. Cal. Civ. Code § 1798.140(v)(1) ("A profile is a collection of information that reflects the consumer's "preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes").

access code, password, or credentials allowing access to an account, (2) a consumer's precise geolocation, (3) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership, (4) the contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication, (5) a consumer's genetic data, (6) personal information concerning a consumer's health, and (6) personal information collected and analyzed concerning a consumer's sex life or sexual orientation.[81]

In addition, the CCPA regulates the collection, sale, and processing of personal data.[82] However, if the information collected is deidentified or aggregated, businesses are allowed to collect, use, sell, or disclose consumer information.[83]

Finally, the CCPA only applies to for-profit entities doing business in California that meet any one of three thresholds: (1) gross revenue greater than $25 million (2) receives or shares the personal information of more than 50,000 consumers, households, or devices, or (3) 50 percent or more of its annual revenues are derived from selling consumers' personal information.[84] It only applies to data collected from residents of California and not to those who are there temporarily.[85] Non-profits and government entities are not subject to the CCPA.

b. Lawful Data Collection and Right to Opt-Out

The CCPA requires businesses, before or at the first point of collection, to inform consumers of the categories and purposes for which their personal information is collected and whether such information is sold or shared.[86] Special notice must be given if the information is sensitive personal information.[87] In addition, the amount of time the business intends to keep the information or what criteria determines the length of time such information is kept must also be included in its initial disclosure.[88]

If a business shares or sells information with a third party, it must enter into an agreement.[89] The third party must agree to limit the use or sale of information and to comply with the CCPA.[90] The business

81. Cal. Civ. Code § 1798.140(ae) (1)– (2).
82. Cal. Civ. Code §§ 1798.140(f), (y), (ad).
83. Cal. Civ. Code § 1798.145(a)(6).
84. Cal. Civ. Code § 1798.140(d)(1).
85. Cal. Civ. Code § 1798.140(i).
86. Cal. Civ. Code § 1798.100(a)(1).
87. Cal. Civ. Code § 1798.100(a)(2).
88. Cal. Civ. Code § 1798.100(a)(3).
89. Cal. Civ. Code § 1798.100(d).
90. *Id.*

also has the right to take reasonable steps to ensure compliance and to take remedial action if the third party violates the agreement.[91] Consumers are also protected in this scenario, the CCPA requires a notice to consumers that this information may be sold or shared and that consumers have the "right to opt-out" of the sale or sharing of their personal information.[92]

The CCPA also has rules for the collection of minor's data. A business shall not sell the information of a consumer if they have actual knowledge the consumer is under the age of sixteen.[93] Further, the business needs affirmative consent to sell the information if the child is between the ages of thirteen and fifteen, and parental consent is needed if they are younger than thirteen.[94] "A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age."[95]

c. Rights of the Data Subjects

California consumers have the right to access. Under the CCPA, consumers can request the following personal information from a business: (1) the categories of personal information it has collected about that consumer, (2) the categories of sources from which the personal information is collected, (3) the business or commercial purpose for collecting, selling, or sharing personal information, (4) the categories of third parties to whom the business discloses personal information, and (5) the specific pieces of personal information it has collected about that consumer.[96] Businesses must provide consumers with their personal information in a format that is "easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance."[97] More, businesses must provide these records and information free of charge.[98]

One right that was not in the original CCPA but was added under the CPRA and better aligns the law with the GDPR, is the right to rectify inaccurate personal information. Businesses are required to use

91. *Id.*
92. Cal. Civ. Code § 1798.120(a)–(b).
93. Cal. Civ. Code § 1798.120(c).
94. Id.
95. Id.
96. Cal. Civ. Code § 1798.110(a).
97. Cal. Civ. Code § 1798.130(a)(2).
98. Id.

commercially reasonable efforts to correct inaccurate information and must inform the consumer of this right during the initial disclosures.[99]

The CCPA also provides the consumer the option to request that a business delete any personal information about the consumer they have in their possession and this right must be informed before or at the time of collection.[100] Businesses must notify all third parties, to whom they have sold or shared this personal information, to delete the information unless this proves impossible or involves disproportionate effort. The CCPA requires third parties to delete, or enable the requesting business to delete, personal information about the consumer used or held by a third party upon such request.[101]

d. Controller's Obligations Regarding Data Security

Under the CCPA, businesses must implement reasonable security practices and procedures to prevent unauthorized access, destruction, or disclosure. What is considered reasonable is based on the nature of the personal information.[102]

Consumers have a private right of action when there is a data breach and certain personal information that would permit access to an account, is subject to theft, disclosure, or unauthorized access. However, businesses are not liable if they implemented and maintained reasonable security procedures and practices appropriate to the nature of the information.[103] Damages are limited to between $100 and $750 per consumer per incident or actual damages, whichever is greater.[104] The court can also grant injunctive or declaratory relief, or "[a]ny other relief the court deems proper."[105]

Before initiating a claim, consumers must provide a business with thirty days' written notice to the business that held the data subject to the breach and identify the specific provisions the consumer alleges have been violated.[106] There will be no statutory damages if the business is able to cure the violation and provide notice that they have been cured and won't happen again.[107] The consumer is not required to give notice if they are seeking pecuniary or actual damages as a

99. Cal. Civ. Code § 1798.106.
100. Cal. Civ. Code § 1798.105(a)–(b).
101. Cal. Civ. Code § 1798.105(c).
102. Cal. Civ. Code § 1798.100(e).
103. Cal. Civ. Code § 1798.150(a)(1).
104. *Id.*
105. *Id*.
106. Cal. Civ. Code § 1798.150(b).
107. Id.

result of a violation of this section.[108] The CCPA holds that the private right of action is limited and does not apply to any other section of the CCPA.[109]

The California Attorney General is empowered to bring suit for violations of the CCPA. Businesses are liable for a fine between $2,500 and $7,500 for each intentional violation.[110] A business is also potentially liable to be fined up to $7,500 for each violation involving the personal information of a consumer whom the business has actual knowledge is under 16 years of age.[111]

2. Virginia

Virginia became the second state to pass comprehensive data privacy legislation when Governor Ralph Northam signed the Virginia Consumer Data Protection Act (VCDPA) in March of 2021.[112] Virginia was the first state to do so without the threat of a referendum. In some situations, the VCDPA is more robust than the CCPA and borrows from the GDPR, and in other situations, it is even less stringent than the CCPA.

a. Definitions and Scope of the VCDPA

The definition of consumer under the VCDPA is quite narrow and is limited only to consumers "acting in an individual or household context," and excludes persons acting in a commercial or employment context.[113] This same narrow approach applies to the sale of personal information. The VCDPA provides that a sale of personal information is merely an exchange for monetary consideration only and excludes disclosures to a business affiliate.[114]

