SMU | Dedman School of Law

SMU Law Review

Volume 77 | Issue 2 Article 10

2024

Growing Tensions: Consumer Privacy and Corporate Disclosures

Megan Wischmeier Shaner
University of Oklahoma

Growing Tensions: Consumer Privacy and Corporate Disclosures

*Megan Wischmeier Shaner**

ABSTRACT

Data privacy and data security have become key issues for legislators, regulators, and individual citizens. Roughly two-thirds of Americans believe their data is being regularly tracked, monitored, and collected by companies and the government. A majority of U.S. adults also believe their data is less secure today than five years ago, expressing concerns that they have little control over how their personal information is being used and that the entities who control their data are not responsible stewards. In the absence of comprehensive federal regulation, a continuous stream of privacy statutes have been proposed at the state level. Beginning with California in 2018, a handful of states enacted major comprehensive data privacy legislation. The number of states adopting consumer privacy laws has more than doubled in 2023 alone, and 2024 is on pace to exceed the prior year's adoption rate.

Data privacy legislation obligates businesses operating in those states to comply with additional regulations regarding the collection, use, and disclosure of personal information and provides "consumers" with new rights over their personal data. Broad in scope, these state privacy statutes apply to not only traditional consumers, but also shareholders and—in some states—employees, officers, and directors of a corporation. This article discusses the growing tensions between compliance with privacy statutes and corporate disclosure activities. In light of impending conflicts between these two areas of the law, this article proposes legislative and judicial paths for navigating and reconciling the competing legal obligations. As more and more states, as well as the federal government, are contemplating adopting consumer privacy statutes, consideration of the interplay and impact of privacy statutes on corporate actions is crucial.

DOI: https://doi.org/10.25172/smulr.77.2.9

* Kenneth E. McAfee Centennial Chair in Law, President's Associates Presidential Professor, University of Oklahoma College of Law. For helpful comments and discussions, sincere thanks go to Kara Bruce, Elisabeth de Fontenay, Geeyoung Min, and Alex Platt. I would also like to thank the participants in the Winter Deals Conference whose thoughtful comments and questions contributed to the completion of this paper. All errors and omissions are my own.

TABLE OF CONTENTS

INTRODUCTION

"THE twenty-first-century economy will be fueled by personal data."[1] The amount of data being generated around the world is growing exponentially.[2] A 2013 study reported that—primarily due to the expansive use of the Internet—ninety percent of the world's data had been generated in just the preceding two years.[3] And with "over 205,000 new gigabytes [being] created" every second (which is "the equivalent of 150 million books"), the amount of data now available eleven years after

1. Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, Council on Foreign Rels. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/N7PF-W4LB].

2. *See Data: A Small Four-Letter Word Which Has Grown Exponentially to Such a Big Value*, Deloitte (July 13, 2023) [hereinafter *Data: A Small Four-Letter Word*], https://www2.deloitte.com/cy/en/pages/technology/articles/data-grown-big-value.html [https://perma.cc/H3A3-K4F9] ("It's projected that by 2025 our global data volume will reach 175 zetabytes. To put this in physical terms, this translates to a stack of blu-ray discs that could reach the moon 23 times!"); Mwalimu Phiri, *Exponential Growth of Data*, Medium (Nov. 19, 2022), https://medium.com/@mwaliph/exponential-growth-of-data-2f53df89124 [https://perma.cc/RWN8-6PSR] ("The evolution of technology and its dominating impact in every aspect of life, is generating a vast amount of data at an incalculable pace."). For a discussion of what is "data," see Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. Rev. 423, 426–28 (2018) (discussing the information amassed from users accessing the Internet-of-things); Xuan-Thao N. Nguyen, *Collateralizing Privacy*, 78 Tul. L. Rev. 553, 564–67 (2004) (discussing the aggregation of consumer data into datasets and databases).

3. *See* SINTEF, *Big Data, for Better or Worse: 90% of World's Data Generated over Last Two Years*, Sci. Daily (May 22, 2013), https://www.sciencedaily.com/releases/2013/05/130522085217.htm [https://perma.cc/V3ZQ-46D6].

that study is vast.[4] Labeled the "new gold," information is being monitored, collected, and analyzed by public and private entities for its strategic and economic value.[5] In particular for Internet-based companies, consumer information and consumer databases are considered prized assets.[6] As former LinkedIn Chief Executive Officer Jeff Weiner summed up, "Data really powers everything that we do."[7]

The expansion in data creation and collection has led data privacy and data security to become topics of great interest and concern to legislators, regulators, and individual citizens.[8] There has been increased attention on how data is being collected and utilized, especially by technology companies and social media platforms.[9] A recent survey by the Pew Research Center found that roughly two-thirds of Americans believe their data is being regularly tracked, monitored, and collected by companies and the government.[10] At steadily increasing rates, Americans also express feeling that their data is less secure than it was in the past.[11] Powerless when it comes

4. Elvy, *supra* note 2, at 427; *see* Jeff Desjardins, *How Much Data Is Generated Each Day?*, World Econ. F. (Apr. 17, 2019), https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f [https://perma.cc/CYV5-LZU3] ("[T]he entire digital universe is expected to reach 44 zettabytes by 2020. If this number is correct, it will mean there are 40 times more bytes than there are stars in the observable universe.").

5. *See Data: A Small Four-Letter Word*, *supra* note 2; Robert Peck, *Mark Cuban: "Data Is the New Gold"*, Credit Suisse Grp. (June 22, 2017), https://www.credit-suisse.com/corporate/en/articles/news-and-expertise/mark-cuban-data-is-the-new-gold-201706.html [https://perma.cc/H2QN-38A9]; Julia Alpert Gladstone, *Data Mines and Battlefields: Looking at Financial Aggregators to Understand the Legal Boundaries and Ownership Rights in the Use of Personal Data*, 19 J. Marshall J. Comput. & Info. L. 313, 329 (2001) ("[C]onsumer profiles are a valuable intangible asset."); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056–57 (2004) ("The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from this trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information."); Maria Castañón Moats, Barbara Berlin & Joseph Nocera, *Trust, Risk, and Opportunity: Overseeing a Comprehensive Data and Privacy Strategy*, Harv. L. Sch. F. on Corp. Governance (Dec. 26, 2022) ("In today's world, data is power. The ability to collect and use vast amounts of data can give companies a competitive advantage.").

6. *See* Gladstone, *supra note 5, at* 329 (noting the "use of customer databases has become a critical strategy to successful business"); Xuan-Thao N. Nguyen, *Commercial Law Collides with Cyberspace: The Trouble with Perfection—Insecurity Interests in the New Corporate Asset*, 59 Wash. & Lee L. Rev. 37, 41–42 (2002) (noting that "due to the cyberspace nature" of Internet companies, their most important assets are intangibles).

7. Phiri, *supra* note 2.

8. *See* Lisa Hawke, *Data Privacy Day 2018: Data Breaches, Harm, and Culture*, Bloomberg L. (Jan. 29, 2018), https://news.bloomberglaw.com/legal-ops-and-tech/data-privacy-day-2018-daa-breaches-harm-and-culture [https://perma.cc/4ERS-YA4J].

9. *See id.*; Cesare Fracassi & William Magnuson, *Data Autonomy*, 74 Vand. L. Rev. 327, 329 (2021) ("Major newspapers have written exposés about the myriad ways in which technology companies are exploiting and monetizing our data.").

10. *See* Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Rsch. Ctr. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information [https://perma.cc/J3AU-G44G] (surveying a random sample of more than 10,000 Americans).

11. *Compare id.* (70% of U.S. adults reporting, in 2019, that they think their personal data is less secure than it was five years ago), *with* Kenneth Olmstead & Aaron Smith, *Americans and Cybersecurity*, Pew Rsch. Ctr. (Jan. 26, 2017), https://www.pewresearch.org/

to personally controlling and protecting their data, a large percentage of the public is concerned over how companies use the data they collect.[12] In fact, most Americans surveyed lack trust that the institutions collecting their personal data will keep it secure, refrain from misuse, admit mistakes, and take responsibility when the security of such data is compromised.[13]

Data breach scandals have contributed to a greater awareness of the volume of information collected as well as the security (or lack thereof) of such information.[14] Companies such as AT&T, Equifax, Facebook, Uber, Capital One, Yahoo, IBM, T-Mobile, and Twitter—among many others—have made headlines after large data breaches were reported or exposed.[15] Given the regularity of such breaches, it is no surprise that a majority of Americans have reported experiencing "some form of data theft," and "roughly three-in-ten Americans have experienced some kind of data breach in the past 12 months."[16] The vulnerability of consumers' personal information to financial crime and identity theft has made data privacy and

---

internet/2017/01/26/americans-and-cybersecurity/ [https://perma.cc/8JY6-KPWW] (49% of U.S. adults reporting, in 2017, that they "feel that their personal information is less secure then it was five years ago").

12. *See* Auxier et al., *supra* note 10, at 2 (finding that most Americans surveyed "feel they have little or no control over how these entities use their personal information"); *see also* S. Judiciary Comm., 115th Cong., Rep. on Internet Service Providers: Customer Privacy 1-2 (2018) [hereinafter Senate Judiciary Committee Report], https://digitalcommons.law.scu.edu/historical/1748 [https://perma.cc/8L4E-6GD3].

13. *See* Auxier et al., *supra* note 10, at 4 ("For example, 79% of Americans say they are not too or not at all confident that companies will admit mistakes and take responsibility if they misuse or compromise personal information, and 69% report having this same lack of confidence that firms will use their personal information in ways they will be comfortable with."); Olmstead & Smith, *supra* note 11, at 10 (many Americans "lack trust in key institutions—especially the federal government and social media sites—to protect their personal information").

14. *See, e.g.*, Joseph Damon, Jason Epstein & Amelia Lant, *The New California Consumer Privacy Act of 2018: A Practical Analysis*, JD Supra (July 9, 2018), https://www.jdsupra.com/legalnews/the-new-california-consumer-privacy-act-33874 [https://perma.cc/9UA4-NVHB]; Heather Kelly, *California Passes Strictest Online Privacy Law in the Country*, CNN (June 29, 2018), https://money.cnn.com/2018/06/28/technology/california-consumer-privacy-act/index.html [https://perma.cc/DE39-XJY4]; Allison Grande, *Google Data Leak Exposes Breach Disclosure Conundrums*, Law360 (Oct. 12, 2018), https://www.law360.com/articles/1091877/google-data-leak-exposes-breach-disclosure-conundrums [https://perma.cc/9UA4-NVHB].

15. *See* Shira Ovide, *Hackers stole almost everyone's AT&T phone records. What should you do?*, Wash. Post (July 12, 2024), https://www.washingtonpost.com/technology/2024/07/12/att-data-breach-hack-calls-texts-what-do/; Nicole Hong, Liz Hoffman & AnnaMaria Andriotis, *Capital One Reports Data Breach Affecting 100 Million Customers, Applicants*, Wall St. J. (July 30, 2019), https://www.wsj.com/articles/capital-one-reports-data-breach-11564443355 [https://perma.cc/4PFZ-JZ5F]; Keman Huang, Xiaoqing Wang, William Wei & Stuart Madnick, *The Devastating Business Impacts of Cyber Breach*, Harv. Bus. Rev. (May 4, 2023), https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach [https://perma.cc/5KJA-KZXL]; Lee Mathews, *Equifax Data Breach Impacts 143 Million Americans*, Forbes (Sept. 7, 2017), https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/amp/ [https://perma.cc/5FH5-DNNW]; Kate Conger & Kevin Roose, *Uber Investigating Breach of Its Computer Systems*, N.Y. Times (Sept. 15, 2022), https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html; Aaron Drapkin, *Data Breaches That Have Happened in 2022, 2023, and 2024 So Far*, Tech.co (Feb. 19, 2024), https://tech.co/news/data-breaches-updated-list [https://perma.cc/6JQS-YP4J]; *see also* Auxier et al., *supra* note 10.

16. *See* Auxier et al., *supra* note 10, at 18; Olmstead & Smith, *supra* note 11, at 2 (reporting that "[a] majority of Americans (64%) have personally experienced a major data breach").

security an issue on the forefront of legislative activity.[17] In his 2023 State of the Union Address, President Joseph R. Biden, Jr. renewed calls for federal lawmakers to pass legislation addressing companies' ability to collect, use, and share consumers' personal data.[18]

Privacy and data security issues affect virtually every company across all industries around the world.[19] Unlike other Western countries, however, the United States has failed to adopt a comprehensive data privacy framework. Currently, the U.S. relies on a patchwork of sector-based laws and regulations that protect certain categories of information.[20] These include laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), the Driver's Privacy Protection Act (DPPA), the Children's Online Privacy Protection Act (COPPA), and the Family Educational Rights and Privacy Act of 1974 (FERPA).[21] While there is strong interest within Congress to address the exponential increase of personal data being collected by companies and the mounting data privacy issues, partisan differences on key issues have, to date, prevented any significant progress on a comprehensive federal law in this space.[22] In the absence of federal action and following the European Union's adoption of its own comprehensive privacy regulations—the General Data Protection Regulation (GDPR)[23]—states have rushed to fill the void through adoption of their own comprehensive data privacy laws.[24]

---

17. *See* Hawke, *supra* note 8; O'Connor, *supra* note 1 (discussing the data breaches at Equifax, Yahoo, Deep Root Analytics, and Uber).

18. Allison Grande, *Biden Pushes for Targeted Ad Ban, Tighter Data Privacy Rules*, Law360 (Feb. 7, 2023), https://www.law360.com/corporate/articles/1573751 [https://perma.cc/E6ZD-C5U7] (quoting President Biden's speech: "[And] it's time to pass bipartisan legislation to stop Big Tech from collecting personal data on our kids and teenagers online, ban targeted advertising to children, and impose stricter limits on the personal data that companies collect on all of us.").

19. *See* Hawke, *supra* note 8.

20. *See* Mary D. Fan, *The Right to Benefit from Big Data as a Public Resource*, 96 N.Y.U. L. Rev. 1438, 1454–55 (2021).

21. *See* Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 Fla. L. Rev. 365, 409 n.250, 413–15, 424 (2019).

22. *See* Fan, *supra* note 20, at 1459; Jason Hirsch, *A New Digital Age: Why COVID-19 Necessitates Preemptive Federal Action to Regulate Data Privacy*, 94 Temp. L. Rev. Online 1, 2 (2022).

23. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Council Directive 95/46/EC, 2016 O.J. (L 119) [hereinafter GDPR], eur-lex.europa.eu/eli/reg/2016/679/oj [https://perma.cc/4A6C-NFLP].

24. This paper is using the definition of "comprehensive data privacy laws" or "comprehensive state privacy laws" frequently used in other academic and practitioner writing on the subject:

> [S]tate data privacy regulations governing the rights of consumers and imposing obligations on covered entities. These regulations generally apply only to non-governmental organizations meeting certain thresholds. They commonly exclude employment-related data (except in California) and provide exemptions, such as for non-profits or certain regulated industries subject to other regulations like the GLBA and HIPAA.

Ctr. for Info. Pol'y Leadership, Hunton Andrews Kurth, Comparison of U.S. State Privacy Laws: Data Protection Assessments 2 n.3 (Feb. 8, 2024), https://www.

