2021

Catalyzing Privacy Law

Anupam Chander
Georgetown University Law Center

Margot E. Kaminski
University of Colorado Law School

William McGeveran
University of Minnesota Law School

Article

Catalyzing Privacy Law

Anupam Chander,[†] Margot E. Kaminski,[††] and William McGeveran[†††]

† Professor of Law, Georgetown University Law Center; J.D., Yale Law School; B.A., Harvard University.

†† Associate Professor of Law, University of Colorado Law School; Director, Privacy Initiative, Silicon Flatirons Center. J.D., Yale Law School; B.A., Harvard University.

††† Associate Dean for Academic Affairs and Julius E. Davis Professor of Law, University of Minnesota Law School. J.D., New York University Law School; B.A., Carleton College.

The authors are grateful for insightful comments by students in the Technology Law Colloquium at Georgetown and the Law and Economics Workshop at Minnesota, by professors and students at Cardozo School of Law, and by professors at faculty workshops at Loyola, Villanova, and William & Mary law schools and at the 2019 Privacy Law Scholars Conference hosted at Berkeley Law. We thank in particular William Buzbee, Laura Dickinson, Roger Ford, Lydia de la Torre, Meg Jones, Christina Mulligan, Orla Lynskey, Paul Ohm, Neil Richards, and Joris van Hoboken. We also thank our superb editors at the *Minnesota Law Review*, especially Matthew Cavanaugh, Alina Yasis, and Melanie Griffith. Anupam Chander gratefully acknowledges a Google Research Award for related research. William McGeveran gratefully acknowledges funding by the Wargo Research Scholar Fund. We received excellent research help from Shiwen Cai, Lydia Davenport, Xinge He, Anna Kvinge, Romina Montellano Morales, Paige Papandrea, Caroline Schmitz, and librarian Heather Casey. The views herein (and all errors) are the authors' alone.

INTRODUCTION

When the General Data Protection Regulation (GDPR) took effect in May 2018, it positioned the European Union as the world's privacy champion.[1] A flurry of emails updating privacy policies landed in inboxes across the globe, attesting to the international reach of the European rule.[2] A month later, California enacted the California Consumer Privacy Act (CCPA), establishing the nation's most stringent omnibus privacy protections, effective as of January 1, 2020.[3] California, the home of many of the world's largest data-based enterprises,[4] emerged as a dark horse contender in the privacy regulator race. In the past year, state after state considered broad data privacy legislation,[5] and eleven comprehensive federal privacy bills were introduced in Congress.[6]

1. Adam Satariano, *G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. TIMES (May 24, 2018), https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html [https://perma.cc/24RK-ZMJV].

2. Brian Fung, *Why You're Getting Flooded with Privacy Notifications in Your Email*, WASH. POST (May 25, 2018, 3:15 PM), https://www.washingtonpost.com/news/the-switch/wp/2018/05/25/why-youre-getting-flooded-with-privacy-notifications-in-your-email [https://perma.cc/MGR2-XYGW].

3. *See* CAL. CIV. CODE §§ 1798.100–.199 (2018); Daisuke Wakabayashi, *Silicon Valley Faces Regulatory Fight on Its Home Turf*, N.Y. TIMES (May 13, 2018), https://www.nytimes.com/2018/05/13/business/california-data-privacy-ballot-measure.html [https://perma.cc/7XTE-3LU3].

4. Hank Tucker, *World's Largest Technology Companies 2020: Apple Stays on Top, Zoom and Uber Debut*, FORBES (May 13, 2020, 5:30 AM), https://www.forbes.com/sites/hanktucker/2020/05/13/worlds-largest-technology-companies-2020-apple-stays-on-top-zoom-and-uber-debut [https://perma.cc/L473-BYT3].

5. *See infra* Part III.B.1.

6. *See* Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019) (Sen. Maria Cantwell); Online Privacy Act of 2019, H.R. 4978, 116th Cong. (2019) (Rep. Anna Eshoo); Designing Accounting Safeguards To Help Broaden Oversight and Regulations on Data Act, S. 1951, 116th Cong. (2019) (Sen. Mark Warner); Do Not Track Act, S.