Like the CCPA, the VCDPA covers businesses that control or process the personal data of 100,000 or more consumers per year.[115] However, while the CCPA covers companies that have $25 million in revenue or get 50 percent or more of their revenue from data selling, the VCDPA only covers businesses that have $25,000 and derive more

108. Id.
109. Cal. Civ. Code § 1798.150(c).
110. Cal. Civ. Code § 1798.155(a).
111. *Id.*
112. Sarah Rippy, *Virginia passes the Consumer Data Protection Act*, International Association of Privacy Professionals, March 3, 2021, https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/.
113. Va. Code Ann. § 59.1-575.
114. *Id.*
115. Va. Code Ann. § 59.1-576.

than 50 percent of their gross revenue from the sale of personal data.[116]

b. Consent and Lawful Data Collection

The VCDPA and GDPR share similarities in requiring a contract between the controller and processor.[117] This contract sets forth the controller's instructions and the processor's duties to comply with the controller and the requirements of the Act.[118]

However, the VCDPA acts more as a middle ground between the CCPA and the GDPR on certain issues. Unlike the GDPR which has an opt-in requirement and the CCPA has an opt-out option for data collection, the VCDPA has an opt-in consent for sensitive information.[119] Sensitive information is a "category of personal data that includes biometric data, data collected from children, precise geolocation data and personal data that reveals racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation or citizenship or immigration status."[120]

c. Rights of the Data Subjects

The VCDPA provides the same rights to data subjects as those of the CCPA. These include the right to (i) opt out of data processing, (ii) access personal data, (iii) correct inaccuracies in personal data, (iv) deletion, and (v) obtain a portable copy of personal data. The right to opt-out is limited to (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling to further decisions that produce legal or similarly significant effects concerning the consumer.[121]

d. Controller's Obligations Regarding Data Security

Under the VCPA, data controllers are required to implement and maintain security practices that protect the "confidentiality, integrity, and accessibility of personal data."[122] These practices shall "be appropriate to the volume and nature of the personal data at issue.[123] More, controllers are required to undertake data protection assessments in certain situations.[124] If violations occur, VCDPA applies civil penalties

116. *Id.*
117. Va. Code Ann. § 59.1-579(A)–(B).
118. *Id.*
119. Va. Code Ann. § 59.1-578(A)(5).
120. Va. Code Ann. § 59.1-575.
121. Va. Code Ann. § 59.1-577(A).
122. Va. Code Ann. § 59.1-578(A)(3).
123. *Id.*
124. Va. Code Ann. § 59.1-580.

of up to $7,500 per violation and reasonable expenses, including investigation costs and attorneys' fees.[125]

Perhaps the biggest difference between the VCDPA and CCPA is the lack of a private right of action. While the CCPA has a narrow private right of action, it is noteworthy that Virginia decided not to include one when they are common in consumer protection legislation.[126]

3. Colorado

Colorado was the third state to pass comprehensive privacy legislation after Governor Jared Polis signed the Colorado Privacy Act (CPA) into law on July 7, 2021.[127] Colorado's data privacy regulations has some unique provisions, most notably that it also applies to nonprofit organizations.[128] Additionally, businesses must have a universal opt-out mechanism , aligning more closely with GDPR standards than other states' requirements.[129]

a. Definitions and Scope of the CPA

The CPA imposes obligations on companies to protect the privacy of consumers' personal data. Personal data is defined under the CPA as "information that is linked or reasonably linkable to an identified or identifiable individual." It does not include employment data, deidentified, or publicly available data.[130]

The CPA applies to entities that control the data of at least 100,000 Colorado residents. Additionally, it applies if an entity controls the data for 25,000 consumers and "derives revenue or receive a discount on the price of goods or services from the 'sale' of personal data."[131] A sale means "the exchange of personal data for monetary consideration or other valuable consideration by a controller to a third party."[132] This definition is like California's CCPA but broader than Virginia's, which only includes monetary consideration. As a result, data transfers like sharing cookies with marketers and advertisers to

125. Va. Code Ann. § 59.1-584(C), (D).

126. Va. Code Ann. § 59.1-584(E).

127. Cynthia J. Larose & Christopher J. Buontempo, *And Now There are Three . . .. The Colorado Privacy Act*, National Law Review (July 16, 2021), https://www.natlawreview.com/article/and-now-there-are-three-colorado-privacy-act.

128. Colo. Rev. Stat. Ann. § 6-1-1303(23)(a).

129. Colo. Rev. Stat. Ann. § 6-1-1306(1)(a)(IV)(A)–(B).

130. Colo. Rev. Stat. Ann. § 6-1-1303(17).

131. Colo. Rev. Stat. Ann. § 6-1-1304(1).

132. Colo. Rev. Stat. Ann. § 6-1-1303(23)(a).

target users across different platforms might qualify as a sale under the CPA.

One unique aspect of the CPA is that non-profit entities are not exempt under the Act. This is like the GDPR approach, but the CPA does not apply to government entities.

b. Consent and Lawful Data Collection

The CPA shares several similarities with its Virginia counterpart. Both require consumers to consent or opt-in to the sharing of sensitive data.[133] Also, both limit the protection of information to the personal or household context and specifically exclude commercial or employment contexts.[134]

However, Colorado is unique from all other states in its "Universal Opt-Out Mechanism," which communicates a consumer's "affirmative, freely given, and unambiguous choice to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data."[135] The purpose of the universal opt-out is to provide consumers with a simple and easy-to-use method that allows consumers to "automatically exercise their opt-out rights with all Controllers they interact with without having to make individualized requests with each Controller."[136]

The CPA also imposes a duty of transparency on the controller and contains the same disclosures required to be given to consumers as the CCPA and VCDPA.[137]

c. Rights of the Data Subjects

The CPA gives Colorado residents the same rights as those provided under the CCPA and VCDPA. These include (i) the right to opt out of data processing, (ii) the right to access, (iii) the right to correction, (iv) the right to deletion, and (v) the right to data portability.[138]

d. Controller's Obligations Regarding Data Security

A controller is given a duty of care regarding the data that they collect and receive under the CPA. The controller must take "reasonable measures to secure personal data during both storage and use from unauthorized acquisition." The security the controller imple-

133. Colo. Rev. Stat. Ann. § 6-1-1308(7).
134. Colo. Rev. Stat. Ann. § 6-1-1303(6)(a).
135. Colo. Rev. Stat. Ann. § 6-1-1306(1)(a)(IV)(A)–(B).
136. 4 CCR 904-3 Rule 2.02.
137. Colo. Rev. Stat. Ann. § 6-1-1308(a).
138. Colo. Rev. Stat. Ann. § 6-1-1306.

ments must be "appropriate to the volume, scope, and nature of the personal data processed and the nature of the business."[139]

Colorado has the stiffest sanctions of all state data privacy acts. The potential civil penalty maximum is $20,000 per violation, increased to $50,000 for violations committed against an elderly person.[140] There is no text in the CPA providing a private right of action.