California led the way at the state level in regulating data privacy and security.[25] In 2018, it adopted the most comprehensive and sweeping privacy law in the United States—the California Consumer Protection Act of 2018 (CCPA).[26] In a manner similar to the GDPR, the CCPA establishes new data rights for "consumers" as well as responsibilities for "businesses" that are controllers or processers of personal data.[27] Virginia and Colorado followed California's lead and enacted their privacy statutes in 2021, with Utah and Connecticut not far behind in 2022.[28] These four states' statutes all went into effect during 2023.[29] 2023 also brought a flurry of new states adopting privacy legislation.[30] Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, and Texas all adopted comprehensive consumer privacy laws, more than doubling the number of states with such regulations.[31] And adoptions have continued apace with seven states adopting privacy statutes in just the first half of 2024 and several others considering proposed legislation on the topic.[32]

While all the state privacy statutes adopted to date are based on the same foundational principals as California's CCPA, each one is slightly different from the others.[33] There are, however, clear patterns beginning to emerge in how state legislatures are approaching general privacy protection. Nevertheless, these differences indicate that there is no clear consensus yet on a standard approach to regulating and protecting consumer data.

All of the state privacy statutes are similar in the wide-ranging protections they afford.[34] The breadth of these statutes means that they can cover individuals well beyond the traditional, individual consumers envisaged as needing protection. In California (the most far-reaching of the statutes),

---

informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comparison_us_state_privacy_laws_dpa_feb14.pdf. [https://perma.cc/NFP7-GYUJ]. It should be noted that this paper focuses on data *privacy* statutes, which are to be distinguished from data *breach* statutes. Forty-eight states have passed data breach laws which require entities to notify individuals if their information is compromised. *See* O'Connor, *supra* note 1.

25. *See* O'Connor, *supra* note 1.

26. *See* Fan, *supra* note 20, at 1459 ("California's recent law remains the most sweeping American effort to protect consumer data privacy.").

27. *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199.100.

28. *See* discussion *infra* Part I.B.2–3.

29. *See* discussion *infra* Part I.B.3.

30. *See* discussion *infra* Part I.B.4.

31. *See* discussion *infra* Part I.B.4. It should be noted that Florida is not always included in the list of states adopting comprehensive data privacy statutes. The state's statutory provisions include numerous exceptions and unique thresholds resulting in only a limited set of entities such as largest tech giants like Amazon.com, Inc. and Alphabet Inc. being subject to its requirements. *See infra* note 175 and accompanying text. Additionally, consistent with other writing on state consumer privacy laws, this article excludes Washington state's My Health, My Data Act from its discussion. Washington's statute is generally excluded as it is a narrower privacy law that targets the regulation of only health data and not consumer information more broadly. *See* Amy Olivero & Anokhy Desai, *Washington's My Health, My Data Act*, INT'L ASS'N PRIV. PROS. (Apr. 2023), https://iapp.org/resources/article/washington-my-health-my-data-act-overview/ [https://perma.cc/4RV8-RD37] (discussing Washington's health privacy law).

32. *See infra* Part I.B.4. The 2024 adopters include Kentucky, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey, and Rhode Island.

33. *Id.*

34. *See infra* Part I.B.

employees, directors, and officers of a business are all included under the sweeping definition of "consumer."[35] In addition, under the overwhelming majority of the existing state statutes, shareholders would likewise fall within the statutes' definitions of "consumer."[36] As a result, most current state privacy laws require covered businesses to provide notice to shareholders of their data processing practices and will require these businesses to respond to consumer rights requests from these individuals.[37]

Beyond the notice and disclosure obligations, state privacy statutes will also have a broader impact on how corporations operate. The GDPR, which has been in effect longer than any of the state statutes, is already having such an effect. For example, New York federal courts have had to consider the burdens the GDPR's requirements impose upon the civil discovery process.[38] In addition, a German court had to consider whether disclosure by a company of information identifying one of its shareholders to another of that company's shareholders was prohibited by the GDPR.[39] It is only a matter of time before the courts will have to wrestle with the impact of U.S. state privacy statutes on corporations' activities. Accordingly, this paper analyzes the different points of tension between the state privacy statutes' obligations and corporate governance activities. The goal of such analysis is to (i) provide a roadmap for states with privacy statutes on how these tensions should be analyzed and resolved when they arise as well as (ii) highlight points of tension that can be avoided in the drafting of such statutes which would benefit both state legislatures that are currently considering adopting privacy statutes and any future comprehensive federal privacy laws.

Considering the interplay of privacy statutes and corporate activities is vital at this juncture in the development of U.S. privacy law. In addition to the twenty states that have thus far enacted privacy legislation, as of July 1, 2024, there are six other states currently considering bills for the 2024 legislative session.[40] Commentators predict this is the beginning of a wave of privacy legislation, with other states following in the footsteps of these initial

35. Cal. Civ. Code §§ 1798.100–1798.199.100.

36. *See infra* Part II.

37. *See, e.g.*, Cal. Civ. Code §§ 1798.100–1798.199.100.

38. *See In re* Hansainvest Hanseatische Inv.–GmbH, 364 F. Supp. 3d 243, 252 (S.D.N.Y. 2018) (conditionally granting an application for serving subpoenas made under 28 U.S.C. § 1782 for GDPR-protected custodians only insofar as applicants would, among other things, assume the costs of GDPR compliance during production and indemnify respondents against any liabilities arising from violating European privacy laws or regulations); Pearlstein v. BlackBerry Ltd., 332 F.R.D. 117, 122 (S.D.N.Y.) (declining to compel production of a potential witness's home address in a GDPR-protected country where the witness has not consented to the address's production), *reconsideration denied in part and granted in part*, 2019 WL 5287931 (Sept. 20, 2019).

39. *See* Odia Kagan, *German Court Rules Company Can Disclose Shareholder Information to Other Shareholders*, Fox Rothschild (Sept. 23, 2019), https://dataprivacy.foxrothschild.com/2019/09/articles/european-union/gdpr/german-court-rules-company-can-disclose-shareholder-information-to-other-shareholders/# [https://perma.cc/BDQ5-DNUF].

40. *See infra* note 80 and accompanying text (discussing legislative activity across the states). There are also nine states with privacy bills that are currently inactive—Georgia, Hawaii, Louisiana, Maine, Missouri, New York, Vermont, West Virginia, and Wisconsin.

adopters. As more and more states adopt their own legislation, their decisions will create compliance obstacles where different requirements conflict or are inconsistent.[41] As one commentator has cautioned: "Each state's unique privacy laws complicate the patchwork of laws with which entities must comply. Critics of this state-by-state approach express concerns related to the significant compliance costs companies would incur to properly navigate numerous unique data privacy laws."[42] Moreover, as more and more states pass individual privacy statutes, it will put continued pressure on Congress to act and pass federal privacy regulation. In light of follow-on legislation in other states and the potential for preemptive federal legislation, identifying and correcting where privacy obligations and corporate governance activities conflict and are potentially irreconcilable is crucial.

This paper proceeds as follows. Part I discusses the state of data privacy regulation in Europe and the United States. It first provides an overview of the European Union's GDPR— a sweeping comprehensive data protection regime that has served as the backdrop and basis for state privacy statutes. Part I also describes the statutory framework set forth in each of the five states that were in the first wave of privacy statutes: California, Virginia, Connecticut, Colorado, and Utah. A summary and comparison of the most recent second wave of privacy statutes then follows. This discussion highlights the similarities and differences among these statutes as well as the patterns emerging in how state legislatures are approaching the regulation of data. Part II discusses the application of state privacy statutes to corporate actors and activities such as annual shareholders meetings and books and records inspection rights. This Part analyzes the impact state privacy laws will have on different corporate activities and compliance with corporate codes. Finally, Part III sets forth ex-ante and ex-post solutions for addressing the tensions in simultaneous, yet at times conflicting, compliance with state privacy laws and corporate laws and norms. This Part first provides a legislative remedy for state and federal legislatures considering adopting data privacy statutes so as to avoid a conflict with corporate disclosure requirements. Then, it provides a framework for courts to use in analyzing the conflict between already adopted state privacy rules and corporate disclosure obligations. This framework of analysis maintains the policy goals underlying each area of the law as well as the reasonable expectations of participants in the corporate enterprise.

I. DATA PRIVACY LEGISLATION

At present, the U.S. lacks a comprehensive data privacy framework to govern the collection and privacy of individuals' data.[43] The overall approach of early U.S. privacy laws focused on (i) specific industries

41. Hirsch, *supra* note 22, at 12.

42. *Id.*; *see also* CTR. FOR INFO. POL'Y LEADERSHIP, *supra* note 24, at 1 ("The ever-growing number of privacy laws enacted by state legislatures and the lack of a uniform federal standard have left organizations in the United States wrestling with inconsistent legal obligations regarding the collection and use of personal data.").

43. Fan, *supra* note 20, at 1454–55.

(e.g., health care, banking, and education); (ii) specific practices (e.g., telemarketing); or (iii) specific types of data (e.g., biometrics, facial recognition, and genetic information).[44] At the federal level, these laws include the Health Insurance Portability and Accountability Act of 1996, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Driver's Privacy Protection Act, the Children's Online Privacy Protection Act, and the Family Educational Rights and Privacy Act of 1974.[45] State law further adds to this mix, most prominently in the form of data breach laws.[46] These state statutes require private businesses and government entities to notify individuals in the event of a security breach involving personally identifiable information.[47] Data breach notification statutes vary in meaningful ways from state to state, and states are continually amending their provisions in divergent ways, creating challenges for organizations in complying with a wide range of requirements.[48] This "piecemeal patchwork" of federal and state laws has been critiqued as confusing, at times contradictory, and overall failing to adequately protect Americans' data.[49] Not surprisingly, data privacy regulation in the U.S. has been described as the "Wild West."[50]

Existing efforts to enact federal comprehensive data privacy regulations have thus far failed.[51] While there is strong interest within Congress to enact federal law in this area, there is also strong partisan disagreement regarding key components.[52] As a result, every bill introduced in Congress has failed to make significant progress toward passage.[53] The European Union, by contrast, enacted comprehensive privacy regulations in the GDPR,

44. Kirk J. Nahra, *Why the National Debate on Privacy Law Matters to Business Lawyers*, A.B.A. (May 3, 2022), https://www.americanbar.org/groups/business_law/resources/business-law-today/2022-may/why-the-national-debate-on-privacy-law-matters/ [https://perma.cc/233E-7GCV].

45. Rustad & Koenig, *supra* note 21, at 409 n. 250, 413–15, 424.

46. O'Connor, *supra* note 1.

47. *See Security Breach Notification Laws*, Nat'l Conf. State Legislatures (Jan. 17, 2022), https://www.ncsl.org/technology-and-communication/security-breach-notification-laws [https://perma.cc/D5MM-GVZK].

48. *See* Jennifer J. Hennessy, Chanley T. Howell, Jennifer L. Urban, Steven M. Millendorf, Aaron K. Tantleff & Samuel D. Goldstick, *State Data Breach Notification Laws*, Foley & Lardner LLP (Dec. 1, 2023), https://www.foley.com/en/insights/publications/2019/01/state-data-breach-notification-laws [https://perma.cc/AFW9-7XRN].

49. *See* Jennifer Huddleston, *Preserving Permissionless Innovation in Federal Data Privacy Policy*, 22 J. Internet L. 17, 18, 21 (2019); O'Connor, *supra* note 1.

50. *See* Huddleston, *supra* note 49, at 18.

51. *See* Joe Duball, *American Privacy Rights Act Markup Canceled, Next US House Steps Uncertain*, Int'l Ass'n Priv. Pros. (June 27, 2024), https://iapp.org/news/a/american-privacy-rights-act-markup-canceled-next-us-house-steps-uncertain [https://perma.cc/2AGJ-L73D]; Hirsch, *supra* note 22, at 12.

52. *See* Hirsch, *supra* note 22, at 12 ("While there is bipartisan support in Congress for a federal data privacy law, three issues have frustrated efforts to pass legislation: (1) whether state privacy laws should be expressly preempted, (2) whether to include a private right of action for consumers, and (3) whether the Federal Trade Commission (FTC) should be the federal agency that enforces corporate compliance practices."); Fan, *supra* note 20, at 1459 (describing how "there is strong interest within Congress to address these concerns, but a lack of consensus on how to resolve key issues"); David McCabe, *Congress and Trump Agreed They Want a National Privacy Law. It is Nowhere in Sight*, N.Y. Times (Oct. 1, 2019), https://www.nytimes.com/2019/10/01/technology/national-privacy-law.html [https://perma.cc/5SJ9-DNF5] (describing talks of a federal data privacy law).

53. *See* Fan, *supra* note 20, at 1459.

which became effective in May 2018.[54] In response to the GDPR, and in the absence of a U.S. federal solution, many states began to design their own data privacy laws.[55] This Section discusses the current state of privacy law in the United States. It begins with a brief overview of the European Union's GDPR, since U.S. state laws have used the GDPR's framework as the foundation for their statutes.

A. European Union's General Data Protection Regulation

Concern over the control, access, and use of personal data is not unique to the United States. Indeed, it is an issue of global concern.[56] The European Union (EU) was an early mover in the international community on this issue. After years of intense negotiation and thousands of proposed amendments, the General Data Protection Regulation was finalized in April 2016 and went into effect on May 25, 2018.[57] Unlike the sectoral approach to data privacy taken by the U.S., the GDPR is a sweeping omnibus data protection regime that provides harmonization of data protection and privacy across all EU Member States.[58] Described as an "unprecedented leap in data privacy law," the GDPR employs broad definitions of "personal data" and "processing," applies to entities of all sizes that process personal data, provides consumers with new rights, expands jurisdictional reach to non-European companies, and imposes large penalties for violations.[59]

The GDPR is based on a notice-and-choice model.[60] Accordingly, the GDPR's provisions focus on five main objectives:

> (1) requiring companies to write clear and straightforward privacy policies; (2) requiring companies to receive affirmative consent from customers before the company can utilize the customer's data; (3) encouraging companies to increase transparency in how and why user data is transferred, processed, and used in automated decisions; (4) providing data subjects more rights over their data; and (5) granting the European Data Protection Board strong enforcement authority.[61]

---

54. GDPR, *supra* note 23.

55. *See* Ctr. for Info. Pol'y Leadership, *supra* note 24.

56. *See* Fan, *supra* note 20, at 1447 ("Consumers in the United Kingdom, Germany, and India—who, along with Americans, represent the largest portion of online users—have similarly widespread concern over how companies use their data, according to a 2014 survey."); Rustad & Koenig, *supra* note 21, at 441–48 (discussing privacy laws around the world).

57. *See* Rustad & Koenig, *supra* note 21, at 369–70; Julia Powles, *The G.D.P.R., Europe's New Privacy Law, and the Future of the Global Data Economy*, New Yorker (May 25, 2018), https://www.newyorker.com/tech/annals-of-technology/the-gdpr-europes-new-privacy-law-and-the-future-of-the-global-data-economy [https://perma.cc/54GL-9LH9]; GDPR, *supra* note 23, at para. 6.

58. *See* European Commission Memorandum, Questions and Answers—General Data Protection Regulation (Jan. 24, 2018), https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387 [https://perma.cc/N67J-RE4T]; Rustad & Koenig, *supra* note 21, at 379 ("The GDPR provides for both greater centralization of data protection enforcement and a 'consistency mechanism.'").

59. Elizabeth L. Feld, *United States Data Privacy Law: The Domino Effect After the GDPR*, 24 N.C. Banking Inst. 481, 489, 491 (2020); *see* European Commission Memorandum, *supra* note 58; GDPR, *supra* note 23, at art. 7, 15, 17.