What is catalyzing U.S. privacy law? The conventional wisdom holds that Europe is setting the global standard for information privacy. There is much truth to this—some 142 countries and counting now have a broad data privacy law, typically modeled on the GDPR.[7] Scholars writing insightfully about the global race to information privacy have tracked the spread of data privacy laws across the world, noting Europe's influence on these developments.[8] In a recent article, Paul Schwartz observes that the European Union pioneered international privacy law to enable commerce among nations within the bloc itself.[9] He argues that other countries largely adopted the European

1578, 116th Cong. (2019) (Sen. Josh Hawley); Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019) (Sen. Edward Markey); Balancing the Rights of Web Surfers Equally and Responsibly (BROWSER) Act of 2019, S. 1116, 116th Cong. (2019) (Sen. Marsha Blackburn); Information Transparency & Personal Data Control Act, H.R. 2013, 116th Cong. (2019) (Rep. Suzan DelBene); Own Your Own Data Act, S.806, 116th Cong. (2019) (Sen. John Kennedy); Data Accountability and Trust Act, H.R. 1282, 116th Cong. (2019) (Rep. Bobby Rush); Social Media Privacy Protection and Consumer Rights Act of 2019, S. 189, 116th Cong. (2019) (Sen. Amy Klobuchar); American Data Dissemination (ADD) Act of 2019, S. 142, 116th Cong. (2019) (Sen. Marco Rubio); *see also* Data Care Act of 2018, S. 3744, 115th Cong. (2018) (Sen. Brian Schatz); Mind Your Own Business Act of 2019, S. 2637, 116th Cong. (2019) (Sen. Ron Wyden) (updating Sen. Wyden's 2018 Consumer Data Protection Act); Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act, S. 2639, 115th Cong. (2018) (Sen. Markey). In June 2020, Senator Sherrod Brown released the "Data Accountability and Transparency Act of 2020" as a discussion draft. Data Accountability and Transparency Act, SIL20719, 116th Cong (2020).

7. The exact number of countries with comprehensive data protection laws depends on one's characterization of any particular law and keeps changing as more countries adopt new laws. While Graham Greenleaf identifies 142 countries and jurisdictions with such laws, Graham Greenleaf & Bertil Cottier, *2020 Ends a Decade of 62 New Data Privacy Laws*, *in* 163 PRIV. L. & BUS. INT'L REP. 24, 24–25 (2020), the United Nations Conference on Trade and Development (UNCTAD) counts 128. *Data Protection and Privacy Legislation Worldwide*, U.N. CONF. ON TRADE & DEV., https://unctad.org/page/data-protection-and-privacy-legislation-worldwide [https://perma.cc/W47P-RHL2]. Most recent laws are modeled on the GDPR. *See, e.g.*, Nigeria Data Protection Regulation (2019), https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf. Among other differences, the Nigerian law permits fines up to two percent of global turnover, not the four percent permitted by the GDPR. *Compare id.* § 2.10(a), *with* General Data Protection Regulation 2016/679, art. 83(5), 2016 O.J. (L 119) 1, 83 [hereinafter GDPR].

8. *See, e.g.*, Graham Greenleaf, *Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels and New Delhi*, *25 May 2018* (U.N.S.W. L. Rsch. Series, Paper No. 18-56, 2018), https://ssrn.com/abstract=3184548.

9. Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 810 (2019) ("[The EU's] power in this regard first developed in response to issues that it faced internally. It needed to harmonize the data processing practices of EU member states. The inward-facing elements of EU data protection law then became an important factor in its adaptability to the rest of the world. Here is a global diffusion story

Union's data privacy model, reflecting its "success in the marketplace of ideas."[10]

Schwartz cites the CCPA as an example of Europe's success in spurring other jurisdictions to enact similar laws.[11] Journalists reporting on the CCPA's enactment, too, have frequently referred to it as "GDPR lite"[12] and "California's version of GDPR."[13] And as the push for federal legislation intensifies, many characterize it as a national response to the GDPR.[14]

This Article challenges this emerging consensus. Despite decades of European privacy law, the United States showed little appetite until now for broad privacy legislation.[15] Instead, norm entrepreneurs in California helped establish a new privacy framework that, as we show, differs significantly—and consciously—from the European model.[16] Our close comparison of the new California and European laws reveals that the CCPA is not simply GDPR-lite: it is both more and less demanding on various points.[17] It offers a fundamentally different regime for data privacy. And the numerous legislative proposals in state

that begins with a response to internal political considerations."); *see also* Michael D. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, 24 COMPUT. L. & SEC. REP. 508, 510 (2008).