4. Utah

Utah was the fourth state to pass a comprehensive data protection act, and the first "red" state to do so. For that reason, Utah might provide the best estimation of what conservatives would like from a national data privacy act.

a. Definitions and Scope of the GDPR

The Utah Consumer Privacy Act (UCPA) has a higher threshold for a business to fall under its regulations than all the other states because it combines the separate thresholds of the other states. The Act applies if the controller conducts or targets business in Utah, has $25 million or more in annual revenue, and there is control or processing of data of 100,000 or more consumers during a calendar year; or 25,000 or more consumers during a calendar year and deriving more than 50% of its gross revenue from personal data sales.[141]

One restrictive provision is Utah's definition of sale of personal data, which includes only monetary consideration, like Virginia.[142] The UCPA also has broad exemptions for third parties that are "consistent with a consumer's reasonable expectations" depending on "the context in which the consumer provided the personal data to the controller."[143] It also excludes disclosures directed by the consumer, performed to provide a product or service to the consumer, or made as part of a proposed or actual merger, an acquisition, or assumption of assets in bankruptcy.[144]

---

139. Colo. Rev. Stat. Ann. § 6-1-1308(d)(5).
140. Colo. Rev. Stat. Ann. § 6-1-112(1)(a)–(c).
141. Utah Code Ann. § 13-61-102(1).
142. Utah Code Ann. § 13-61-101(31).
143. *Id.*
144. *Id.*

b. Consent and Lawful Data Collection

Under the UCPA a consumer's right to opt-out is narrower than the other states and is limited to situations where the data was collected for targeted advertising or the sale of personal data.[145]

c. Rights of the Data Subjects

The most notable departure Utah made compared to other states is the absence of some of the key rights that have been part of data privacy regulations. For example, there is no mention of the right to correction in the UCPA. Another restriction is a consumer's right to deletion, which is limited to personal data that the consumer has provided directly to the controller.[146]

d. Controller's Obligations Regarding Data Security

The UCPA does not require controllers to conduct data risk assessments. While the act requires controllers to enter into data protection agreements with processors, the requirements are less onerous than other states to the point that a processor does not have to comply with reasonable audits or assessments by the controller, or to delete or return all personal data to the controller.[147]

Like other states, the Attorney General has the power to enforce the UPCA, but the power of the AG is limited. Enforcement actions by the Attorney General may only be initiated "[u]pon referral from" the Utah Division of Consumer Protection.[148] Thus, the Attorney General does not have independent authority or discretion to investigate and pursue violations of the UCPA on its own. Instead, the Division must receive a consumer complaint, conduct an investigation, and only refer the matter to the Attorney General on "reasonable cause" that "substantial evidence" supports a finding of the violation identified in the consumer complaint.[149] There is no private right of action under the UCPA.[150]

C. *Comparing EU and US Approaches*

We can see areas of regulation where the US and EU share broad similarities. But based on the state laws that have been passed so far, we can see that there are striking differences between the regulatory

145. Utah Code Ann. § 13-61-201.
146. *Id.*
147. Utah Code Ann. § 13-61-301(2).
148. Utah Code Ann. § 13-61-402.
149. Utah Code Ann. § 13-61-401.
150. Utah Code Ann. § 13-61-305.

regimes. These include what information and who is covered by the regulations. Other differences are the rights given and the duty the data controller has to data collection subjects. Lastly, we see clear differences between how they will attempt to enforce their data privacy regulations. This section will examine some differences and what that could mean for future US data privacy regulations.

1. Comparing Definitions and Scope

The GDPR data protection safeguards have been adopted in some US states, but only for sensitive information. Virginia and Colorado require individuals to opt-in, while California and Utah only allow consumers to limit sharing of sensitive information. This demonstrates that US lawmakers acknowledge the importance of safeguards the GDPR has applied to information but are choosing to do so selectively.

Another key difference is the scope of entities covered under the two approaches. The GDPR applies to any company in the EU or doing business there, regardless of whether they are non-profits or government bodies. The CCPA, on the other hand, targets mainly larger companies and those who deal with the collection and exchange of personal data. Other states have narrower scopes, with some lacking a revenue threshold, which means companies will escape regulation if they aren't processing massive amounts of customer data. Only Colorado has ventured to include non-profits under their data privacy protection umbrella.

2. Vast Differences in Approach to Consent and Lawful Data Collection

The biggest difference in its approach to data privacy is the GDPR's default option of opt-in and the CCPA's default option of opt-out. Under the GDPR, businesses need to have a lawful basis to collect data from data subjects, and if the basis is consent, then the controller must get the data subjects to agree to the processing. Under the CCPA, businesses can process personal information for any purpose, unless the consumer exercises their right to opt out. However, in Virginia and Colorado, the idea of opt-in is making its way into the US, just in a more limited form.

3. GDPR's Upper Hand on The Rights of the Data Subjects

The GDPR and state acts provide similar rights for data subjects, but the EU offers some unique rights not provided in US laws. For instance, the EU provides the right to rectification, which is absent

from the US statutes.[151] Additionally, the GDPR grants data subjects the right to object to processing and automated decision-making.[152] Finally, data subjects have the right to restrict processing in certain circumstances.[153] This indicates that EU regulators aim to establish broad and powerful rights, even if it results in compliance issues for entities.

4. Diverse Controller's Obligations for Data Security

The EU views data protection just as much as other valuable company assets. For example, the GDPR requires companies to hire a data protection officer. They have extensive obligations and must be qualified, empowered, and independent. The aim is to prioritize data protection in the same way human resources protections have grown more prominent in C-Suite structures today. The US data privacy acts do not have any such requirements.

Another difference is the EU's approach to data breaches. The EU has strict timelines and technical requirements for companies to follow when there has been a data breach. Under the GDPR data must also be protected in a "reasonable manner." In comparison, the CCPA does not provide such technical and rigid requirements. There is no timeline for when the data controller must give notice to the consumer or regulatory authorities. This demonstrates how the EU is willing to require businesses to protect the rights to data security, whereas the US relies on a balance between market forces and consumer expectations to regulate data breaches.

The penalties for data breaches under both regulations vastly differ in scope but lead to similar outcomes. As mentioned above, GDPR enforcement is delegated to the member state DPAs who can fine entities as much as 20 million euros or 4% of global revenues, resulting in significant fines for America's largest tech companies.[154] In keeping with the European preference for bureaucracy over litigation, there are no private rights of action for statutory damages.

The US also uses fines as a means of enforcement. In Virginia, the CCPA limits fines to between $2,500 and $7,500 for each unintentional and intentional violation.[155] More, as discussed above, under the

151. Parliament and Council Regulation 2016/679, art. 16, 2016 O.J. (L 119) 1, 43 (EC).

152. Parliament and Council Regulation 2016/679, art. 21, 2016 O.J. (L 119) 1, 45 (EC); Parliament and Council Regulation 2016/679, art. 22, 2016 O.J. (L 119) 1, 46 (EC).