60. *See* Elvy, *supra* note 2, at 475.

61. Feld, *supra* note 59, at 481–82.

The regulations apply to any entity involved in the processing of personal data of individuals located in the EU.[62] The GDPR employs a broad definition of "personal data"—"any information relating to an identified or identifiable natural person"[63]—reaching broader than U.S laws that focus their protection on discrete categories of information.[64] It similarly defines "processing" broadly to include "any operation or set of operations which is performed on personal data or on sets of personal data."[65] As a result, the GDPR applies to a wide range of data types and a wide variety of data usages.[66] The GDPR then divides entities involved in processing personal data into two categories: "controllers" and "processors."[67] The GDPR imposes obligations on controllers and processors of EU personal data, including: strict data processing requirements, data breach notifications, adoption of data security measures, data minimization, and implementation of governance measures to ensure accountability.[68] In addition, the GDPR provides for expanded individual rights with respect to personal data.[69] These include: the right to be forgotten, the right to object to certain uses of data, the right to rectify incorrect data, the right of portability, the right of access, and the right to be notified of a data breach.[70] "The rights and obligations in the GDPR are [then] backed by potentially substantial legal sanctions, including potentially hefty fines. [In addition,] [d]ata users also may sue for damages."[71]

Given its extraterritorial reach and potential threat of large sanctions, "[t]he GDPR has been influential in setting standards for data protection beyond its territorial scope, as companies streamline operations across borders and nations wishing to do business in Europe adopt equivalent protections."[72] Examples of countries that have seen this effect include

62. *See* Caroline Krass, Alexander H. Southwell, Ahmed Baladi, Emanuelle Bartoli, James A. Cox, Michael Walther, Ryan T. Bergsieker & Jason N. Kleinwaks, *The General Data Protection Regulation: A Primer for U.S.-Based Organizations that Handle EU Personal Data*, Gibson Dunn (Dec. 4, 2017), https://www.gibsondunn.com/the-general-data-protection-regulation-a-primer-for-u-s-based-organizations-that-handle-eu-personal-data/ [https://perma.cc/P68Y-BBX3].

63. GDPR, *supra* note 23, at art. 4(1).

64. *See* Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 Denv. L. Rev. 93,114–16 (2020).

65. GDPR, *supra* note 23, at art. 4(1).

66. Krass et al., *supra* note 62.

67. *See id.* A "controller" "determines the purposes and means of the processing of personal data." GDPR, *supra* note 23, at art. 4(7). A "processor" "processes personal data on behalf of the controller." GDPR, *supra* note 23, at art. 4(8).

68. *See* Krass et al., *supra* note 62; Sarah Shyy, *The GDPR's Lose-Lose Dilemma: Minimal Benefits to Data Privacy & Significant Burdens on Business*, 20 U.C. Davis Bus. L.J. 137, 150–55 (2020); *see also* Fan, *supra* note 20, at 1448 ("The GDPR also requires data 'controller[s]' to implement 'data protection by design and by default,' secure and protect data, and conduct 'data protection impact assessment[s],' among other obligations."); Jones & Kaminski, *supra* note 64, at 115–16.

69. *Id.* at 116.

70. *See* Rustad & Koenig, *supra* note 21, at 377.

71. Fan, *supra* note 20, at 1452.

72. *Id.* at 1454 ; *see also* Jones & Kaminski, *supra* note 64, at 112 ("The GDPR is on the radar of many American companies because of the breadth of what it covers, its extraterritorial reach, and its potential threat of large fines.").

Canada, Israel, and Japan, which have created privacy regimes compatible with the GDPR.[73] Most recently, China finalized its Measures on the Standard Contract for Outbound Cross-Border Transfer of Personal Information, restricting the transfer of personal information out of China.[74] In the U.S., "[t]he GDPR has triggered a domino effect of U.S. state legislatures enacting consumer protection and data laws."[75] As discussed below, while not as broad as the GDPR, these states' laws parallel the GDPR both in the rights they provide to individual consumers and the obligations they impose on businesses that handle personal information.

B. U.S. State Law

Following the EU's adoption of the GDPR, the trend of enacting comprehensive federal privacy laws in the United States initially appeared to be gaining momentum.[76] To date, however, such efforts have stalled.[77] In the absence of federal privacy protection, there has been a growing movement at the state level. As of July 2024, twenty states[78]—California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia—have enacted legislation to address data privacy requirements.[79] Six additional states have

73. *See* O'Connor, *supra* note 1.

74. *See* Lisa M. Ropple, Elizabeth Cole, Oliver Haas, Lilian He, Jork Hladjk, Jerry C. Ling & Undine von Diemar, *China Finalizes Measures on the Standard Contract for Cross-Border Transfers of Personal Information*, Jones Day (Mar. 2023), https://www.jonesday.com/en/insights/2023/03/china-finalizes-measures-on-the-standard-contract-for-crossborder-transfers-of-personal-information [https://perma.cc/3DE2-75GB]. The Measures on the Standard Contract for Outbound Cross-Border Transfer of Personal Information are part of China's Personal Information Protection Law which was adopted in 2021. Ting Zheng & Ziyan "Frank" Xue, *Cross-Border Data Transfers Under China's Personal Information Protection Law*, Nat'l L. Rev. (June 1, 2023), https://www.natlawreview.com/article/cross-border-data-transfers-under-china-s-personal-information-protection-law [https://perma.cc/ZX9J-Z546].

75. Feld, *supra* note 59, at 489; *see generally* Steven W. Stone & Gregory T. Parks, *GDPR's New Requirements: What Investment Managers, Funds, Banks, and Broker–Dealers Need to Know*, Morgan Lewis (Apr. 17, 2018), https://www.morganlewis.com/pubs/2018/04/gdprs-new-requirements-what-investment-managers#:~:text=Investment%20managers%2C%20funds%2C%20banks%2C%20and%20broker%2Ddealers%20will,similar%20anti%2Dmoney%20laundering%20requirements [https://perma.cc/95AG-HTCG].

76. Fan, *supra* note 20, at 1459.

77. *See id.* at 1460 (2021) (describing the stalled efforts to enact privacy legislation at the federal level); Duball, *supra* note 51. For more information on the progress of different efforts to enact privacy legislation at the federal level, see Müge Fazlioglu, *US Federal Privacy Legislation Tracker*, Int'l Ass'n Priv. Pros. (Mar. 2024), https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/ [https://perma.cc/2PJ9-QFXS].

78. Some sources do not include Florida as having enacted comprehensive privacy laws as the statute has many carve-outs resulting in significantly more limited applicability then the other states that have adopted such statutes. Andrew Folks, *Defining "Comprehensive": Florida, Washington and the scope of state tracking*, Int'l Ass'n Priv. Pros. (Feb. 22, 2024), https://iapp.org/news/a/defining-comprehensive-florida-washington-and-the-scope-of-state-tracking/ [https://perma.cc/DTU4-NA3U].

79. Andrew Folks, *US State Privacy Legislation Tracker*, Int'l Ass'n Priv. Pros. (May 6, 2024), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/98CY-RCY9].

privacy statutes under consideration in 2024.[80] Commentators predict this to be the beginning of a wave of privacy legislation, with other states following in the footsteps of these initial adopters.[81] Illustrating the rapid momentum in this area, in 2023, fifty-nine comprehensive consumer privacy bills were considered, a 103% increase from the twenty-nine bills considered in 2021.[82] In addition, between 2018 and 2022, thirty-nine different states had considered comprehensive consumer privacy laws in at least one instance, with many states considering the issue multiple times.[83]

Privacy legislation at the state level raises challenges for businesses in their attempts to comply with the rapidly expanding array of state laws. Attorneys and commentators have cautioned that to the extent future privacy laws deviate significantly from the initial five state privacy laws that went into effect in 2023, entities that operate at a national level will face mounting compliance challenges.[84] This Section analyzes the twenty state privacy statutes enacted to date. California, a leader in consumer protection legislation, was the first mover in this space, adopting its privacy legislation in 2018.[85] Virginia and Colorado enacted their privacy statutes in 2021,[86] with Utah and Connecticut not far behind in 2022.[87] An "unprecedented" wave of privacy statutes occurred in 2023, with eight new states adopting comprehensive privacy laws and many more still

80. The U.S. State Privacy Legislation Tracker, which is maintained by the International Association of Privacy Professionals, lists six states as having privacy legislation introduced thus far in 2024: Illinois, Massachusetts, Michigan, North Carolina, Ohio, and Pennsylvania. *US State Privacy Legislation Tracker 2024: Comprehensive Consumer Privacy Bills*, Int'l Ass'n Priv. Pros., https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf [https://perma.cc/TLW5-Z9MP]; *see also* Brenna Goth & Skye Witley, *Data Privacy 'Panoply' Looms as States Move to Fill Federal Hole*, Bloomberg L. (Jan. 19, 2023), https://news.bloomberglaw.com/privacy-and-data-security/data-privacy-panoply-looms-as-states-move-to-fill-federal-hole# [https://perma.cc/2WXD-KUNC] (listing the following states as having introduced privacy statutes for consideration in 2023: Iowa, Kentucky, Mississippi, New Jersey, New York, Oklahoma, Oregon, and Tennessee). Many other states have, in prior years, considered privacy statutes but to date have not adopted anything.

81. *See* Summer Kim, *Consumer Primacy: A Dynamic Model of Corporate Governance for Consumer-Centric Businesses*, 2022 Utah L. Rev. 235, 281–83 (2022) (describing California's privacy statutes as having a "contagion effect" and spurring other states to follow suit in adopting such legislation); Mark E. Schreiber, *Washington State Takes the Lead in CCPA Copycat Legislation Race, Trends Emerge*, McDermott Will & Emery (Mar. 4, 2020), https://www.mwe.com/insights/washington-state-takes-the-lead-in-ccpa-copycat-legislation-race-trends-emerge/ [https://perma.cc/FBL6-HUFX] (noting that "copycat" legislation of California's Consumer Privacy Act has been introduced across the United States at a "dizzying pace").

82. *See IAPP US State Comprehensive Privacy Laws Report*, Int'l Ass'n Priv. Pros. (Jan. 2024), https://iapp.org/media/pdf/resource_center/us_state_privacy_laws_report_2024_overview.pdf [https://perma.cc/UY3L-VN5X].

83. *Id.*

84. *See* Goth & Witley, *supra* note 80 ("The growing number of comprehensive and increasingly specific privacy bills in state legislatures carry the potential of new compliance and liability risks, attorneys said.").

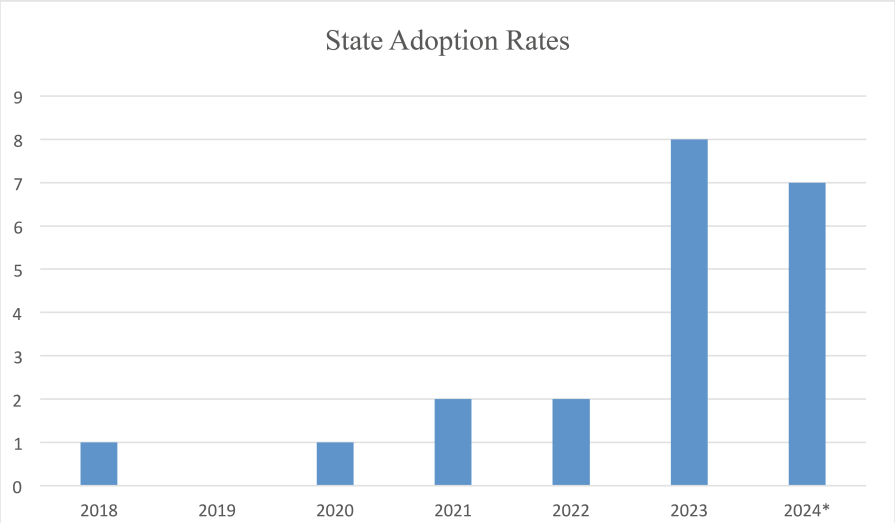
85. *See* California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100–.198. California was similarly a leader in adopting a data breach notification statute, with its adoption in 2003. *See* O'Connor, *supra* note 1.

86. *See* Consumer Data Protection Act, Va. Code Ann. §§ 59.1-571 to -581 (2021); Colorado Privacy Act, Colo. Rev. Stat. §§ 6-1-1301 to -1313 (2021).

87. *See* Conn. Gen. Stat. Ann. § 42-515 (West 2022); Consumer Privacy Act, Utah Code Ann. §§ 13-61-101 to -404 (West 2022).

considering proposed privacy legislation.[88] Thus far in 2024, seven more states—Kentucky, Maryland, Minnesota, Nebraska, New Jersey, New Hampshire, and Rhode Island—have enacted statutes.[89] Table 1 illustrates the growth over the years in state privacy legislation.[90]

Table 1. *as of July 1, 2024



2018	CA (CCPA)
2019	
2020	CA (CPRA)
2021	CO, VA
2022	CT, UT
2023	DE, FL, IN, IA, MT, OR, TN, TX
2024	KY, MD, MN, NE, NH, NJ, RI

88. The 2023 adopters are: Delaware, Florida, Iowa, Indiana, Montana, Oregon, Tennessee, and Texas. *See* CTR. FOR INFO. POL'Y LEADERSHIP, *supra* note 24, at 2; *see also* Lakshmi Gopal, *State Privacy Law Update*, 79 BUS. LAW. 221, 231 (2024) ("This year, states have shown clear willingness to establish privacy safeguards on a range of privacy issues."); F. Paul Pittman & Abdul M. Hafiz, *New Jersey Enacts Comprehensive Data Privacy Law*, WHITE & CASE: ALERT (Feb. 5, 2024), https://www.whitecase.com/insight-alert/new-jersey-enacts-comprehensive-data-privacy-law [https://perma.cc/QU8P-WPHS].

89. *See US State Privacy Legislation Tracker*, INT'L ASS'N PRIV. PROS. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/#enacted-laws [https://perma.cc/9AKN-WYKQ]; *see also* Natasha G. Kohne, Michelle A. Reed, Rachel Claire Kurzweil & Joseph Hold, *New Jersey Data Protection Act: What Businesses Need to Know*, AKIN GUMP (Feb. 13, 2024), https://www.akingump.com/en/insights/alerts/new-jersey-data-protection-act-what-businesses-need-to-know#_edn22 [https://perma.cc/7UU8-H7Z5]; Kirk J. Nahra, Ali A. Jessani & Genesis Ruano, *New Hampshire Legislature Passes a Comprehensive Privacy Law*, WILMERHALE (Jan. 9, 2024), https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240109-new-hampshire-legislature-passes-a-comprehensive-privacy-law [https://perma.cc/AW58-WSNJ].

90. *See* Table 1.

California's Act served as an initial blueprint for the states that followed—however, none of the adopted or proposed laws that have followed are identical to it (or to each other). The following discussion highlights the commonalities and inconsistencies among the different statutes. In addition, as more and more states adopt privacy legislation, there are emerging points of convergence in how state legislatures are approaching general privacy protection laws.