10. Schwartz, *supra* note 9, at 818.

11. *Id.* at 816 ("Ideas matter. Even though the adequacy requirement provides an impressive fulcrum for international influence, the global success of EU data protection is also attributable to the sheer appeal of high standards for data protection. This appeal cannot alone be explained by the force of EU market power or even specific EU negotiating strategies. To illustrate, this Article can point to an example from the United States, namely, the enactment of the California Consumer Privacy Act (CCPA) of 2018."). Global legal convergence can indeed be the result of normative agreement. *See, e.g.*, Anupam Chander & Randall Costa, *Clearing Credit Default Swaps: A Case Study in Global Legal Convergence*, 10 CHI. J. INT'L L. 639, 640 (2010) (arguing that in the wake of the 2008/2009 financial crisis, the United States and Europe "converged on a similar clearing structure largely because of its compelling logic").

12. *See, e.g.*, Kayvan Alikhani, *Regulatory Disruption: Is Your Business Ready To Comply with the CCPA?*, FORBES (June 6, 2019, 9:15 AM), https://www.forbes.com/sites/forbestechcouncil/2019/06/06/regulatory-disruption-is-your-business-ready-to-comply-with-the-ccpa [https://perma.cc/Y56A-BDRE].

13. *See, e.g.*, George P. Slefo, *Marketers and Tech Companies Confront California's Version of GDPR*, ADAGE (June 29, 2018), https://adage.com/article/digital/california-passed-version-gdpr/314079 [https://perma.cc/U7M7-7BKN].

14. *See, e.g.*, Elizabeth Schulze, *The US Wants To Copy Europe's Strict Data Privacy Law—but Only Some of It*, CNBC (May 23, 2019, 1:16 AM), https://www.cnbc.com/2019/05/23/gdpr-one-year-on-ceos-politicians-push-for-us-federal-privacy-law.html [https://perma.cc/3KEP-JXBQ].

15. *See infra* note 20 and accompanying text.

16. *See infra* Part II.

17. *See infra* Part II (comparing the GDPR and the CCPA).

houses show greater fealty to California's model than to the European antecedent.[18] Bills pending before Congress reflect pressure not from Brussels, but from Sacramento.

Thus, California has emerged as a kind of privacy superregulator, catalyzing privacy law in the United States. Rather than the supranational EU, the subnational state of California—and, more specifically, a small network of determined individuals within that state—is now driving privacy in a significant part of the world. The emergence of the CCPA demonstrates the central role of local networks and norm entrepreneurship, contesting on the ground of what we call "data globalization."[19]

We are thus witnessing a paradigm shift in the policy conversation around data privacy law. Until now, the rules of transatlantic privacy rested on awkward negotiated mechanisms to transfer data between two seemingly irreconcilable regimes.[20] Now we are witnessing what might be characterized as a regulatory race on both sides of the ocean.[21]

This Article is the first to critically evaluate the relationship between California's privacy law, Europe's data protection regulation, and possible future state and federal privacy law.[22] This study is also of practical interest, answering questions for individuals and

18. *See* sources cited *supra* note 6.

19. *See* discussion *infra* Part III.C (explaining how data globalization helped propel the CCPA to its current status).

20. *See* Directive 95/46/EC, 1995 O.J. (L 281) 31 (establishing pre-GDPR rules regulating the processing and movement of personal data); PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 1–2 (1996) (comparing European countries' comprehensive data protection laws to other countries' less thorough laws). *But see* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 281–82 (2011) (arguing that the regimes are more similar than different in practice); *see also* William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 1025 (2016) (demonstrating similarities in enforcement between different data privacy regimes despite differences in the law on the books).

21. *See, e.g.*, Sara Merken, *States Follow EU, California in Push for Consumer Privacy Laws (1)*, BLOOMBERG L., https://news.bloomberglaw.com/privacy-and-data-security/states-follow-eu-california-in-push-for-consumer-privacy-laws-1 (Feb. 6, 2019, 3:02 PM).