153. Parliament and Council Regulation 2016/679, art. 18, 2016 O.J. (L 119) 1, 44 (EC).

154. Lawson Mansell, *GDPR Fines Increasing, but Big Tech Companies Avoid Maximum Fines*, Milken Institute (Oct. 5, 2022), https://milkeninstitute.org/article/tech-regulation-digest-october-2022-gdpr.

155. Cal. Civ. Code § 1798.155(a).

CCPA, there are private rights of actions for consumers, a staple of consumer protection law, but it is limited to data breaches. The other US states limit their enforcement to the Attorney General and Colorado is again an outlier with its high level of fines for violations.

5. Key Takeaways of the EU and US Approach to Data Privacy

While the intention and scope of the regulations are similar, key differences indicate how the US and EU will approach data privacy in the future. First, the GDPR applies to an almost limitless number of entities, whereas the US acts have seemed to be targeted only toward for-profit entities. Second, the GDRP also imposes different levels of duties and regulatory scrutiny that hint at the dissimilar ways they view the role of government in regulation and protection. Third, we see the different enforcement styles signal the approach they plan to take against violators of the regulations. While these differences could dissipate towards greater symmetry between the regulatory regimes, they could also foreshadow the different paths the US and EU will take toward privacy regulation.

III. EU and US actions in other commercial fields demonstrate fundamental differences in regulatory approaches

The US and EU have distinct differences regarding fundamental rights. These include the necessary amount of government intervention in market regulation, ensuring fairness, and protecting fundamental rights. These differences manifest themselves in their approach toward balancing costs and innovation, their reliance on empirical analysis, and the EU's preference for promoting broad goals compared to the US's focus on preserving the market. In this section, I will explore three areas where these differences are apparent: Antitrust laws (or competition laws in the EU), Genetically Modified Organism (GMO) regulations, and Environmental, Social, and Governance (ESG) disclosures. It is possible that these divergent approaches to regulation could portend a similar divergence in data privacy.

A. *Antitrust*

Antitrust and competition laws in both the US and EU touch upon market regulation, consumer protection, and citizen's rights, which may show the path of US divergence from EU law on data regulation. Like the GDPR, European competition laws have become the stan-

dard for nations around the world to base their own laws on.[156] The reason EU competition law has been so widely imported is that the laws are simple, and the regulatory regime is easier to implement. Additionally, the EU has a more administrative way of dealing with violations, in contrast to the more legalistic approach of the US settlement system.[157]

European approaches to competition law can be traced to their divergent view on government involvement in regulating the economy. Europe is more hands-on in order to preserve "a highly competitive social market economy."[158] Meanwhile, the US is more hands-off to preserve market efficiency.[159]

The EU has shown a proclivity to enforce its laws based on standards of fairness, whereas the US tends to require a showing of some kind of damages to the consumer in order to preserve market efficiency. One example is their approach to predatory pricing. Under EU competition law, if predatory pricing is shown, it is a per se violation.[160] While the US had previously used the same approach, the law now requires plaintiffs to show that the defendant cannot recoup their losses.[161]

Another example of different approaches to government intervention from the US and EU relates to exploitive abuses, such as excessive prices. The US's market-friendly discourages intervention unless there is a showing of another type of antitrust violation.[162] On the other hand, the EU has regulations in place to deal with these abuses more regularly.[163]

This difference in views has also influenced both the US and EU's approach to the use of empirical evidence in an attempt to regulate Antitrust behavior. The US tends to discourage intervention and show a greater trust and reliance on economic analysis and empirical evidence in its regulation of antitrust behavior. In contrast, although the

156. Anupam Chander et. al., *Catalyzing Privacy Law*, 105 Minn. L. Rev. 1733 (2021); Max Huffman & Andre Fiebig, *EU Competition Law: § 17:1*, Antitrust & American Bus. Abroad (4th ed. 2023)

157. Antonios E. Platsas, *Comparing and Contrasting the EU and the US Approach in Competition Law: So Close but So Far*, EU Antitrust: Hot Topics & Next Steps 481, 483–85 (2022).

158. Consolidated Version of the Treaty on the Functioning of the European Union art. 3, 2012 O.J. (C 326/51)

159. Antonios E. Platsas, *Comparing and Contrasting the EU and the US Approach in Competition Law: So Close but So Far, EU Antitrust: Hot Topics & Next Steps* 481, 482 (2022).

160. *Id.* at 483–85, 490

161. *Id.* at 490.

162. *Id.*

163. *Id.*

EU certainly uses empirical evidence, it is more likely to ignore that evidence if it feels there is a correction that needs to be made.[164]

However, while the US seems to have a more hands-off approach to competition regulation, the difference in enforcement regimes reveals this is not always the case. The US government can levy both civil remedies and even criminal penalties against a violator of Antitrust law.[165] Additionally, US law usually provides a private right of action along with administrative remedies.[166] On the other hand, the EU does not have criminal penalties for violating its competition laws and lacks substantial private rights of action.[167] This demonstrates that while the US government tends to have a narrower scope in its regulation, it has sufficient means to enforce its laws when necessary.

In short, the US and EU have both taken steps to regulate the collection and use of data, similar to their actions in the antitrust and competition arena. But the differences in their regulation of competition show that their solutions to a common problem are strongly influenced by their approach to the market and citizen-consumer protection.

B. *GMOs*

We see some of the same themes of government intervention, consumer protection, and trust of empirical analysis in the way the US and EU have approached GMOs. Specifically, the regulation of GMOs and data protection have developed along a similar path due to their rapid introduction and similar reactions from the public on both continents.

GMOs came onto the scene in the US in the early 1970s, when scientists began combining genes of different organisms to create new ones.[168] Like recent digital technology advancements, GMOs were seen as groundbreaking work that should not be impeded, and ripe for commercial exploitation.[169] In 1980, the Supreme Court allowed biotechnology products to be patented, and GMOs expanded rapidly.[170] Despite a limited understanding of the technology, the growth in profits allowed the early creators of GMOs to advocate for loose regula-

164. *Id.*

165. Eleanor M. Fox, *US and EU Competition Law: A Comparison*, Peterson Institute for International Economics, 341 (1999).

166. *Id.*

167. *Id.*

168. Diamond v. Chakrabarty, 447 U.S. 303 (1980)

169. *Id.*

170. *Id.*

tions, and public opinion never fully turned against the products.[171] There are parallels in the way internet technology has spread in the US, where technology became an integral part of everyday life without much regulatory oversight while its effects were still being understood.