1. California

In response to concerns over the ever-increasing amount and use of data in today's digital economy and corresponding calls for protections for privacy and security of personal data, California became the first state to enact enhanced privacy rights through the passage of the California Consumer Privacy Act (CCPA) of 2018.[91] Described as the strictest and most sweeping general privacy and data security legislation in the country, the CCPA provides for greater regulation of the collection, maintenance, sale, or other transfer of consumers' personal information as well as data breaches in the absence of reasonable security measures.[92] As a result, Californians gained new privacy rights and protections, several of which resemble those in the GDPR.[93] Following its initial adoption, the CCPA has been amended by regulations issued by the California Attorney General,[94] the California legislature,[95] and California voters. The latter acted through the California Privacy Rights Act of 2020 (CPRA), which was approved on November 3, 2020, as Proposition 24.[96]

The CPRA establishes rights for "consumers" as well as responsibilities for "businesses" that are controllers or processers of personal data.[97]

---

91. Cal. Civ. Code §§ 1798.100–.199 (West 2022); A.B. 375, 2017–2018 Reg. Sess. (Cal. 2018) (approved by the Governor June 28, 2018; filed with the Secretary of State June 28, 2018; adding Title 1.81.5 to the California Civil Code, effective Jan. 1, 2020).

92. *See* Pritesh P. Shah & Daniel F. Forester, *Impact of the California Consumer Privacy Act on M&A*, Harv. L. Sch. F. on Corp. Governance (June 20, 2019), https://corpgov.law.harvard.edu/2019/06/20/impact-of-the-california-consumer-privacy-act-on-ma/#:~:text=For%20instance%2C%20a%20business%20that,sale%20of%20their%20personal%20information. [https://perma.cc/7HHB-3F5S]; James G. Snell & Miriam Farhi, *Consumer Privacy Act of 2018 Brings Some GDPR Aspects Stateside*, Perkins Coie (June 29, 2018), https://www.perkinscoie.com/en/news-insights/california-consumer-privacy-act-of-2018-brings-some-gdpr-aspects.html [https://perma.cc/9PWG-TYH8]. Both the adoption and breadth of the act is not surprising given California's reputation as having some of the strongest consumer protection laws in the United States. *See* Kim, *supra* note 81, at 281.

93. Snell & Farhi, *supra* note 92.

94. Cal. Code Regs. tit. 11, §§ 999.300–.337 (West 2020); *see also* Cal. Civ. Code § 1798.185(c) (West 2020).

95. *See* A.B. 25, 2019–20 Reg. Sess. (Cal. 2019); A.B. 874, 2019–2020 Reg. Sess. (Cal. 2019); A.B. 1146, 2019–2020 Reg. Sess. (Cal. 2019); A.B. 1202, 2019–2020 Reg. Sess. (Cal. 2019); A.B. 1355, 2019–2020 Reg. Sess. (Cal. 2019); A.B. 1564, 2019–2020 Reg. Sess. (Cal. 2019); A.B. 713, 2019–2020 Reg. Sess. (Cal. 2020); A.B. 1281, 2019–2020 Reg. Sess. (Cal. 2020); S.B. 980, 2019–2020 Reg. Sess. (Cal. 2020).

96. California Privacy Rights Act of 2020, 2020 Cal. Legis. Serv. Prop. 24 (to be codified at Cal. Civ. Code §§ 1798.100–.199). For purposes of this paper, the collective, amended legislation will be referred to as the CPRA.

97. *Id.*

Based on the same notice-and-choice model as the GDPR,[98] the CPRA requires "businesses" to notify "consumers" about the types of "personal information" they collect, from what sources they collected such information, and for what purposes they are collecting such information.[99] Businesses must also disclose to a consumer when personal information is "sold," "shared," or "disclosed," and to whom it is being sold and shared.[100] In addition, consumers have the right to: opt out of their data being utilized for certain purposes, say "no" to the sale or sharing of personal information, access personal information that is collected and correct any errors in such information, and request that the business delete the consumer's information.[101] The CPRA further protects consumers who invoke their privacy rights under the Act from retaliation or discrimination by businesses.[102] The CPRA also imposes data minimization requirements, data security and care obligations, and data protection assessments on controllers of consumer data.[103] Finally, the CPRA provides for a limited private right of action and statutory damages in the event of a data breach resulting from the business's failure to implement and maintain reasonable security procedures and practices.[104]

The breadth of the CPRA is evident upon close inspection of the definitions of some of its key terms, in particular "business" and "consumer." The businesses that are covered by the CPRA include any for-profit corporation[105] doing business in California that collects (directly or indirectly through a third party) consumers' personal information and satisfies one or more of the following requirements: it (i) has at least $25 million in annual gross revenue, or (ii) alone or in combination, receives, buys, sells, or shares for commercial purposes, personal information on at least 100,000 California consumers or households, or (iii) derives more than half of its annual revenues from the sale of personal information.[106] In addition, any majority-owned subsidiary or parent company of a CPRA-defined "business" that shares common branding (e.g., shared name, trademark or service mark) is subject to the statute's requirements.[107] There is no requirement that a corporation have a physical presence in the state to be subject to

98. *See* Elvy, *supra* note 2, at 475. Compared to the GDPR, however, "the CCPA is less comprehensive and burdensome for data gatherers" and contains even less fines. Fan, *supra* note 20, at 1457 (describing the differences between the CCPA and GDPR).

99. Civ. §§ 1798.100(a), .110, .130.

100. *Id.* §§ 1798.115, .130.

101. *Id.* §§ 1798.105, .106, .120, .121, .130, .135.

102. *Id.* § 1798.125.

103. *Id.* §§ 1798.100(c), .100(e), .185(a)(15)(B).

104. *Id.* § 1798.150(c).

105. The CCPA's definition of "business" also includes "a sole proprietorship, partnership, limited lability company. . .association, or other legal entity." *Id.* § 1798.140(d)(1). The focus of this article is, however, only on the CCPA's impact on corporations.

106. *Id.*

107. *Id.* § 1798.140(d)(2) (defining "control" as "ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company").

the CPRA. The CPRA does not, however, apply to government agencies, non-profit businesses, or certain small businesses.[108] Overall, it is predicted that the CPRA will cover a large number of businesses located inside and outside of California, as the state is the world's fifth-largest economy.[109] Moreover, small businesses that do not meet the $25 million gross revenue threshold alone may nevertheless be subject to the statute if they control or are controlled by a business and share common branding with a business that meets the above criteria.[110]

The "consumer" who is protected under the CCPA is defined as a "natural person who is a California resident."[111] Accordingly, employees, applicants, shareholders, suppliers, and contractors, among others beyond the traditional consumer-customer, would all be included in this definition.[112] Recognizing the incredible breadth of this definition, the California legislature amended the statute to exempt personal information "collected by a business about a natural person" who is "acting as job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business."[113] This was, however, only a limited exemption until January 1, 2021.[114] The provisions of Proposition 24 (CPRA) then extended the exemption to January 1, 2023.[115] To date, those exemptions have not been extended. Thus, as of the writing of this paper, employees, directors, and officers of a corporation are once again included in the CPRA's sweeping "consumer" definition.

2. Virginia

The Virginia legislature adopted the Virginia Consumer Data Privacy Act (VCDPA) in March 2021, and it became effective January 1, 2023.[116] The VCDPA is based on the same foundational privacy principles as California's CCPA: "notice, choice, access, and security."[117] However, Virginia's statute uses terminology similar to the EU's GDPR and has less

---

108. *Id.* § 1798.140(d). In addition, certain types of information are exempt from protection under the Act including information already covered by: Health Insurance and Portability and Accountability Act of 1996, Gramm-Leach-Bliley Act, Fair Credit Reporting Act, Driver's Privacy Protection Act. *See id.* § 1798.145(c)(1), (e) & (f).

109. *See* Thomas Fuller, *The Pleasure and Pain of Being California, the World's 5th-Largest Economy*, N.Y. Times (May 7, 2018), https://www.nytimes.com/2018/05/07/us/california-economy-growth.html [https://perma.cc/B4NG-E7YY].

110. Civ. § 1798.140(d)(2).

111. *Id.* § 1798.140(i). California has approximately forty million residents. United States Census Bureau, *Quick Facts: California*, https://www.census.gov/quickfacts/fact/table/CA/PST045222 [https://perma.cc/D4ZM-GD43].

112. Civ. § 1798.140(i).

113. *Id.* § 1798.145(m)(1)(A); A.B. 25, 2019–2020 Reg. Sess. (Cal. 2019).

114. A.B. 25, 2019–20 Reg. Sess. (Cal. 2019).

115. Civ. §§ 1798.145(m)(4), (n)(3) ("This subdivision shall become inoperative on January 1, 2023.").

116. Va. Code Ann. §§ 59.1-575 to 59.1-585 (2021).

117. *VCDPA Series: Part 1*, Troutman & Pepper (Apr. 2021), https://www.troutman.com/images/content/2/7/276871/VCDPA-Overview-and-Introduction-Part-1.pdf [https://perma.cc/8H88-JUHN].

prescriptive requirements.[118] The businesses subject to the obligations in the VCDPA are:

> [P]ersons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that (i) during a calendar year, control or process personal data of at least 100,000 consumers or (ii) control or process personal data of at least 25,000 consumers and derive over fifty percent of gross revenue from the sale of personal data.[119]

Like California, the VCDPA exempts certain entities from its requirements, including: government authorities, agencies, or political subdivisions of Virginia; financial institutions or data subject to Title V of the Gramm-Leach-Bliley Act; nonprofit organizations; or institutions of higher education.[120] The VCDPA seeks to regulate businesses when acting as a "controller" or "processor" of consumer data. A "controller" means "the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data," while a "processor" means "a natural or legal entity that processes personal data on behalf of a controller."[121]

The VCDPA provides "consumers" with many of the same rights as its California predecessor, such as the rights to (i) know and access personal information, (ii) correct inaccurate personal information, (iii) delete personal data, (iv) transfer data to another, (v) opt out of the sale of personal data, and (vi) nondiscrimination for invoking rights under the act.[122] The VCDPA also offers protection against targeted advertising or profiling not contained in the California Act.[123] Unlike the CCPA, however, the VCDPA does not provide for a private right of action for violations under the law; rather, the state's attorney general is charged with enforcement.[124]

The VCDPA also imposes largely similar duties as the CCPA on business who control personal information of consumers. Specifically, controllers

---

118. Kirk J. Nahra, Ali A. Jessani, Samuel Kane & Genesis Ruano, *State Comprehensive Privacy Law Update for 2023*, WilmerHale (Jan. 19, 2023), https://www.wilmerhale.com/en/insights/blogs/WilmerHale-Privacy-and-Cybersecurity-Law/20230119-state-comprehensive-privacy-law-update-for-2023 [https://perma.cc/5WRT-YG9V] (describing how the VCDPA uses "controller" and "processor" as opposed to "business" and "service provider"—terms used in the CCPA); *VCDPA Series*, *supra* note 117.

119. Va. Code Ann. § 59.1-576.

120. *Id.* The Act also excludes certain types of information from its purview: health information under HIPAA, certain types of health records and information or documents covered by the federal health laws such as the Health Care Quality Improvement Act, personal data used or shared in certain types of research, de-identified information, information related to a consumer's credit that is regulated by and authorized under the federal Fair Credit Reporting Act, data in connection with the Driver's Privacy Protection Act of 1994, the Family Educational Rights and Privacy Act, and the Farm Credit Act. *See id.* § 59.1-576(C).

121. *Id.* § 59.1-575; Sanford P. Shatz & Paul J. Lysobey, *Update on the California Consumer Privacy Act and Other States' Actions*, 77 Bus. Law. 539, 543 (2022). The Act defines "process" or "processing" as "means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data." Va. Code Ann. § 59.1-575.

122. Va. Code Ann. § 59.1-577(A); Shatz & Lysobey, *supra* note 121, at 543–44.

123. Va. Code Ann. § 59.1-577(A)(5).

124. *Id.* § 59.1-577(C).

have the following duties: (i) transparency in privacy notices, (ii) specification regarding how data is used, (iii) minimization of data use, (iv) data security and care, (v) consent regarding sensitive data, and (vi) avoiding secondary use of data.[125]

Overall, the Virginia statute has a narrower application than California's statute in two respects. First, the Act applies to the "sale" but not "sharing" of personal information, whereas the CCPA covers both.[126] Second, the Virginia statute does not define "consumer" in the same sweeping manner as the CCPA. Rather, "consumer" includes a "natural person who is a resident of the Commonwealth acting only in an individual or household context."[127] The Act specifically excludes job applicants to, or employees of, a covered business or those acting in a commercial context, such as an agent or independent contractor of a controller or processor.[128]

3. Colorado, Connecticut & Utah

Virginia's statute, not California's statute, has largely served as the model for the subsequent state privacy laws that have been adopted and are being proposed.[129] Colorado's, Connecticut's, and Utah's privacy statutes each went into effect during 2023. The Colorado Consumer Protection Act (CPA) was signed into law on July 7, 2021, and became effective on July 1, 2023.[130] Of note, in a significant departure from the California and Virginia laws, Colorado's Privacy Act does not exclude nonprofits from its requirements.[131] Similar to Colorado, the Connecticut Data Privacy Act (CTDPA) also went into effect on July 1, 2023.[132] The Connecticut privacy statute adopts large portions of the Colorado and Virginia privacy statutes, sometimes verbatim. Utah's governor signed into law the Utah Consumer Privacy Act (UCPA) on March 24, 2022. This privacy statute went into effect on December 31, 2023.[133] Utah's law, however, is more circumscribed and less stringent than the prior four states' statutes. First, the statute contains a higher threshold for determining which companies are subject to the UCPA.[134] Second, the UCPA mandates less stringent requirements

125. *Id.* §§ 59.1-578, 59.1-580.

126. *See* Cal. Civ. Code § 1798.140(ad)(1). Relatedly, California's statute includes the sale for money or other consideration while Virginia's statute only includes the sale of data for money. *See id.*

127. Va. Code Ann. § 59.1-575.

128. *Id.* §§ 59.1-575, 59.1-576.

129. *See* Nahra, Jessani, Kane & Ruano, *supra* note 118.

130. An Act Concerning Additional Protection of Data Relating to Personal Privacy, Colo. Rev. Stat. §§ 6-1-1301 to -1313 (2023).

131. *See* David M. Stauss, *Colorado Privacy Act Resource Center*, HuschBlackwell, https://www.huschblackwell.com/industries_services/colorado-privacy-act [https://perma.cc/M3YP-PAB5].

132. An Act Concerning Personal Data Privacy and Online Monitoring, Conn. Gen. Stat. §§ 42-515 to -526 (2023).

133. Utah Consumer Privacy Act, Utah Code Ann. §§ 13-61-101 to -404 (West 2022).

134. The UCPA applies to any entity that (1) conducts business in Utah or produces products or services that are targeted to Utah residents; (2) has annual revenue of $25 million or more; and (3) annually controls or processes the personal data of at least 100,000 Utah residents, or controls or processes the personal data of at least 25,000 Utah residents and derives

(e.g., no requirement to conduct data protection assessments for certain types of activities) and provides consumers no right to correct personal data or appeal a company's decision to deny a consumer request.[135] These differences in the Utah statute as well as Colorado's inclusion of nonprofits as subject to the statute's requirements indicate that there is no clear consensus yet on the standard approach to privacy legislation.