The situation was the opposite in Europe, where GMOs were immediately viewed with suspicion, and regulation was dissipated amongst the member-states. The media in Europe focused on the lack of tangible benefits, the risk of harm, and the uncertainty of the technology. Negative public reaction push EU politicians and bureaucrats to take a hard line in their regulation of the emerging technology.[172]

Such differences in how the two bodies regulate GMOs can be attributed to the EU's precautionary principle.[173] This principle holds that if there is a chance the goods or market will cause harm, and there is no clear benefit, it should be highly regulated. Stated otherwise, a "[l]ack of solid scientific evidence about a potential risk should not discourage preventative regulation."[174] On the other hand, the US approach to GMOs allows technology to proceed if there is any proven benefit without a proven negative. There is a tendency for the EU to be wearier of false negatives, and the US wearier of false positives.[175]

It should follow that two entities as large as the US and EU would have enough staff with technical expertise to safely regulate GMOs that can please both parties. However, the problem is not determining the appropriate level of safety, but rather how to reconcile the divergent viewpoints on market regulation and risk assessment when it comes to emerging technologies. The EU has shown an inclination to slow down innovation in emerging technologies if the potential risks are outweighed by the benefits. We can see this line of thinking in its approach to the GDPR. New companies hoping to take advantage of the opportunity that collection brings will have to comply with stringent standards to use this ability. Conversely, the US tends to favor innovation over unclear harms and thus is likely to view data regulation in a similar manner.

---

171. Marc Firestone, *A Quick Look at Two Areas of Doctrinal Difference Between EU and U.S. Decision Makers*, 20 Tul. J. Int'l & Comp. L. 1, 31–32 (2011).

172. *Id*. at 32–33

173. *Id*. at 33

174. Ashley Henson, *Reaching for Environmental and Economic Harmony: Can TTIP Negotiations Bridge the U.S.-EU Chemical Regulatory Gap?* 43 Ga. J. Int'l & Comp. L. 727, 735 (2015).

175. Firestone, *supra* note 170 at 32.

C. *ESG*

ESG disclosure is a window into how the US and EU approach enforcing fairness and their willingness to intervene in the markets. In April 2021, the EU released the Corporate Sustainability Reporting Directive (CSRD) which mandates rigorous disclosure of Environmental, Social, and Governance (ESG) standards. The directive aims to "end greenwashing, strengthen the EU's social market economy, and lay the groundwork for sustainability reporting standards at [a] global level."[176] The CSRD will take effect in 2023.[177]

The CSRD will apply to companies in the EU, including subsidiaries of US companies, meeting at least two of the following three requirements: (1) more than 250 employees, (2) a turnover of more than _40 million, or (3) total assets of _20 million.[178] Additionally, the CSRD will apply to companies listed on an EU-regulated stock market, regardless of their location.[179] Non-EU undertakings that generate revenues in the EU above _150 million, and have either a large or listed EU subsidiary or a significant EU branch (generating _40 million in revenues) are also required to comply with the CSRD.[180] Like the GDPR, US companies that meet presence or operations thresholds in the EU will also be subject to CSRD.[181] Companies may be asked to report this information to the SEC, as other parties they deal with will be required to report their upstream and downstream effects.[182]

These new regulations introduce the concept of double materiality, which requires companies to report on ESG issues that are not only material to investors but also impact the wider public and the environ-

176. European Parliament Press Release IPR/49/611, Sustainable Economy: Parliament Adopts New Reporting Rules for Multinationals (Nov. 10, 2022).

177. Addisu Lashitew, *The coming of age of sustainability disclosure: How do rules differ between the US and the EU?* The Brookings Institution, (June 6, 2022), https://www.brookings.edu/blog/future-development/2022/06/06/the-coming-of-age-of-sustainability-disclosure-how-do-rules-differ-between-the-us-and-the-eu/.

178. Kolja Stehl, Leonard Ng & Matt Feehily, *EU Corporate Sustainability Reporting Directive—What Do Companies Need to Know*, Harvard Law School Forum on Corporate Governance, August 23, 2022, https://corpgov.law.harvard.edu/2022/08/23/eu-corporate-sustainability-reporting-directive-what-do-companies-need-to-know/#1b.

179. *Id.*

180. *Id.*

181. Emma Bichet, Jack Eastwood & Michael Mencher, *EU's New ESG Reporting Rules Will Apply to Many US Issuers*, Harvard Law School Forum on Corporate Governance, (November 23, 2022), https://corpgov.law.harvard.edu/2022/11/23/eus-new-esg-reporting-rules-will-apply-to-many-us-issuers/.

182. *Id.*

ment.[183] In March 2022, the SEC proposed a new set of rules on climate-related disclosures to provide greater accuracy and transparency for investors.[184] While the implementation of the new rules has been postponed, "given the greater acceptance of ESG and investors' need for accuracy in the reporting of ESG information, many expect that 2023 will see the rules finalized and an implementation process started."[185] The SEC was reluctant to weigh into the regulation of ESG reporting, but after the EU embraced ESG regulation, the SEC followed suit.[186]

The SEC proposed rules require listed companies to disclose information about their direct greenhouse gas (GHG) emissions, indirect emissions from purchased electricity or other forms of energy, and certain types of GHG emissions from upstream and downstream activities in their value chain. These are known as scopes 1,2, and 3 respectively. Companies must disclose information under scope 3 only if they have publicly set an emissions reduction target or the emissions are deemed material.[187]

The definition of material is based on the single materiality principle, which means it "emphasizes investor-focused risk governance and financial materiality."[188] This means that impacts on society do not need to be disclosed unless the information is material to investors, and thus the law does not try to advance a societal green agenda but informs the investing public.[189]

The CSRD, like the GDPR, has a wide breadth and can potentially affect almost every industry in the Union. The CSRD provides extensive standards in multiple environmental, social, and governance domains. The SEC regulations are very narrow and are in furtherance of the SEC's mandate to keep market information honest and transparent, as shown by the use of the single materiality principle.

There is also a difference in the applicability of the regulations. The SEC rules are expected to cover around 7,000 public companies that sell securities.[190] Under the CSRD, the number of companies regu-

183. Press Release, European Commission, *Sustainable finance: Political agreement on Corporate Sustainability Reporting Directive will improve the way firms report sustainability information*, (July 26, 2022). https://ec.europa.eu/newsroom/fisma/items/754701/en.

184. Zach Warren, *Upcoming SEC Climate Disclosure Rules Bring Urgency to ESG Data Strategy Planning*, Reuters, January 30, 2023, https://www.reuters.com/legal/legalindustry/upcoming-sec-climate-disclosure-rules-bring-urgency-esg-data-strategy-planning-2023-01-30/.

185. *Id*.

186. Lashitew, *supra* note 176.

187. *Id.*

188. *Id.*

189. *Id.*

190. *Id.*

lated is expected to rise from 11,700 companies covered by the current rules to 50,000 companies under the CSRD.[191]

While the U.S. has rejoined the Paris Agreement under President Biden, the lack of federal legislation on climate change to drive policy forward has led to more narrow approaches like those of the SEC. On the other hand, the EU passed a climate change law that legally commits EU countries to meet the Paris Agreement climate reduction benchmarks.[192] This gives its regulatory bodies a legal mandate to try and get companies to commit to greater disclosure and transparency. "A big difference we are seeing with the proposed legislation is how narrow the US is being, with the EU being fairly technical."[193]

Both the US and EU have similar approaches to data protection and ESG reporting. Like the GDPR, the CSRD combines the enforcement of broad goals with the creation of fairness in the markets. The CSRD does so by protecting the environment and social goals and implementing rigorous reporting requirements. However, the US only took action after the EU. There is also a desire for narrower government intervention and more trust in the markets to provide necessary regulation.

There are certain elements common to the US and EU's approach to regulation that are present in the three previous areas. One of these is the level of government intervention in the markets, with the EU showing a stronger urge to intervene, while the US has a proclivity to trust the market for proper regulation. Another area is the potential imposition of costs that could stifle innovation. More generally, the EU is more cautious in approving emerging technologies and more willing to reject empirical data. This is enabled by the EU's desire to promote broad goals across the EU compared to the US where a showing of harm is usually required for government intervention. These differences have pushed US and EU law areas further apart and could do the same in the data protection realm.

IV. How Structural Differences Between the EU and the US Could Affect Federal Regulation

A. *Differences in Legislative Philosophy*

We should not expect a GDPR-style law in the United States due to differences in legislative processes and philosophies between the US and the EU governments. The enactment of federal legislation in the

191. Stehl, Ng & Feehily, *supra* note 177.
192. Lashitew, *supra* note 176.
193. *Id.*

US is more of an ad-hoc process than in the EU. Any member of Congress can introduce legislation and what they propose can be heavily influenced by lobbyists, campaign donors, and public interest groups. Unlike the EU, there is no requirement for a detailed analysis of the bill's impact and no requirement to consult with outside stakeholders. This results in the introduction of many bills, helping signify progress on an issue, but very few bills make it out of committee, and even fewer become law.[194]

The EU has a different system for enacting its regulations. Only the European Commission can propose legislation to Parliament and the Council. The Commission is staffed by Eurocentric bureaucrats whose job is to study and craft regulations for enactment across the entire EU. These regulations go through an arduous process, which includes a detailed description of the proposed legislation, extensive stakeholder consultation, and a full assessment of its impact by several EU regulatory bodies. Few regulations are proposed, but they have a broad scope and are likely to pass.[195]

The US legislative process's informal nature makes it more susceptible to hidden influences on laws that the public may not be aware of. Members of Congress need to be elected and then reelected and this requires extensive campaign support and contributions.[196] Consequently, those with the most influence tend to craft bills without consulting impacted stakeholders or the public.[197]

On the other hand, the European Commission is the only body that can introduce legislation, which means unelected bureaucrats who create regulations are required to go through mandatory consultations with impacted stakeholders.[198]The GDPR was the outcome of an almost decade-long effort and long-term study of the influence and impact the of EU's data privacy regulation. In contrast, the US introduced many bills over the years attempting to enact a nationwide data privacy regime, but none have embraced the need for a complete overhaul of data privacy. Instead, they have focused on regulating the current market. The GDPR was the brainchild of bureaucrats with a broad mandate from its members, whereas a US data privacy bill is more likely to be the result of tough compromises between the tech

194. Richard W. Parker & Alberto Alemanno, *A Comparative Overview of EU and US Legislative and Regulatory Systems: Implications for Domestic Governance & the Transatlantic Trade and Investment Partnership*, 22 Colum. J. Eur. L. 61, 70 (2015).

195. *Id*. at 68.

196. *Id*. at 90.

197. Reeve T. Bull, *Market Corrective Rulemaking: Drawing on EU Insights to Rationalize U.S. Regulation*, 67 Admin. L. Rev. 629, 657–58 (2015).

198. *Id.* at 68.

sector, data privacy interest groups, and their congressional allies. This does not signal legislation with the same scope as the GDPR.

Further, the discrepancy in expertise among legislators can be seen in the questions posed by Congress members during committee hearings with tech industry leaders. Many members displayed a complete lack of knowledge on some of the leading issues regarding data protection and privacy.[199] This lack of knowledge on crucial issues makes US politicians more susceptible to outside parties' arguments and influence.[200] Additionally, such lack of expertise among US politicians explains why the US has lagged behind the EU in the data protection realm.

Finally, it is important to reiterate the contrasting regulatory approaches of the EU and the US. The EU tends to use the precautionary principle, which prioritizes caution when regulating the market, as discussed above in their regulation of GMOs. On the other hand, the US uses a more balanced cost-benefit analysis to decide if the negatives outweigh the positives. The way the EU applies the precautionary principle signals that the US law won't venture to be as expansive as the GDPR.[201]

In terms of antitrust laws, US authorities are more likely to allow certain practices if they benefit consumers.[202] In doing so, they are more susceptible to arguments that consumers benefit from sharing their information, which is why the US may choose an opt-out approach rather than the opt-in consent that the EU requires. However, because data is valuable, there will likely be a balance struck between benefits to companies, benefits to consumers, and consumer data protections. This explains why the US and Europe have different approaches to consent– opt-in provides the assumption that data protection is a personal right, and third parties need to ask for permission, whereas opt-out lets the market run its course and protects consumers who may feel harmed.

B. *Political Influence*

While we have discussed the GDPR on the assumption that it is a stricter regulatory system than the US, it is important to acknowledge the impact of politics on both. The US is home to numerous technol-

199. Kassandra Polanco, *Trimming the Fat: The GDPR As A Model for Cleaning Up Our Data Usage*, 36 Touro L. Rev. 603, 605 (2020).

200. Araz Taeihagh, M Ramesh & Michael Howlett, *Assessing the Regulatory Challenges of Emerging Disruptive Technologies*, 15 Regul. & Governance 1009, 1010–1011 (2021).

201. Henson, *supra* note 173.

202. Firestone, *supra* note 170 at 32.

ogy companies that have brought the current focus on data privacy and protection. These companies are likely to exert pressure on US politicians to not adopt similar broad measures as the GDPR. While the US system is prone to political influence at the enactment stage, the EU is susceptible to political influence at the enforcement level.[203]

The nascent record of GDPR enforcement has shown that the breadth of the European laws may have less impact based on the DPA's different levels and styles of enforcement. Countries like Italy, Spain, and Romania have brought a high number of cases and levied a high number of fines, but these fines can be as low as 150 Euros, with enforcement decisions targeting even the smallest entities for lack of compliance.[204] On the other hand, countries like Ireland and Luxembourg have brought fewer enforcement actions but have imposed substantial fines. This is due to the presence of large American technology companies that benefit from their favorable tax regimes.[205]

Ireland has become a stumbling block for those hoping for a broad application like the GDPR in the US. It has had several decisions overturned by the EU after criticism from other countries' DPAs and public backlash. The Irish Data Protection Commission (DPC) discovered during an investigation that Meta had been careless in its handling of minors' information.[206] The original ranged from 30-50 million Euros, but after protests from multiple DPAs, the DPC was forced to reconsider and ended up levying a fine of 405 million Euros.[207]

In another case, the DPC investigated Meta for whether it violated GDPR consent requirements.[208] The DPC originally found that the

---

203. Katie Arcieri, *Big Tech Unlikely to Face Major US Legislation In 2023, But EU Threats Loom*, S&P Global Market Intelligence (Jan. 12, 2023), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/big-tech-unlikely-to-face-major-us-legislation-in-2023-but-eu-threats-loom-73689665; Ryan Browne, *How Ireland lost its chance to become Big Tech's 'super regulator,'* CNBC (May 4, 2022), https://www.cnbc.com/2022/05/04/how-ireland-lost-its-chance-to-become-big-techs-super-regulator.html.