Overall, Colorado, Connecticut, and Utah provide the same basic categories of rights to "consumers": (i) the right to know whether their data is being processed, (ii) the right to access their personal data, (iii) the right to correct their data,[136] (iv) the right to delete personal data they provided to a controller, (v) the right to copy their data in a portable and readily usable format, (vi) the right to opt out of the sale, profiling, or targeted adverting of their personal data,[137] (vii) the right to appeal a business's decision under the act,[138] and (viii) the right to avoid discrimination for exercising a right under the statute.[139] In addition, all of the statutes contain largely the same privacy notice requirements and impose the same duties on controllers—transparency, purpose specification, data minimization, data security/care, sensitive data consent, and avoiding secondary use.[140]

Finally, like Virginia's statute, these three privacy statutes do not sweep as broadly as California's CCPA. In particular, the definition of "consumer" is limited to individuals who are a resident of the applicable state and acting in their role as an individual or household and not in an employment or commercial context.[141] Thus, an individual who represents a company in a business-to-business context, or an individual employed by a company,

---

over 50% of its gross revenue from the sale of personal data. *See id.* § 13-61-102(1). The $25 million revenue threshold is also contained in the CCPA. CAL. CIV. CODE § 1798.140(d)(1)(A) (West 2022). Virginia, Colorado and Connecticut, by contrast do not have an annual gross revenue requirement. Their statutes apply to businesses that process data of at least 100,000 consumers or process data of at least 25,000 consumers and derive at least 50% of gross revenues from selling personal data. *See, e.g.*, COLO. REV. STAT. § 6-1-1304(1).

135. *See* VA. CODE ANN. § 59.1-580(A)(5) (2023); COLO. REV. STAT. § 6-1-1309(1)–(2); *Utah Consumer Privacy Act*, SULLIVAN & CROMWELL LLP (Apr. 27, 2022), https://www.sullcrom.com/SullivanCromwell/_Assets/PDFs/Memos/sc-publication-utah-becomes-fourth-us-state-to-enact-comprehensive-privacy-law.pdf [https://perma.cc/Z8W6-LNEW] ("Unlike the VCDPA and the CPA, the UCPA applies only to businesses with annual revenue of $25 million or greater, applies certain requirements only to personal data that consumers provided to those businesses, instead of all the information that those businesses obtain, does not provide a right for consumers to opt out of profiling, and does not require businesses to affirmatively assess data processing with 'a heightened risk of harm,' such as the use of sensitive data and profiling.").

136. Utah does not provide a right to correct. *See generally* UTAH CODE ANN. §§ 13-61-101 to -404.

137. Utah only provides an opt out right for the sale of personal data or targeted advertising using personal data and not for profiling. *See id.* § 13-61-201(4).

138. Utah does not provide a right to appeal. *See generally id.* §§ 13-61-101 to -404.

139. While Colorado and Connecticut do not have a nondiscrimination provision in their respective privacy statutes, they each impose a duty on controllers not to violate existing nondiscrimination laws. *See* COLO. REV. STAT. § 6-1-1308(6); CONN. GEN. STAT. § 42-520(a)(5) (2023).

140. Utah does not impose a secondary use duty. *See generally* UTAH CODE ANN. §§ 13-61-101 to -404.

141. *See, e.g.*, UTAH CODE ANN. § 13-61-101(10); COLO. REV. STAT. § 6-1-1303(6).

or a job applicant is not a "consumer" who is covered by the statute's protections.[142] Moreover, Connecticut and Colorado further exempt national securities associations registered pursuant to the Securities Exchange Act of 1934 from their statutes' requirements.[143]

4. The Second Wave of Consumer Data Privacy Statutes

The year 2023 saw continued legislative interest in regulating consumer data privacy. Thirty-two states considered such legislation with eight of those states passing comprehensive data privacy laws.[144] Delaware, Florida, Iowa, Indiana, Montana, Oregon, Tennessee, and Texas all enacted data privacy legislation in 2023.[145] And in just the first six months of 2024, adoption rates have nearly matched that of the previous year with seven new states adopting their own privacy laws.[146] While there are variations among these new statutes, the consensus is that no state has chosen to "reinvent the data-privacy wheel."[147] The following briefly describes this second wave of statutes.

Iowa was the first consumer data privacy law adopted in 2023.[148] The Iowa Data Privacy Law is somewhat more limited than Virginia's and notably does not include a revenue threshold in specifying what entities are subject to the statute.[149] While Iowa's statute contains the same basic consumer rights and obligations on businesses as other state statutes, it does not provide for a right to opt out of profiling or a right to correct information.[150] The Indiana Data Privacy Law was adopted next and is largely the same as Iowa's statute, refraining from including a revenue threshold in defining what entities are subject to the law and similarly omitting an opt-out option for profiling.[151]

---

142. *See* Utah Code Ann. § 13-61-101(10); Colo. Rev. Stat. § 6-1-1303(6).

143. *See, e.g.*, Colo. Rev. Stat. § 6-1-1304(2)(m).

144. *See US State Privacy Legislation Tracker 2023*, Int'l Ass'n Priv. Pros. https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_2023.pdf [https://perma.cc/YYP2-4H7N].

145. *Id.*

146. *See supra* note 89.

147. Gopal, *supra* note 88.

148. *See* Iowa Code §§ 715D.1–.9 (2023); *see also* Nyambura Kiarie, *U.S. State Data Privacy Laws: What You Need to Know*, AuditBoard (Nov. 22, 2023), https://www.auditboard.com/blog/updates-to-us-state-data-privacy-laws/ [https://perma.cc/X36Q-WBFM] (comparing the different privacy laws passed in 2023). The Iowa Data Privacy Law was signed into law on March 28, 2023 and will go into effect on January 1, 2025. David P. Saunders & Allison Tassel, *Iowa's New Privacy Law: The Basics*, McDermott Will & Emery (Apr. 10, 2023), https://www.mwe.com/insights/iowas-new-privacy-law-the-basics/ [https://perma.cc/KB77-R3CX].

149. *See* F. Paul Pittman, Abdul M. Hafiz & Nathan Swire, *Iowa Enacts Data Privacy Legislation with Senate File 262*, White & Case: Alert (Apr. 21, 2023), https://www.whitecase.com/insight-alert/iowa-enacts-data-privacy-legislation-senate-file-262 [https://perma.cc/TSQ3-V5VW]. The statute does exempt government entities, nonprofits, HIPAA-covered entities, higher education institutions and GLBA-regulated entities and data, and federally protected data from its provisions.

150. *See id.* Like Virginia, Iowa's statute does not include a private right of action.

151. *See* Ind. Code Ann. § 24-15-1-1 (West 2023); F. Paul Pittman, Abdul M. Hafiz & Andrew Hamm, *Indiana Becomes the Seventh State to Enact a Comprehensive Data Privacy Law*, White & Case: Alert (May 10, 2023), https://www.whitecase.com/insight-alert/indiana-becomes-seventh-state-enact-comprehensive-data-privacy-law [https://perma.cc/KDT4-DTYG]. The Indiana Data Privacy Law was signed into law on May 1, 2023 and will go into effect on January 1, 2026. *See id.*

Tennessee and Montana adopted their consumer privacy statutes not long after Indiana.[152] Each of these statutes notably diverge from prior privacy laws in how they structure their jurisdictional thresholds. Unlike other states, Tennessee defines 'covered entities' as meeting both a processing *and* revenue threshold, thus making it more restrictive in its applicability.[153] Montana, on the other hand, has a broader jurisdictional reach with the lowest threshold of any of the comprehensive privacy laws adopted at that time. The Montana Consumer Data Privacy Act applies to entities that (i) control or process the personal data of not less than 50,000 state residents *or* (ii) control or process the personal data of not less than 25,000 state residents and derive more than 25% gross revenue from the sale of personal data.[154] Commentators have pointed out that this lower threshold is likely to account for the smaller population in Montana and does not indicate a trend in privacy legislation.[155] Of note, Tennessee's statute is the first privacy law to provide for an affirmative defense for controllers and processers if they have a written privacy policy that conforms to the National Institute of Standards of Technology privacy framework.[156] In addition, both Tennessee and Montana provide for a longer right to cure than their predecessor statutes (sixty versus thirty days).[157]

In crafting Texas's privacy statute, the drafters considered issues that had arisen under prior state privacy statutes. Accordingly, Texas's statute attempts to clarify ambiguities in the terminology used as well as reconcile some of the differences between two of the principal consumer privacy statutes—Virginia and California.[158] The Texas Data Privacy and Security

152. The Tennessee Information Protection Act was signed into law on May 11, 2023 and becomes effective on July 1, 2025. *See* 2023 Tenn. Pub. Acts 408; F. Paul Pittman, Abdul M. Hafiz & Yuhan Wang, *Tennessee Passes Comprehensive Data Privacy Law*, WHITE & CASE: ALERT (June 23, 2023), https://www.whitecase.com/insight-alert/tennessee-passes-comprehensive-data-privacy-law [https://perma.cc/ZJN7-SW3M]. The Montana Consumer Data Privacy Act was signed into law on May 19, 2023 and becomes effective on October 1, 2024. *See* MONT. CODE ANN. §§ 30-14-2801 to -2817 (2023); Nancy Libin, Michael T. Borgia, John D. Seiver & Patrick J. Austin, *Montana Consumer Data Privacy Act Signed Into Law*, DAVIS WRIGHT TREMAINE LLP: PRIV. & SEC. L. BLOG (May 23, 2023), https://www.dwt.com/blogs/privacy—security-law-blog/2023/05/montana-consumer-data-privacy-law#print [https://perma.cc/J8BY-GETU].

153. Pittman, Hafiz & Wang, *supra* note 152; *see* 2023 Tenn. Pub. Acts 408. The statute also provides an insurance industry exemption for licensed insurance companies. 2023 Tenn. Pub. Acts 408. California is the only other state that also has an income threshold component to its applicability. *See* CAL. CIV. CODE § 1798.140 (West 2022).

154. MONT. CODE ANN. § 30-14-2803. By way of comparison, most of the other states are based on 100,000 residents. *See, e.g.*, UTAH CODE ANN. §§ 13-61-102 (West 2023).

155. *See* MONT. CODE ANN. §§ 30-14-2801 to -2817; Libin, Borgia, Seiver & Austin, *supra* note 152.

156. 2023 Tenn. Pub. Acts 408; *see also* Gopal, *supra* note 88, at 224 (noting that this affirmative defense imposes extra record keeping obligations on businesses who would want to try to rely on this defense at some point).

157. *See* Kier Lamont, *Tenn. Makes Nine? 'Tennessee Information Protection Act' Set to Become Newest Comprehensive State Privacy Law*, FUTURE OF PRIV. F. (Apr. 24, 2023), https://fpf.org/blog/tenn-makes-nine-tennessee-information-protection-act-set-to-become-newest-comprehensive-state-privacy-law/ [https://perma.cc/PA83-UXQP].

158. *See* James Sullivan & Hayley Curry, *Texas's Tough New Consumer Privacy Law*, DLA PIPER (May 30, 2023), https://www.dlapiper.com/insights/publications/2023/05/texass-tough-new-consumer-privacy-law?utm_source=vuture&utm_medium=email&utm_

Act (TDPSA) applies to individuals and entities if they (1) process or sell personal data and (2) conduct business in Texas or "produce[] a product or service consumed by" Texas residents.[159] Importantly, the TDPSA uses the phrase "consumed by" instead of "targeted to" in an effort to make clear that the statute applies to internet sellers.[160] Additionally, in crafting its jurisdictional thresholds, the statute rejects using revenue thresholds to exempt small business, instead opting to cite to the United States Small Business Administration definition in an effort to provide greater clarity regarding the statute's applicability.[161] The TDPSA also adopts the CCPA's expansive definition of "sale of personal data;"[162] however, in line with all of the other states' privacy statutes, it refrains from adopting a private right of action similar to that in California.[163]

As a general matter, Oregon's privacy statute is not significantly distinguishable in substance from prior state privacy laws. However, commentators have cautioned not to overlook the statute as it has a few notable requirements that make it more stringent than other state laws, such as the statute's applicability to nonprofits, differences in opt-out and opt-in rights, and required disclosures with respect to data processing by third parties.[164] While the thresholds for applicability of Oregon's privacy statutes to businesses are similar to many other states, Oregon's law includes a unique exemption for public corporations not found in other laws.[165]

Like Oregon, Delaware's Personal Data Privacy Act largely tracks the comprehensive data privacy laws passed in other states with respect to the rights provided to consumers and the obligations imposed on businesses.[166] The statute targets businesses conducting business in Delaware or producing products or services targeted to Delaware residents.[167] Its applicability thresholds are the lowest with respect to number of consumers (35,000),

---

campaign=data%20protection%2c%20privacy%20and%20security%20alerts [https://perma.cc/7FDE-STMM]. The Texas Data Privacy and Security Act was signed into law on June 18, 2023 and will be effective on July 1, 2024. *See* Tex. Bus. & Com. Code Ann. § 541.001–.205 (2023).

159. *See id.*

160. *See* Sullivan & Curry, *supra* note 158.

161. *See* Tex. Bus. & Com. § 541.002(3); Sullivan & Curry, *supra* note 158.

162. *See* Tex. Bus. & Com. § 541.001(28).

163. The TDPSA also attempts to reconcile the Virginia and California statutes' differences on controller responsibilities. *See generally* Tex. Bus. & Com. § 541.001–.205. And uniquely, it does not include a sunset period in its cure provisions like many of the other states.

164. *See* F. Paul Pittman, Abdul M. Hafiz & Nathan Swire, *Oregon Passes Comprehensive Data Privacy Law*, White & Case: Alert (Sept. 20, 2023), https://www.whitecase.com/insight-alert/oregon-passes-comprehensive-data-privacy-law [https://perma.cc/NMF8-DSUT]. Oregon's applicability to non-profit organizations is like that found in Colorado. *See id.* And Oregon's provisions regarding the ability of consumers to opt out of profiling is similar to provisions found in Montana's and Indiana's statutes. *See id.* The Oregon Consumer Privacy Act was signed into law on July 18, 2023 and will become effective on July 1, 2024. Or. S.B. 619-B (2023).

165. Or. S.B. 619-B § 2(2)(a).

166. The Delaware Personal Data Privacy Act was signed into law on September 11, 2023 and will become effective on January 1, 2025. *See* Del. Code Ann. tit. 6, § 12D-101–111 (West, Westlaw through 2023–2024 legislation).

167. *See id.* § 12D-103(a); *see also* Jason J. Rawnsley & Matthew D. Perri, *Delaware Enacts Personal Data Privacy Act*, Richards Layton & Finger (Sept. 20, 2023), https://www.rlf.com/delaware-enacts-personal-data-privacy-act/ [https://perma.cc/6XJS-P3BU].

recognizing, in a similar way that Montana's statute does, the smaller population of the state.[168] Like Oregon and Colorado, Delaware's statute does not exclude nonprofit companies from its purview.[169]

Florida also adopted consumer privacy legislation in 2023, but the law is significantly more limited in applicability than any of the other state statutes. The Florida Digital Bill of Rights (FDBR) grants Florida consumers certain rights relating to the processing of their personal data by businesses in a similar manner to that of Texas and California.[170] Importantly, the statute has numerous exceptions and unique applicability thresholds resulting in most businesses being exempt from many of its provisions.[171] For example, the FDBR applies to for-profit businesses that conduct business in Florida and generate more than 1 billion dollars in global gross annual revenue as well as:

> (1) generate 50 percent or more of their global gross annual revenue from the sale of advertisements online; (2) operate an app store or digital distribution platform that offers at least 250,000 different software applications for consumers; or (3) operate certain kinds of consumer smart speaker and voice command component services.[172]

The FDBR also exempts twenty-one categories of information from its provisions.[173] Moreover, the statute addresses many new privacy issues such as censorship, disclosure of how political ideology influences search algorithms, and limitation on the collection of information regarding children.[174] As a result, the statute has been described as one primarily targeting big tech giants like Amazon.com, Inc. and Alphabet Inc.[175]

As of July 1, 2024, seven additional states have adopted comprehensive consumer privacy statutes.[176] This new crop of statutes provide for consumer

---

168. *See* tit. 6, § 12D-103(a).

169. *See id.* § 12D-103(b). However, nonprofit organizations "dedicated exclusively to preventing and addressing insurance crime" are exempt. *See id.* § 12D-103(b)(3).

170. The FDBR was signed into law on June 6, 2023 and will be effective on July 1, 2024. Fla. Stat. Ann. §§ 501.701–722 (West 2024). The social media moderation provision became effective on July 1, 2023. Fla. SB 262 §§ 4–27 (2023) (creating Fla. Stat. §§ 501.70–501.721 and amendments to Fla. Stat. §§ 501.171, -16. -53); *Florida Comprehensive State Privacy Law Sent to Governor for Signature*, Hunton Andrews Kurth (May 17, 2023), https://www.huntonprivacyblog.com/2023/05/17/florida-comprehensive-state-privacy-law-sent-to-governor-for-signature/# [https://perma.cc/69WH-2WWW].

171. *See* Fla. Stat. § 501.702, .704.

172. Gopal, *supra* note 88, at 223 (citing Fla. Stat. § 501.702(9)(a)(6)).

173. *See* Fla. Stat. § 501.704.

174. *See* Fla. Stat. § 112.23 (West, Westlaw through 2023 Reg. Sess.).

175. *See, e.g.*, Skye Witley, *DeSantis Takes Swing at Big Tech in New Florida Privacy Law (1)*, Bloomberg L., https://news.bloomberglaw.com/privacy-and-data-security/florida-enacts-privacy-law-that-takes-a-big-swing-at-big-tech [https://perma.cc/746V-28X9] ("But Florida's take on consumer data privacy also tackles issues that state Republicans have raised with tech platforms, like the alleged censorship of conservative views online."); Gopal, *supra* note 88, at 223.

176. The New Jersey Privacy Act was signed into law on January 16, 2024 and will become effective on January 15, 2025. S.B. 332, 220th Gen. Assemb., Reg. Sess. (N.J. 2024). New Hampshire's consumer data privacy act was signed into law on March 6, 2024 and will become effective on January 1, 2025. S.B. 255-FN, 2024 Leg., Reg. Sess. (N.H. 2024). The Kentucky Consumer Data Protection Act was signed into law on April 4, 2024 and will become effective on January 1, 2026. Natasha G. Kohne, Rachel Clarie Kurzweil & Joseph Hold, *Kentucky*

rights and controller/processor obligations that largely align with other state privacy laws.[177] There continue to be, however, notable variations among the states with respect to terms like applicability thresholds, entity and information exemptions,[178] whether non-monetary consideration is a "sale" of data,[179] requirements for universal opt out mechanisms,[180] and cure periods.[181] A comparison of the applicability thresholds illustrates the wide array of individual state tailoring in these laws. Nebraska, for example, does not use numerical thresholds for consumers or revenue as the trigger for the statute's applicability.[182] On the other end of the spectrum, New Hampshire, Maryland, Kentucky, Rhode Island, and Minnesota include consumer *and* revenue thresholds for the statutes' applicability, although the exact thresholds vary from state to state.[183] And in the middle of these

Data Protection Act: What Businesses Need to Know, Akin Gump (May 30, 2024), https://www.akingump.com/en/insights/blogs/ag-data-dive/Kentucky-data-protection-act-what-businesses-need-to-know [https://perma.cc/SC4Y-UME6]. Governor Wes Moore signed into law the Maryland Online Data Privacy Act on May 9, 2024 and it will become effective on October 1, 2025. F. Paul Pittman & Abdul M. Hafiz, *Maryland Enacts Comprehensive Data Privacy Law*, White & Case: Alert (May 14, 2024) [hereinafter Pittman & Hafiz, *Maryland*], https://www.whitecase.com/insight-alert/maryland-enacts-comprehensive-data-privacy-law [https://perma.cc/KGH4-KA2Q]. Minnesota's Consumer Data Privacy Act was signed into law on May 24, 2024 and will become effective on July 31, 2025. *See Minnesota Enacts Comprehensive Privacy Legislation*, Fredrickson (June 4, 2024), https://www.fredlaw.com/alert-minnesota-enacts-comprehensive-privacy-legislation [https://perma.cc/5HC4-EEYH]. On April 17, 2024, the Nebraska Data Privacy Act was signed into law, and it will become effective on January 1, 2025. F. Paul Pittman, Abdul M. Hafiz & Yixin Yan, *Nebraska Enacts Comprehensive Data Privacy Law*, White & Case: Alert (Apr. 25, 2024), https://www.whitecase.com/insight-alert/nebraska-enacts-comprehensive-data-privacy-law [https://perma.cc/9N3B-4YM9]. Finally, Rhode Island became the twentieth state with a privacy statute on June 28, 2024, when the Rhode Island Data Transparency and Privacy Protection Act was passed into law. It will take effect on January 1, 2026. F. Paul Pittman & Abdul M. Hafiz, *Rhode Island Enacts the Data Transparency and Privacy Protection Act, Joining the US Data Privacy Landscape*, White & Case: Alert (July 2, 2024) [hereinafter Pittman & Hafiz, *Rhode Island*], https://www.whitecase.com/insight-alert/rhode-island-enacts-data-transparency-and-privacy-protection-act-joining-us-data [https://perma.cc/X6TR-K8ZT].

177. *See* Kohne, Reed, Kurzweil & Hold, *supra* note 89; Nahra, Jessani, Kane & Ruano, *supra* note 118.

178. For example, Minnesota and Nebraska follow in Texas' footsteps in exempting small businesses from the statute's purview, while the majority of states do not provide for such an exemption. Minn. Stat. § 325O.03 (2024); 2024 Neb. Leg. Bill 1074 § 3(1)(c). On the other hand, Minnesota differs from many states in that its statute does not exempt non-profit organizations. *See* Fredrickson, *supra* note 176.

179. *Compare* Ky. Rev. Stat. § 367.1(27) (2024) (providing that non-monetary consideration is not a sale), *with* Md. Code Ann., Com. Law § 14-4601(FF) (2024) (providing that monetary or other valuable consideration (i.e., non-monetary) is a sale).

180. For example, Kentucky and Rhode Island do not require a universal opt-out mechanism in its statute, while Maryland and other states do. *See* Kohne, Kurzweil & Hold, *supra* note 176; Pittman & Hafiz, *Rhode Island*, *supra* note 176.

181. Kentucky and Nebraska do not follow other states in sunsetting their cure provisions, instead providing for permanent cure periods. *See* Kirk J. Nahra, Ali A. Jessani & Samuel Kane, *Kentucky Nears Enactment of a Comprehensive Privacy Law*, WilmerHale (Mar. 22, 2024), https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240321-kentucky-nears-enactment-of-a-comprehensive-privacy-law [https://perma.cc/GC2A-LGL2]; Pittman, Hafiz & Yan, *supra* note 176.

182. *See* 2024 Neb. Leg. Bill 1074 § 3. Texas is the only other state that lacks numerical thresholds in its applicability provisions. *See supra* note 158 and accompanying text.

183. *See* S.B. 255-FN, 2024 Leg., Reg. Sess. (N.H. 2024) (stating a threshold of 35,000 consumers or 10,000 consumers and more than twenty-five percent of gross revenue comes from

two approaches is New Jersey, which provides for numerical thresholds of consumers but does not provide for a minimum amount or percentage of revenue from the sale of personal data to trigger the law's applicability.[184] This feature is unique to only New Jersey. Moreover, beyond deviations in key terms, some of the 2024 statutes introduced new concepts altogether in their privacy laws.[185] Overall, 2024 continues the trend of individual state tailoring in crafting privacy laws, with no two statutes being the same.

* * *

The second wave of privacy statutes all follow the same basic framework, use similar terminology, impose similar obligations on businesses, and provide for largely the same core consumer rights as the first wave of statutes.[186] Nevertheless, there are still notable variances across these state statutes in terms of scope and applicability.[187] As a result, there has yet to emerge a clear "template" for crafting privacy legislation. Rather, states have adopted three models to address consumer privacy. The first approach is California's, which, as described above, is the most sweeping of the privacy models.[188] While several states have used parts of the California scheme as a basis for their statutes, no other state has addressed data protection in such a broad manner.[189]

The second approach is modeled after Virginia's statute, which is considered more business-friendly and less restrictive than states like California or Connecticut.[190] The Virginia approach has been described as "harmonizing

---

the sale of personal data); KY. REV. STAT. § 367.2(1) (stating a threshold of 100,000 consumers or 25,000 consumers and more than fifty percent of gross revenue comes from the sale of personal data); MD. CODE ANN., COM. LAW § 14-4602 (2024) (stating a threshold of 35,000 consumers or 10,000 consumers and more than twenty percent of gross revenue comes from the sale of personal data); MINN. STAT. § 325O.03 (2024) (stating a threshold of 100,000 consumers or 25,000 consumers and more than twenty-five percent of gross revenue comes from the sale of personal data); R.I. GEN. LAWS § 6-48.1-4 (2024) (stating a threshold of 35,000 consumers or 10,000 consumers and more than twenty percent of gross revenue comes from the sale of personal data).

184. S.B. 332, 220th Gen. Assemb., Reg. Sess. (N.J. 2024). New Jersey also does not exempt non-profit organizations, nor does it exclude information covered by FERPA (which is different than most privacy statutes). *Id.* Finally, New Jersey's definition of sensitive data is broader than that of other states. *Id.* at § 1.

185. Minnesota, for example is the first state to require a controller to maintain a personal data inventory as well as have its privacy law apply to EdTech companies. *See* FREDRICKSON, *supra* note 176. In addition, it provides consumers with the right to question a controller's profiling decisions. *See id.* In contrast to Minnesota, Rhode Island's statute has been critiqued as an outlier due to its failure to include many provisions common to other state privacy laws. *See* Joe Duball, *Rhode Island's Comprehensive Privacy Bill Raises Patchwork Misalignment Concerns*, INT'L ASS'N PRIV. PROS. (June 21, 2024), https://iapp.org/news/a/omissions-misalignment-raise-questions-with-rhode-island-s-comprehensive-privacy-bill [https://perma.cc/BKD9-2CFY].

186. *See* Nahra, Jessani, Kane & Ruano, *supra* note 118. Florida would be the only exception to this statement due to the limited number of businesses that are subject to its provisions. *See* FLA. STAT. ANN. §§ 501.702, .704 (West 2024).

187. *See* Nahra, Jessani, Kane & Ruano, *supra* note 118.

188. *See supra* note 20 and accompanying text.

189. For example, California is the only state that provides for a private right of action to enforce violations of its statute. *See* CAL. CIV. CODE § 1798.150 (West 2022).

190. *See* discussion *supra* Section I.B.2.

state laws with those global best practices that businesses might find easier to implement."[191] Examples of states that follow in Virginia's footsteps in this regard include Iowa, Indiana, Kentucky, Nebraska, Tennessee, Texas, and Utah.[192]

The third emerging approach to privacy law is based on Connecticut's statute, which is viewed as demanding more from businesses when it comes to data protection. The Connecticut model has been described as coming "closest to global best practices, making it easier for U.S. businesses to offer their products and services on the global market."[193] Examples of states that follow the Connecticut approach include Delaware, Maryland, Montana, Oregon, New Jersey, and Colorado.

II. PRIVACY LAWS' APPLICATION TO CORPORATE ACTIVITY

The breadth of state privacy statutes means that can they cover individuals beyond the traditional, individual consumer envisaged as needing protection. In California, for example, recognizing that directors, officers, employees, and owners of corporations fell within the statute's original, broad definition of "consumer," exemptions were temporarily put in place for individuals acting in these roles.[194] Such exemptions have expired, however, resulting in these actors all falling back under the purview of that state's statute again.[195]

Interestingly, while personal information regarding a corporate director or officer (when used in the context of such person's role) had (for a limited time) been exempt from the requirements of the CCPA, shareholder information was not.[196] In reviewing the statutory provisions, shareholders of a corporation similarly fall within the statute's purview. A shareholder who is a resident of California would fall under the statute's broad definition of "consumer." Both the 2019 amendments (AB25) and 2020's Proposition 24 provide for the exemption of "owners" from the definition of "consumer." The CCPA (as amended) defines "owner" as a natural person who either (i) "has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business," (ii) "has control in any manner over the election of a majority of the directors or of individuals exercising similar functions," or (iii) "has the power to exercise

191. Gopal, *supra* note 88, at 225.

192. *See, e.g.*, Utah Code Ann. §§ 13-61-101 to -404 (LEXIS through 2d Spec. Sess. laws of 2023).

193. Gopal, *supra* note 88, at 225.

194. *See* Cal. Civ. Code §§ 1798.145(m)(4), (n)(3).

195. *See id.* § 1798.145(m)(4).

196. Notably, the definition of "officer" under the CCPA and AB25 would only cover some, but not necessarily all officers of a corporation. *Id.* § 1798.145(m)(2)(D). "Officer" is defined as "a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, including a chief executive officer, president, secretary, or treasurer." *Id.* Thus, individuals appointed as officers pursuant to the bylaws or another officer (and not by the board) would not be covered under this definition. *See id.*

a controlling influence over the management of a company."[197] While some large shareholders may fall under this definition, the vast majority of shareholders who are natural persons will not meet the statute's definition of *owner*.[198] In addition, non-owner shareholders are unlikely to be engaged in the type of activity that would trigger the business-to-business exception added to the Act in 2019 in AB 1355. That exception applies to:

> [P]ersonal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who acted or is acting as an employee, owner, director, officer, or independent contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit, or government agency.[199]

Thus, most individual, human shareholders will be considered *consumers* under the CCPA.[200]

As discussed above, and illustrated in Table 2, the other nineteen states with privacy statutes draw narrower definitions of *consumer*.[201] These states exclude individuals acting in an employment context (whether as an employee or job applicant) or in a commercial or business-to-business context from the definition of *consumer*.[202] Directors and officers of a corporation will likely fall outside of these states' statutory provisions under the employment exemption and also because their information is not being collected in an individual or household context. Shareholders, on the other hand, appear to fall within fourteen of the twenty states' definitions of

197. *Id.* § 1798.145(m)(2)(E).

198. *See id.* And for those shareholders who do meet the definition of "owner," those will mostly be entity–shareholders not natural persons.

199. *Id.* § 1798.145(n)(1).

200. *See id.*

201. *See infra* Table 2.

202. *See supra* notes 141–142 and accompanying text; IOWA CODE § 715D.1(7) (West, Westlaw through 2024 Reg. Sess.) (excluding natural persons "acting in a commercial or employment context" form the definition of "consumer"); IND. CODE ANN. § 24-15-1-1 (LEXIS through Pub. L. No. 255-2023); 2023 Tenn. Pub. Acts 408; TEX. BUS. & COM. CODE ANN. § 541.001(7); 2023 OR. S.B. 619; FLA. STAT. § 501.702(8) (West 2024); S.B. 332, 220th Gen. Assemb., Reg. Sess. (N.J. 2024). Montana's statute is even more explicit than the others, providing that:

> [Consumer] does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit, or government agency.