204. Brian Daigle & Mahnaz Khan, *The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities*, 332 Journal of International Commerce and Economics 1, 8 (2020); https://www.usitc.gov/publications/332/journals/jice_gdpr_enforcement_0.pdf; CMS, GDPR Enforcement Tracker Report, https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/numbers-and-figures (last visited Apr. 1, 2023).

205. *Id.* at 21.

206. Press Release, Data Protection Commission, *Data Protection Commission announces decision in Instagram Inquiry*, (September 15, 2022), https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-instagram-inquiry.

207. *Id.*

208. Press Release, Data Protection Commission, *Data Protection Commission announces conclusion of two inquiries into Meta Ireland*, (January 4, 2023), https://dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland.

consent Meta obtained was lawful and did not levy any fines. However, after submitting its proposal, there was once again dissent from several other DPAs, and the European Data Protection Board (EDPB) ordered Ireland to reconsider.[209] As a result, the EDPB confirmed that Meta violated transparency and lawful consent regulations, leading the DPC to impose a 390 million Euro fine and a requirement for Meta to bring its data processing into compliance within three months.[210]

There are two ways to view these results. First, companies cannot locate themselves in the most business-friendly countries to escape enforcement of the GDPR. Second, the distributed enforcement system is flawed because of the disparity between what varying countries think is a fair fine. It is crucial for countries like Ireland to step up enforcement because the benefits that data provides to these companies, and the value these companies provide to countries like Ireland, must be balanced with individual privacy. Without proper oversight, enforcement of the GDPR could weaken over time.

C. *Differences in Regulatory Legal Cultures*

One of the main reasons we will not see GDPR-style regulation in the US is the different legal approaches to litigation. The US values the ability of markets to regulate behavior and individual autonomy over government mandates. In contrast, the EU prioritizes "social-protection norms."[211]

The US is likely to favor a system that gives parties the chance to enforce their rights through litigation, rather than government bureaucracy. The US legal system is set up this way, attorneys for private parties rather than judges or government regulators bring private claims, present evidence of violations and damages, and invocation new legal arguments to enforce rights.[212] Also, US law has more detailed statutes and regulations that employ specific legal procedures.[213]

This is in stark contrast to Europe's approach where legal decision-making relies on regulatory agencies and government bureaucracy, the statutes are broader, and regulation is worked out informally be-

209. *Id.*

210. *Id.*

211. Chander et. al., *supra* note 157, at 1762.

212. Robert A. Kagan, *American and European Ways of Law: Six Entrenched Differences, UC Berkeley: Institute of European Studies 1*, 5 (2006), https://escholarship.org/uc/item/3kt912b3.

213. *Id*. at 6.

tween parties and government bureaucrats.[214] Thus, it is not surprising that the language of the GDPR is vague and it is expected that regulators and parties will work together to form how the regime will govern. However, the US business community is more hostile to government intervention and thus less inclined to accept a strict regulatory system like the GDPR.[215] In short, the vague language and European approach to enforcement of the GDPR will not happen in the US.

V. WHAT WILL FEDERAL REGULATION OF DATA PRIVACY LOOK LIKE?

A. *Differences Between the Current Data Protection and Privacy Regimes*

The GDPR had an impact on how US jurisdictions have implemented their own data protection and privacy bills. Some of the groundbreaking features of the GDRP, such as the right to deletion, access, correct, and restriction have been incorporated in different states. However, despite these influences, no state has chosen to be as expansive as the GDPR. Controllers and processors are required to report more with the GDPR, which mandates the appointment of a DPO and the need to give greater information to data subjects and regulators.

The GDPR also treats data as a fundamental right while the US treats data as a consumer product. Accordingly, the GDPR regulates non-profits and government agencies as much as private entities because the damage resulting from their misuse is the same as a private company. Comparatively, US data laws regulate companies that are using data to make a profit, an important difference in scope.

Another important difference from the GDPR approach to data regulation is California's choice to use an opt-out system instead of an opt-in one. The right to opt-in gives the impression that the right must be given away by choice, not some information that consumers choose to protect. While Colorado and Virginia require opt-in for sensitive information, the choice not to extend this option to all information indicates how American authorities view the needed breadth of data protection.

Finally, it is worth noting that California was the first state to establish strong statutory data regulations and consumer protections, creating a template for other US states in terms of legislation. If a federal

214. *Id.*; Chander et al., *supra* note 157 at 1760.
215. *Id*. at 1787.

bill were to be passed, it seems unlikely that it would go further than the existing state bills unless there was a significant public outcry or shift in opinion. While there are variations in the bills, there are certain core elements that are consistent across all regulatory systems These elements are likely to remain in place, as the US tends to prioritize reducing the burden on businesses as discussed above. It is important to recognize that despite differences between bills, they all aim to strike a balance between the needs of businesses and consumers, rather than solely concentrating on compliance with a rights-based regime.

B. *Where We Are Heading*

The lack of uniformity in US data privacy and protection regulations has a negative impact on companies' innovation and profits, consumer knowledge and trust, and the government's ability to work efficiently. Although certain sectors such as finance and healthcare have data protection measures, other critical parts of the economy lack stability and the overall regime needs to be addressed.[216] Courts have struggled to apply the law to modern data practices and have precluded executive action from having any meaningful effect.[217] The courts specifically struggle with defining data as it is an intangible and highly elusive concept for courts to define yet has become a critical part of our lives.[218]

It is likely that federal preemption will replace the myriad of state laws due to the high costs businesses face in complying with similar but different laws and regulations from various states.[219] More states are passing laws relating to data protection and privacy with twenty-nine states considering over sixty bills on data regulation in 2022, compared to only two in 2017.[220] Businesses have complained that complying with different state laws will divert resources that can be better spent on innovation and growth.[221] They also fear that they may have to comply with fifty different state regulations if there is no federal

---

216. Kessler, *supra* note 5; Polanco, *supra* note 198.

217. Luis Miguel M. del Rosario, *On the Propertization of Data and the Harmonization Imperative*, 90 Fordham L. Rev. 1699, 1703 (2022).