MONT. CODE ANN. § 30-14-2802(6)(b) (2023). Connecticut, Delaware, Maryland, New Hampshire, and Rhode Island have similar language in their statutes. *See, e.g.*, CONN. GEN. STAT. ANN. § 42-515(8) (West 2022); DEL. CODE ANN. tit. 6, § 12D-102(8) (West, effective Jan. 1, 2025); MD. CODE ANN., COM. LAW § 14-4601(H)(2) (2024); N.H. REV. STAT. § 507-H:1(VIII) (2024); R.I. GEN. LAWS § 6-48.1-2(10) (2024).

consumer as they are residents acting in an individual context.[203] Notably, this conclusion is consistent with the EU's GDPR.[204]

Table 2. Exclusions from definition of "consumer"

State	No exclusions	Individual acting in a "commercial or employment context"	Individual acting in a "commercial or employment context or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency"
CA	X		
CO		X	
CT			X
DE			X
FL		X	
IN		X	
IA		X	
KY		X	
MD			X
MN		X	
MT			X
NE		X	
NH			X
NJ		X	
OR		X	
RI			X
TN		X	
TX		X	
UT		X	
VA		X	

203. The six exceptions to this are Connecticut, Montana, Delaware, Maryland, Rhode Island, and New Hampshire, which exclude "owners" from the definition of "consumer." *See, e.g.*, Mont. Code Ann. § 30-14-2802(6)(b) (2023); Conn. Gen. Stat. Ann. § 42-515(8); Del. Code Ann. tit. 6, § 12D-102(8) (Westlaw, effective Jan. 1, 2025); N.H. Rev. Stat. § 507-H:1(VIII) (2024); Md. Code Ann., Com. Law § 14-4601(H)(2); R.I. Gen. Laws § 6-48.1-2(10). While these statutes do not define *owner*, it could reasonably be argued that shareholders would fall within this exclusion. And further, state rulemaking pursuant to privacy statutes could make this issue clear. It should also be noted that in the context of shareholders national securities associations registered pursuant to the Securities Exchange Act of 1934 are exempt from Colorado and Connecticut's statutes. *See, e.g.*, Colo. Rev. Stat. § 6-1-1304(2)(m) (2023).

204. *See generally* General Data Protection Regulation, 2016 O.J. (L 119).

At present, the majority of state privacy laws require covered businesses to provide notice to shareholders of their data processing practices described above and will soon require businesses to respond to consumer rights request from these individuals. This is a similar outcome to that under the GDPR. The notice and disclosure obligations also extend to California residents who are corporate directors, officers, employees or applicants.[205]

Beyond these new notice obligations, whether other corporate activity is in tension with the goals of the privacy statutes or the actual provisions of the statutes themselves is something corporations and legislators in states considering adopting privacy statutes need to consider. The following Sections analyze different types of corporate actions and how they may or may not be impacted by state privacy statutes. While it appears that Virginia and Connecticut, and not California, are serving as the general models for state privacy law proposals, the breadth of California's statute as well as the scope and scale of the number of businesses and individuals covered by the CCPA cannot be ignored.[206] Thus, the analysis focuses on the application of California's statute with discussion of where the other states' statutes diverge.

A. Mergers and Acquisitions

Under state privacy statutes, consumers have the right to opt out of the processing of personal data for the purpose of selling their personal data.[207] The statutes generally define a sale as involving an exchange of personal data for monetary consideration.[208] However, states like California, Colorado, Connecticut, Maryland, Nebraska, and others are slightly more expansive, including the exchange of personal data for other valuable consideration to also be considered a "sale" or "selling."[209] All of the statutes, however, explicitly exempt the transfer of personal data that is part of a proposed or actual merger or acquisition with a third party.[210] Thus, merger and acquisitions activity should not trigger obligations under state privacy statutes. Of course, going forward, it is important for other states, or a federal privacy statute, to continue to include this exemption.

B. Stock List and the Annual Meeting

Another instance where corporations disclose or share information is related to their annual shareholder meeting. In connection with the annual

205. Sullivan & Cromwell LLP, *supra* note 135.

206. *See* Fuller, *supra* note 109 (stating that California is the world's fifth-largest economy in the world).

207. *See, e.g.* Utah Code Ann. § 13-61-201(4) (West 2023); Colo. Rev. Stat. § 6-1-1306(1)(a)(I)(B).

208. *See, e.g.*, Utah Code Ann. § 13-61-101(31)(a); Ky. Rev. Stat. § 367.1(27) (2024).

209. *See, e.g.*, Colo. Rev. Stat. § 6-1-1303(23)(a) (defining sale, sell or sold as "the exchange of personal data for monetary or other valuable consideration by a controller to a third party"); Cal. Civ. Code § 1798.140(ad)(1) (West 2022); Md. Code Ann., Com. Law § 14-4601(FF) (2024); 2023 Neb. Leg. B. 1074 § 2(29).

210. *See, e.g.*, Utah Code Ann. § 13-61-101(31)(b)(vii); Colo. Rev. Stat. § 6-1-1303(23)(b)(IV); Cal. Civ. Code § 1798.140(ad)(2)(C); Va. Code Ann. § 59.1-575 (2023).

meeting of shareholders, most states require a corporation to prepare and make available for inspection an alphabetical list of the names of all the shareholders who are entitled to notice and, if different, vote at the annual meeting.[211] The list shall be available for inspection by any shareholder for a certain period of time specified in the statute.[212] To the extent shareholders are covered, as is the case in California, as *consumers* under the privacy statutes, states need to consider how stock list disclosures can be reconciled with privacy obligations.[213] Making the stock list available for inspection would not trigger the opt-out rights under privacy statutes related to the sale of personal information because it does not involve the exchange of the information for money or other valuable consideration.[214] In California, consumers' opt-out rights also include the "sharing" of personal information; however, *sharing* is limited to only when it is done "for cross-context behavioral advertising."[215] Moreover, statutes like California's make clear that "[t]he obligations imposed on businesses by this title shall not restrict a business's ability to: comply with federal, *state*, or local laws or comply with a court order or subpoena to provide information."[216] Thus, state corporate law requirements such as the disclosure of the stock list in connection with a shareholders' meeting are exempt from the obligations in the current privacy statutes.[217]

C. Statutory Books and Records Demands

Corporate law provides shareholders, acting in such role, a private right to corporate information.[218] Specifically, most state corporate codes provide shareholders a statutory right to inspect the corporation's books and records.[219] The books and records shareholders can gain access to include, for example, the stock ledger, list of shareholders, financial statements, accounting records, notices to shareholders, the certificate of incorporation, bylaws, written communications to shareholders, meeting minutes, written consents, a list of the names and business addresses of current directors and officers, as well as other books and records.[220] Recent developments

211. *See, e.g.*, Del. Code Ann. tit. 8, § 219 (West 2022); Model Bus. Corp. Act § 7.20(a) (Am. Bar Ass'n, amended 2023).

212. *See, e.g.*, Del. Code Ann. tit. 8, § 219(a) (requiring the list be available for a "period of 10 days ending on the day before the meeting date"); Model Bus. Corp. Act § 7.20(b) (requiring the list to be available for inspection beginning "two business days after notice of the meeting is given for which the list was prepared and continuing through the meeting").

213. *See* Cal. Civ. Code § 1798.140(i).

214. *See* Colo. Rev. Stat. § 6-1-1303(23)(a) (defining sale, sell or sold as "the exchange of personal data for monetary or other valuable consideration by a controller to a third party"); Cal. Civ. Code § 1798.140(ad)(1).

215. Cal. Civ. Code § 1798.140(ah)(1).

216. *Id.* § 1798.145(a)(1)(A) (emphasis added).

217. *See id.*

218. Directors also generally have similar private information rights. *See, e.g.*, Del. Code Ann. tit. 8, § 220 (West 2022); Model Bus. Corp. Act § 16.05 (Am. Bar Ass'n, amended 2023). Books and records demands are predominantly brought by shareholders in comparison to director request. Thus, this Section will focus on shareholder requests.

219. *See, e.g.*, Del. Code Ann. tit. 8, § 220(b).

220. *See, e.g.*, *id.*; Model Bus. Corp. Act §§ 16.01–.02.

in this area of corporate law have made it a space rife for obtaining valuable corporate data. First, the general increase in digital data means that corporations have more information that may be subject to these statutory inspection rights. As explained by two corporate experts:

> Delaware courts continue to liberalize stockholder inspection rights to keep pace with modern society's expanding use of electronically stored information ("ESI") and electronic communication in business. As email and other ESI have become more common and integral in business, the corporate 'paper trail,' once limited to formal board books and the like, has expanded.[221]

Second, there has been a dramatic increase in the amount of inspection claims in Delaware in recent years as well as an increase in the extent of documents requested, far exceeding the prior stock list requests that dominated this space.[222] All told, shareholders are increasingly seeking private data from their corporations through inspection rights.[223]

Given that books-and-records demands have been found to lead to the disclosure of valuable corporate data, it is an area of corporate law poised to come into conflict with consumer privacy statutes. Shareholders and, in California, directors and officers, are *consumers* who receive protections under the privacy statutes.[224] In particular, the stock list, stock ledger, and contact information for directors and officers that may need to be disclosed under corporate inspection statutes raise concerns under state privacy statutes. This information would all fall under the statutes' definitions of "personal data"[225]—"information that is linked or reasonably linkable to an identified individual or an identifiable individual."[226] While publicly available information is excluded from the definition of personal data in the statutes, not all of this information regarding shareholders, directors, and officers would be publicly available.[227] In particular, email addresses and

---

221. Geeyoung Min & Alexander M. Krischik, *Realigning Stockholder Inspection Rights*, 27 STAN. J.L. BUS. & FIN. 225, 231 (2022); *see, e.g.*, *In re* Boeing Co. Derivative Litig., No. 2019-0907-MTZ, 2021 WL 4059934, at *1 (Del. Ch. Sept. 7, 2021); KT4 Partners LLC v. Palantir Techs. Inc., 203 A.3d 738, 752–53 (Del. 2019).

222. *See* James D. Cox, Kenneth J. Martin & Randall S. Thomas, *The Paradox of Delaware's "Tools at Hand" Doctrine: An Empirical Investigation*, 75 BUS. LAW. 2123, 2127 (2021) (finding a "nearly thirteen times increase, in § 220 inspection requests").

223. *See* George S. Geis, *Information Litigation in Corporate Law*, 71 ALA. L. REV. 407, 440 (2019) (observing that "[c]orporate information litigation has grown dramatically, as shareholders increasingly seek private data in various contexts"); *see also* Cox, Martin & Thomas, *supra* note 222, at 5 (describing inspection as a "backdoor method of obtaining pre-filing discovery").

224. *See, e.g.*, CAL. CIV. CODE § 1798.140(i) (West 2022).

225. California uses the phrase "personal information." *Id.* § 1798.140(v).

226. *See, e.g.*, UTAH CODE ANN. § 13-61-101(24)(a) (West 2023); COLO. REV. STAT. § 6-1-1303(17)(a) (2023). However, to the extent that any of this information is publicly available, it is excluded from the definition of "personal data." *See, e.g.*, UTAH CODE ANN. § 13-61-101(24)(b); COLO. REV. STAT. § 6-1-1303(17)(a)–(b).

227. *See, e.g.*, UTAH CODE ANN. § 13-61-101(24)(b); COLO. REV. STAT. § 6-1-1303(17)(a)–(b). "Publicly available information" has been defined as "information that is lawfully made available from federal, state, or local government records and information that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public." COLO. REV. STAT. § 6-1-1303(17)(b).

the number and types of shares an individual owns in a corporation would generally not be publicly available.[228] Moreover, to the extent a books-and-records demand seeks broader access to corporate books and records, and in particular ESI, it could give an inspecting shareholder access to broader categories of consumer information.

Books-and-records inspection rights will not trigger privacy statutes' provisions on opting out for the processing of data for targeted advertising or profiling because that is not the purpose for such inspections. In addition, shareholder inspection rights would not fall within the opt-out rights for *sharing* under California's statute because the sharing of the information would not be for the purpose of cross-context behavioral advertising.[229] Disclosure under books-and-inspection rights could fall within the privacy statutes' definitions of "sale" as it includes "disclosing" or "exchanging" consumer information to a third party, but it must for monetary or, in some states, valuable consideration.[230] While it would not be expected to have an exchange of consideration in the inspection context, corporations would need to be aware of the possible inclusion of shareholder inspections under privacy statutes.

In addition, Utah excludes from its definition of *sale* disclosures to a third party for purposes "consistent with a consumer's reasonable expectations."[231] It could thus be argued that books-and-records inspection rights in accordance with corporate statutes are consistent with a consumer's reasonable expectations. Further, California's statute contains an exemption for compliance with federal, state, or local laws as well as court orders or subpoenas to provide information; however, this would only capture a portion of books-and-records inspection scenarios where the shareholder has sought a court-ordered inspection.[232] In fact, books-and-records statutes are structured such that the process can take place wholly "extrajudicially—that is, privately and outside of formal court proceedings."[233] Under Delaware's Section 220, for example, a stockholder can make a demand to inspect a corporation's "stock ledger, a list of its stockholders, and its other books and records."[234] It is only when a corporation refuses to permit the inspection sought by a stockholder that the stockholder may then involve the courts by seeking an order to compel inspection.[235] And

228. *See* Model Bus. Corp. Act § 16.01(a), (d) (Am. Bar Ass'n, amended 2023) (outlining the records and information a corporation shall maintain).

229. Cal. Civ. Code § 1798.140(ah).

230. California's definition of *sale* is phrased in broader terms than the other states, including "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means." *Id.* § 1798.140(ad)(1); *see also* Tex. Bus. & Com. Code Ann. § 541.001(28) (West 2024) (defining *sale* broadly like the CCPA). By contrast, some of the other states define sale just in terms of an *exchange*. *See, e.g.*, Utah Code Ann. § 13-61-101(31)(a); Colo. Rev. Stat. § 6-1-1303(23)(a).

231. Utah Code Ann. § 13-61-101(31)(b)(iii).

232. *See* Cal. Civ. Code § 1798.145(a)(1)(A).

233. Min & Krischik, *supra* note 221, at 234; *see also id.* at 264 ("There is an argument that it is a feature, not a bug, of current Section 220 procedure that so much of it happens outside the courthouse doors.").

234. Del. Code Ann. tit. 8, § 220(b)(1) (2010).

235. *Id.* § 220(c).

even then, a number of these disputes are negotiated outside of the courtroom, either following the initial demand or after a stockholder seeks a court order to compel inspection.[236] Accordingly, a number of inspection demands are handled extra-judicially and would not trigger the exemption for compliance with other laws or court orders.[237]

In sum, books-and-records inspection rights are an area rife for conflict between a corporation's disclosure of data and privacy statutes' requirements. Given the continual expansion—both in terms of use of the right and disclosure of information—in this area of corporate law, the interplay of these two obligations will need to be addressed. Ironically, these very same inspection rights that exist in tension with consumer privacy rights can also be a key tool for shareholders to monitor a corporation's compliance with the requirements in privacy statutes.