218. *Id.;* Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186, 129 N.E.3d 1197

219. Alexander *supra* note 6, at 200–201.

220. *The Growth of State Privacy Legislation*, International Association of Privacy Professionals, https://iapp.org/, https://iapp.org/resources/article/the-growth-of-state-privacy-legislation-infographic/ (2022).

221. Jordan Yallen, *Untangling the Privacy Law Web: Why the California Consumer Privacy Act Furthers the Need for Federal Preemptive Legislation*, 53 Loy. L.A. L. Rev. 787, 788 (2020).

action.[222] Some businesses argue that consumers will be hurt because certain services may be prohibited in certain places, making certain products available to some consumers and not others.[223] Additionally, businesses believe they will face unclear and possibly devastating litigation costs as a result of these laws.[224] According to the California Attorney General's regulatory impact assessment report, the initial costs for CCPA compliance are projected to reach $55 billion.[225]

As a result of these fears, executives from Amazon, Apple, AT&T, Charter, Google, and Twitter have called on the federal government to take action regarding concerns over data regulation. They tout the benefits federal legislation would bring to businesses and consumers and have been especially focused on keeping a consumer's private right of action out of any federal legislation.[226] While big data companies provide adequate reasoning for the necessity of federal preemption, and many agree there needs to be some overriding federal legislation, the tech industry's proposed bill is likely to draw strong resistance from consumer advocacy and data privacy groups.[227] The enactment of the CCPA in California is an example of how grassroots movements can push legislators to act, despite resistance from the tech lobby. Currently, there is gridlock in Washington D.C. that benefits big technology companies, and without the threat of a grassroots referendum, it may take longer for Congress to act.[228]

The technology sector and data protection advocacy groups have different opinions on data privacy, and the political climate in Washington D.C. adds to the complexity. While the passing of the Utah data privacy bill shows an appetite amongst red states to protect personal information and data, it has a narrower scope, highlighting the gap between conservatives and liberals in their approaches to regulating data collection.

President Obama attempted to persuade Congress to pass a Consumer Privacy Bill of Rights but found little appetite among Democrats and stern opposition from Republicans.[229] The Republican Trump administration also showed no inclination to pass a GDPR-style law, and the current Biden administration has yet to gain suffi-

222. *Id.*
223. Alexander *supra* note 6 at 227
224. Polanco, *supra* note 198, at 619.
225. Kessler, *supra* note 5, at 120.
226. Edgerton, supra note 8.
227. Kessler, *supra* note 5, at 125–26.
228. Arcieri, *supra* note 202.
229. Alexander, *supra* note 6, at 239.

cient support for any privacy bill.[230] Congress is still debating whether there should be a private right of action for a data breach of consumers' information.[231]

Both parties will be concerned about how complying with data protection laws will affect small businesses and start-ups.[232] Consumers may also face negative impacts when they cannot receive the services they were offered due to a lack of data collection.[233] To prevent these effects on businesses, California has implemented a threshold amount of consumers that need to be in a relationship with the data collector.[234]

Some argue that the US should just choose to adopt the GDPR because it would benefit both businesses and consumers by providing uniform laws and established precedent from the EU. This approach provides "uniformity, adaptability, and accountability [that] balances the consumer-business relationship and creates a cohesive, enforceable law capable of handling technology's fluid landscape."[235]

Further, some companies may decide there are benefits to the adoption of GDPR standards such as the harmonization of products or the goodwill it may garner from the public. Apple CEO Tim Cook has supported the passage of the GDPR and has advocated for a US law that is similar in scope.[236] To this end, Apple has introduced policies and product features that allow users to see what data Apple is collecting from them and to request that the company delete it.[237] This suggests that even if the US does not enact a GDPR-style law, private companies may still comply with its regulation.

VI. Conclusion

In our current climate, American consumers are demanding more information and protection for their rights. As a result, they are seeking greater transparency and safeguards from companies. Meeting these expectations has become a challenge for businesses, particularly in light of increasing state regulations. Despite an initial fear that American data would be subject to GDPR-style regulations, the recent passage of the US state bills suggests that GDPR-style reforms

230. Kessler, *supra* note 5, at 123–24.
231. *Id.* at 125–126.
232. *Id.*
233. *Id.*
234. Cal. Civ. Code § 1798.140(d)(1).
235. Safari, *supra* note 14, at 825.
236. Chris Baraniuk, *Tim Cook Blasts 'Weaponization' of Personal Data and Praises GDPR*, BBC (Oct. 24, 2018), https://www.bbc.com/news/technology-45963935.
237. *Id.*

are likely to stay on the other side of the Atlantic. This is due, in large part, to the differences in implementation, enforcement, and political climate in the US.

The implementation of these two consumer data regulatory regimes plays a key role. The creation of the GDPR significantly enhanced consumer protection by introducing expansive data privacy rights and broad enforcement mechanisms. The rights of data subjects are accorded utmost priority, and while there may be some tradeoffs for data collectors, they are primarily responsible for bearing the costs associated with these rights. In contrast, the US has shown a preference for narrow and technically specific regulations through state data privacy bills to implement consumer protection measures. The uncoordinated and slow implementation of US laws resulted in some jurisdictions being more business-friendly than others.

Additionally, it is important to consider the notable differences in regulatory frameworks between the EU and the US, particularly in regard to antitrust measures, GMO regulations, and ESG disclosure policies. Even though both regions recognize the significance of regulation in these areas, there remains a significant disparity in the underlying approach to these regulations. However, these differences also provide an opportunity for both regions to learn from one another and potentially solve the same problem. The development of data privacy regulations is an example of this process. The US has a more relaxed stance towards businesses and narrower governmental enforcement, while the EU has a more rigid approach and more governmental influence. As both regions continue to advance and implement these regulations, they will likely learn from each other's successes and potentially replicate them.

Finally, the current political climate in the United States has a pronounced impact on consumer data protection. The recent passage of Utah's data privacy bill highlights a growing appetite amongst red states to protect personal information and data. However, the narrower scope of the bill indicates a difference in how far conservatives and liberals are willing to regulate data. Finding a compromise on this issue is imperative, but the current hyper-partisan climate in D.C. presents significant challenges. Unless another state adopts another GDPR-style regulatory system, it is unlikely that we will see any substantial departure from what states have passed so far.

It is hard to predict the future. Various factors contribute to it, such as technical advances we cannot account for, political change that will bear a strong influence on any regulation, and public opinion that is open to constant fluctuation. Nonetheless, in the interest of addressing

the conflicting legislation on data privacy and protection, federal protection is likely to come as the result of both the business and technology communities exerting pressure on the government to act. With time, lawmakers may also become more comfortable with the experience of states that have already passed legislation, increasing the probability of a federal bill being passed.