III. PATHS FORWARD

In light of the conflicts examined above that arise from certain corporate disclosure activities and consumer data privacy requirements, this Section discusses two different options for navigating and reconciling these competing legal obligations. First, a legislative fix to consumer data privacy statutes is proposed. This remedy is particularly apt for state and federal legislatures who are considering but have not yet adopted privacy statutes.[238] Second, this Section provides a framework for courts to use in analyzing the conflict between already-adopted state privacy rules and corporate disclosure obligations. This framework of analysis aims to maintain the policy goals underlying each area of the law as well as the reasonable expectations of participants in the corporate enterprise.

A. Legislative Remedy

As an initial matter, it is important to point out that, in an era where the private ordering of shareholder rights is flourishing, the protections

236. "[M]any shareholder demands for documents do not lead to litigation. Knowledgeable Delaware attorneys say that once a shareholder makes a request for books and records, it is far more common for companies to produce some documents than to reject the investors' demand and force them to file a lawsuit." Cox, Martin & Thomas, *supra* note 222, at 25 n.104 (citing Kevin Shannon, Corporate Litigation Partner, Potter Anderson Corroon LLP, Address at the Trending Developments: Dealing with Books and Records Inspection Demands at the Third Annual Symposium on Corporate Law (Oct. 12, 2018)). *See* Min & Krischik, *supra* note 221, at 232 (noting that companies may be willing to freely give certain books and records without a fuss). The likelihood of extra-judicial disclosure for inspection demands is in part a result of the shareholder-friendly burdens of proof when seeking to obtain corporate documents. *See* Del. Code Ann. tit. 8, § 220(c) (putting the burden on the corporation to show an improper purpose related to stock list requests); Bucks Cnty. Emp.'s Ret. Fund v. CBS Corp., C.A. No. 2019-0820-JRS, 2019 WL 6311106, at *5 (Del. Ch. Nov. 25, 2019) (stating that § 220 imposes the "lowest burden of proof known in [Delaware] law").

237. *See, e.g.*, Cox, Martin & Thomas, *supra* note 222, at 25 n.104.

238. Of course, states that have already adopted consumer privacy statutes could also take advantage of this remedy through amendments to their existing statutes.

afforded under consumer privacy statutes cannot be similarly addressed.[239] Stated another way, a corporation is unable to address conflicts with consumer privacy statutes through a contract with shareholders or a provision in the entity's organizational documents. This is because consumer privacy statutes typically provide that contracts or agreements purporting to waive or limit the rights or remedies thereunder are deemed void and unenforceable as a matter of public policy.[240] Accordingly, a statutory fix to avoid the conflict in the first place is needed.

The definition of *consumer* is the primary source of the conflict with corporate law. Drafted with broad strokes, most of the current state privacy statutes would apply to shareholders, and California's statute also captures employees, directors, and officers within its terms.[241] Careful statutory drafting can, however, avoid the inclusion of these internal corporate participants. In contrast to California, there are two general approaches privacy laws take to narrow the definition of *consumer*. The majority approach is to exclude individuals acting in a "commercial or employment context" which would not exclude shareholders.[242] The minority approach, on the other hand, provides for a narrower definition of *consumer* which lends itself to excluding shareholders.[243] The Montana Consumer Data Privacy Act is an example of this approach. The Act's definition excludes:

> [A]n individual acting in a commercial or employment context or as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit, or government agency.[244]

Accordingly, directors and officers are expressly excluded from the Act.[245] While the Montana Act (and the other states that have similar language) does not define *owner*, shareholders are generally referred to as owners of

---

239. *See* Megan Wischmeier Shaner, *Interpreting Organizational "Contracts" and the Private Ordering of Public Company Governance*, 60 Wm. & Mary L. Rev. 985, 985 (2019) [hereinafter Shaner, *Interpreting Organizational "Contracts"*] (discussing the expansion of corporate contracting rights under Delaware law); Megan Wischmeier Shaner, *Corporate Resiliency and Relevancy in the Private Ordering Era*, 2022 Colum. Bus. L. Rev. 804, 804 (2022) [hereinafter Shaner, *Corporate Resiliency*] (discussing Delaware corporate law's endorsement of the private ordering of corporate governance rights).

240. *See, e.g.*, Cal. Civ. Code § 1798.192 (West 2022) ("Any provision of a contract or agreement of any kind, including a representative action waiver, that purports to waive or limit in any way rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable.").

241. *See supra* notes 91–95 and accompanying text (discussing the CCPA's broad definition of consumer).

242. *See* Table 2.

243. *See id.*

244. Mont. Code Ann. §§ 30-14-2802(6)(b) (2023). Connecticut, Delaware, Maryland, Rhode Island, and New Hampshire have similar definitions of consumer. *See, e.g.*, Conn. Gen. Stat. Ann. § 42-515(8) (West 2022); Del. Code Ann. tit. 6, § 12D-102(8) (West, Westlaw through 2023–2024 Sess.); R.I. Gen. Laws § 6-48.1-2(10) (2024).

245. *See* Mont. Code Ann. § 30-14-2802(6)(b).

a corporation and thus it can be argued that they are excluded from the definition of *consumer*.[246] However, in light of disagreement over whether shareholders truly own the corporation in which they hold shares of stock, or rather only own an equity interest in the corporation, future privacy statutes should add to the Montana model and include a definition of *owner* that makes clear that shareholders would fall under this term.[247] Alternatively, shareholders could be added to the list of excluded individuals from the definition of *consumer*.

Finally, it is important to note that the Montana definition recognizes that individuals may wear many hats—at times they are acting in a shareholder or director capacity and at other times in an individual consumer capacity. Accordingly, the statute makes clear that the excluded individuals are only excluded to the extent that they are acting in the enumerated excluded roles.[248] Thus, to the extent that an employee, owner, director, or officer of a company was not acting in their official capacity but in their individual, personal capacity, they would be considered a *consumer* and protected by the statute.[249]

B. Judicial Analysis

As more and more state consumer data privacy statutes become effective, it is only a matter of time before the courts will have to wrestle with the impact of these statutes on corporate disclosure activities. The first step in analyzing whether disclosure of director, officer, or shareholder information violates a privacy statute is determining whether or not the disclosure was made to an internal participant in the corporation.[250] Because all of the disclosure activities occurring under state corporate law would involve

246. *See* Charles R.T. O'Kelley, Robert B. Thompson & Dorothy S. Lund, Corporations and Other Business Associations 152 (Wolters Kluwer 2022) ("Corporate ownership interests are represented by shares. . . . Thus, holders of those shares are the corporation's risk bearers and residual claimants.").

247. *See* Lynn Stout, The Shareholder Value Myth: How Putting Shareholders First Harms Investors, Corporations, and the Public (2012) (arguing that shareholders do not own the corporation); Martin Lipton, Comments at American Enterprise Institute Roundtable, Was Milton Friedman Right About Shareholder Capitalism? (Oct. 6, 2020) (transcript available at https://petergeorgescu.com/wp-content/uploads/2021/07/MLipton_ColumbiaAEI.docx.pdf [https://perma.cc/T8TC-F3M5]) ("I don't view the shareholders as outright owners of the corporation in the way one would own a house or a car. They're investors in the corporation and own the equity, and they are thus important constituents, but they are not the owners of the corporation as a whole."). While California's statute defines owner to include stock ownership, it limits the definition to those shareholder who have a controlling stake or influence. *See* Cal. Civ. Code § 1798.145(m)(2)(E) (West 2022). The proposal here would define owner not based on a percentage of stock ownership, rather holding one share of stock would be considered an owner.

248. *See* Mont. Code Ann. § 30-14-2801(6)(b) (stating that only those "communications or transactions with the controller [that] occur solely within the context of that individual's role [as an employee, owner, director, officer or contractor] with the company, partnership, sole proprietorship, nonprofit, or government agency").

249. *See id.* § 30-14-2802.

250. *See, e.g.*, *id.*

internal corporate actors, this analysis will focus only on that situation.[251] It is important to note, however, that the following analysis would not necessarily apply in the same manner for disclosure of data to parties outside of the corporation.

While some of the state consumer privacy statutes provide exemptions for compliance with federal, state, and local laws as well as court orders and subpoenas, not all do.[252] Further, as discussed above, a major area where the disclosure of corporate information could run afoul of consumer data privacy statutes, even if they contain such an exemption, is books-and-records demands, in particular where such demands are settled extrajudicially.[253] So how should a court analyze a conflict between the requirements of a state consumer privacy statute and corporate disclosures to internal corporate actors? The answer lies in the cornerstone of recent corporate private ordering caselaw—implied consent.

Courts and scholars have long described a corporation's organizational documents, together with the state corporate code, as a "flexible contract" (1) between the State and the corporation, (2) between the corporation and its shareholders, and (3) among a corporation's shareholders.[254] When an individual or entity invests in a corporation through the purchase of shares of stock, they are assenting to be bound by the terms of this flexible contract.[255] Accordingly, courts have held, for example, that shareholders have implicitly consented to be bound by changes to the bylaws or charter of the corporation that impact their rights, even if done unilaterally by the board.[256]

---

251. It should be noted that corporations frequently disclose information regarding their directors, officers, and shareholders to federal regulators and agencies such as the Securities and Exchange Commission. *See, e.g.*, 15 U.S.C. § 78p(a). This disclosure is usually pursuant to federal law requirements and thus is exempted from most state privacy statutes. *See supra* note 216 and accompanying text (discussing California's exemption for compliance with federal, state, or local laws).

252. *See, e.g.*, Cal. Civ. Code § 1798.145(a)(1)(A) (West 2022).

253. *See supra* Part II.C.

254. *See* Boilermakers Local 154 Ret. Fund v. Chevron Corp., 73 A.3d 934, 955–56 (Del. Ch. 2013); Airgas, Inc. v. Air Prods. & Chems., Inc., 8 A.3d 1182, 1188 (Del. 2010); Centaur Partners, IV v. Nat'l Intergroup, Inc., 582 A.2d 923, 928 (Del. 1990); *see also* Shaner, *Interpreting Organizational "Contracts"*, *supra* note 239, 989–90.

255. *See Boilermakers*, 73 A.3d at 955–56; Bamford v. Penfold, L.P., C.A. No. 2019-0005-JTL, 2020 WL 967942, at *23 (Del. Ch. Feb. 28, 2020) ("A share of stock represents a bundle of rights defined by the laws of the chartering state and the corporation's certificate of incorporation and bylaws.").

256. *See, e.g.*, *Boilermakers*, 73 A.3d at 956 ("Such a change by the board is not extracontractual simply because the board acts unilaterally; rather it is the kind of change that the overarching statutory and contractual regime the stockholders buy into explicitly allows the board to make on its own."); *see also* Kidsco Inc. v. Dinsmore, 674 A.2d 483, 492 (Del. Ch. 1995) (rejecting the argument that shareholders have a vested right in the bylaws where the corporation's organizational documents make clear that they may be amended at any time); Jill E. Fisch, *Governance By Contract: The Implications for Corporate Bylaws*, 106 Calif. L. Rev. 373, 376 (2018); William Meade Fletcher, Fletcher Cyclopedia of the Law of Corporations § 4176 (updated 2023) ("It is presumed that a person who becomes a shareholder in, or a member of, a corporation does so with knowledge and implied assent that its bylaws may be amended." (citations omitted)).

A similar line of analysis can be applied to a corporation's disclosure of information pursuant to a statutory books-and-records demand or other corporate disclosure activities. Through their purchase of stock, shareholders have assented to a contractual framework that includes information rights.[257] Stated another way, shareholders have consented to a statutory regime that allows for the sharing of their information with other internal corporate participants—officers, directors, and other shareholders.[258] This disclosure of the information is thus necessary for the contractual relationship established under corporate law and does not run afoul of the policy concerns underlying state consumer privacy statutes.[259] Indeed, this reasoning has found footing in the judicial analysis of state privacy law's cousin, the GDPR. While the GDPR differs from U.S. state privacy statutes in some of its requirements, it is based on the same framework and policy and has the same basic rights and protections.[260] Recently, a German court found that the "GDPR does not prohibit a company from disclosing to one company shareholder, information identifying other shareholders in the same company."[261] In reaching this conclusion, the court discussed how the disclosure of the information is necessary for shareholders to exercise their rights within the corporation.[262] By comparison, the GDPR is stricter in its protective requirements than state privacy laws.[263] Thus, if courts, in analyzing the GDPR, have recognized this implied consent to disclosure as not violating the GDPR, a strong argument can be made that the same rationale should hold for state privacy statutes.

CONCLUSION

It is no secret that "[d]ata is the engine of a significant part of today's economy, and the [2024] state and federal legislative landscape promises more attention on privacy and data security."[264] From 2021 to 2023, there was a 103% increase in the number of comprehensive consumer data privacy bills considered across the states.[265] And 2024 looks to be on pace to exceed

257. *See, e.g.*, *Boilermakers*, 73 A.3d at 956 ("In other words, the Chevron and FedEx stockholders have assented to a contractual framework established by the DGCL and the certificates of incorporation that explicitly recognizes that stockholders will be bound by bylaws adopted unilaterally by their boards.").

258. *See id.*

259. *See id.*

260. *See generally supra* Section I.A.

261. Kagan, *supra* note 39.

262. *See id.* ("The purpose of the contract is essentially the exercise of the shareholders' rights, in particular also through the mutual exchange, the exercise of control and, if necessary, the merger of the co-partners, the strengthening of the position of the shareholders. Insight into the composition of the shareholders and the resultant power relations is useful and necessary for each shareholder. This also includes the possibility of influencing them, if necessary through the purchase of company shares.").

263. *See supra* Section I.A.

264. Sheila A. Millar & Tracy P. Marshall, *The State of U.S. Privacy Laws: A Comparison*, Nat'l L. Rev. (May 24, 2022), https://www.natlawreview.com/article/state-us-state-privacy-laws-comparison [https://perma.cc/LMV3-5YTA].

265. *See supra* notes 82–83 and accompanying text (discussing state legislative activity regarding consumer data privacy since 2018).

the prior years' statistics.[266] To date, twenty states have adopted consumer data privacy statutes.[267] Sweeping in nature, these consumer data privacy laws "broadly apply to nearly every aspect of [entities'] day-to-day business operations."[268] As more and more of these statutes become effective, it is only a matter of time before courts will have to resolve clashes between corporate disclosure obligations and consumer privacy requirements.

The proposed remedies in this Article seek to avoid or, at a minimum, ameliorate the tensions growing between consumer privacy law and corporate law. First, state consumer privacy legislation is at a critical juncture. As more and more states and the federal government move forward in drafting and proposing data privacy laws, it is important that they keep these competing interests and obligations in mind. Second, this Article provides a framework for the courts that will have to navigate legal challenges involving the conflicting obligations of state privacy and corporate laws.[269] In both instances, this Article provides paths forward that preserve much needed data security and privacy to consumers without negatively impacting efficient corporate law disclosure activities and governance.[270]

266. *See US State Privacy Legislation Tracker 2024*, Int'l Ass'n Priv. Pros., https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf [https://perma.cc/M9XU-SF4B].

267. *See US State Privacy Legislation Tracker*, Int'l Ass'n Priv. Pros., https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf [https://perma.cc/R2ZX-TUF4].

268. Allison Grande, *What to Watch As Congress Mulls Federal Privacy Legislation*, Law360 (Feb. 25, 2019), https://www.law360.com/articles/1132337/what-to-watch-as-congress-mulls-federal-privacy-legislation [https://perma.cc/8CR7-S2QU].

269. *See supra* Section III.

270. *See id.*