22. The focus of our study is on regulation of the data protection practices of private parties, rather than on the protection of privacy against intrusions by the state—on the regulation of "surveillance capitalism" rather than on more traditional state surveillance. *See* Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 75 (2015) (defining "surveillance capitalism" as a "new form of information capitalism [that] aims to predict and modify human behavior as a means to produce revenue and market control").

businesses alike: For businesses, whose laws should I follow? For individuals, who will protect my privacy? Studying these questions leads, in turn, to another set of inquiries about the ways in which catalysis from the GDPR and CCPA govern privacy outside either Europe or California. When Europe's laws meet California's, who wins? If indeed European or Californian regulation will be applied globally de facto, why then should anyone else legislate?

The answers to all of these questions have implications not only for the shape of information privacy law but for understanding interjurisdictional regulatory dynamics in the digital economy. While data shares some characteristics with cars, pollution, and corporate charters—all the subject of prior globalizations of legal compliance and legal rules[23]—it also differs because of its simultaneous and instantaneous global effects. Data disobeys borders and operates at Internet speed. Equally important, the answers to these questions shed light on the prospects of countries across the world as they vie for advantage in the information age. Ultimately, our account of privacy catalysis tests the operation of both federalism and international regulatory competition in the twenty-first century.

Our analysis proceeds as follows. Part I situates our discussion of regulatory catalysis in data privacy within the broader frame of the theory of regulatory competition, borrowing lessons from areas such as corporate and environmental law. Part II compares the substance of the GDPR and the CCPA and the ways in which their structures promote catalysis in other jurisdictions. Part III turns to the race for data privacy law. We are the first to disentangle the catalytic effects on U.S. federal and state laws coming from both Brussels and Sacramento and to show that the resulting proposals are distinctly American and owe a greater debt to the CCPA than to the GDPR. As it once did with pioneering environmental regulation, California has emerged as a superregulator again, this time with respect to data in the information age.

I. SUPERREGULATORS

U.S. privacy law can be periodized as pre-CCPA and post-CCPA. Until the CCPA, no state or federal statute in the United States imposed privacy protections across all industry sectors and technologies in the manner that European data protection law had done for decades. Ever since the CCPA, Congress and state legislatures across the country

23. *See generally, e.g.*, Robert V. Percival, *The Globalization of Environmental Law*, 26 PACE ENV'T L. REV. 451 (2009).

have been considering huge numbers of data privacy proposals of that scope.[24]

What is prompting this new interest in comprehensive data privacy law in the United States? Many point to the EU's GDPR. After all, the GDPR went into effect in May 2018 to much fanfare. Countries around the world changed their laws to conform more closely with the GDPR, drawn by hopes of achieving a finding of "adequacy," which would facilitate their data trade with European economies.[25] The GDPR also prompted global companies to establish expensive compliance programs and infrastructure.[26] It makes sense, at first glance, to think that Europe has, through the GDPR, driven U.S. states and the federal government to take privacy seriously at last. If so, this development would fit neatly with the larger phenomenon that is sometimes called the "Brussels Effect."[27]

But if this is the case, why did it take so long? Anu Bradford coined the phrase back in 2012,[28] and the EU promulgated its original data protection directive in 1995.[29] If European law prompted soul-searching among American lawmakers, its voyage across the Atlantic proved quite slow.

This Part summarizes overlapping theories of regulatory competition and catalysis, drawn from varied subject matter areas, including corporate and environmental law. In all of these domains, early claims of a race to the bottom spurred by globalization have been challenged by scholars who suggested alternative regulatory dynamics that might lead to a race to the top or a race to the optimum.[30] Often these effects are named for the places where they were first detected: Delaware,

24. *See supra* note 6 (listing recent data privacy bills considered by Congress).

25. Schwartz, *supra* note 9, at 783–86.

26. *See* Mehreen Khan, *Companies Face High Cost To Meet New EU Data Protection Rules*, FIN. TIMES (Nov. 19, 2017), https://www.ft.com/content/0d47ffe4-ccb6-11e7-b781-794ce08b24dc.

27. Mark Scott & Laurens Cerulus, *Europe's New Data Protection Rules Export Privacy Standards Worldwide*, POLITICO (Jan. 31, 2018, 12:00 PM), https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation [https://perma.cc/2RWQ-X4WB].

28. Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 23 (2012) (describing spread of EU-style privacy protections in the wake of the EU's 1995 Data Protection Directive).

29. Directive 95/46/EC, 1995 O.J. (L 281) 31.

30. *See, e.g.*, Ralph K. Winter, Jr., *State Law, Shareholder Protection, and the Theory of the Corporation*, 6 J. LEGAL STUD. 251, 254 (1977) ("[C]ompetitive legal systems should tend toward optimality so far as the shareholders' relationship to the corporation is concerned.").

California, or Brussels.[31] In different ways, these three jurisdictions have emerged as "superregulators." Later in the Article we will consider which of these superregulator effects have catalyzed data privacy rules across the United States.

A. THE DELAWARE EFFECT

Regulatory competition has been investigated in the greatest depth in corporate law.[32] An early view argued that corporations would charter themselves in the most permissive state, leading U.S. states to compete with each other to offer ever more lax corporate law.[33] Some dubbed this the "Delaware Effect,"[34] because two-thirds of all Fortune 500 companies are incorporated in that state.[35]

A critical legal rule made regulatory competition possible. State laws defer to a corporation's decision on its state of incorporation—known as the "internal affairs" doctrine.[36] Thus, a corporation operating principally in California or Kansas can incorporate in Delaware and be assured that relations between its shareholders, directors, and officers will be governed by Delaware law.[37] Without this "internal affairs" rule, a corporation might have to conform to the corporate law

31. *See infra* Parts I.A–C.

32. *See, e.g.*, William L. Cary, *Federalism and Corporate Law: Reflections upon Delaware*, 83 YALE L.J. 663 (1974).

33. Justice Louis Brandeis explained the liberalization of corporate law through this dynamic:

> Lesser States, eager for the revenue derived from the traffic in charters, had removed safeguards from their own incorporation laws. Companies were early formed to provide charters for corporations in states where the cost was lowest and the laws least restrictive. . . . The race was one not of diligence but of laxity.

Liggett Co. v. Lee, 288 U.S. 517, 557–59 (1933) (citations omitted).

34. *See, e.g.*, Bradford, *supra* note 28, at 5.

35. *See* DEL. DIV. OF CORPS., ANNUAL REPORT STATISTICS (2018), https://corpfiles.delaware.gov/Annual-Reports/Division-of-Corporations-2018-Annual-Report.pdf [https://perma.cc/8BRQ-QFLX]. And this does not apply only to large, established corporations: in 2017, over eighty percent of initial public offerings in the United States used Delaware as a corporate home. *Id.*

36. Rogers v. Guar. Tr. Co. of N.Y., 288 U.S. 123, 130 (1933) ("It has long been settled doctrine that a court—state or federal—sitting in one State will as a general rule decline to interfere with or control by injunction or otherwise the management of the internal affairs of a corporation organized under the laws of another State but will leave controversies as to such matters to the courts of the State of the domicile."); VantagePoint Venture Partners 1996 v. Examen, Inc., 871 A.2d 1108, 1112 (Del. 2005) ("The internal affairs doctrine is a long-standing choice of law principle which recognizes that only one state should have the authority to regulate a corporation's internal affairs—the state of incorporation.").

37. *See VantagePoint Venture Partners 1996*, 871 A.2d at 1112.

of all of the jurisdictions in which it operates. The internal affairs doctrine thus allows a company to establish a single regulator for the corporate law affairs of the corporation.[38]

The classic analyses posited that Delaware had cornered the market for incorporations through dubious efforts to favor corporate officers and directors.[39] Ralph Winter famously rejected this claim of an inevitable race to the bottom, arguing that corporate leaders were not in fact free to choose the most permissive jurisdiction because shareholders would penalize them for failing to maximize shareholder value.[40] Where some had derided Delaware's efforts as "law for sale,"[41] Roberta Romano argued that Delaware's efforts were part of the genius of American law.[42] Instead of seeking to race to the bottom to attract corporate charters, Delaware courts, for their part, saw their role as providing special corporate law expertise.[43] Regulatory

38. With respect to corporate law, the European Union did not embrace a similar approach to that in the United States until recently. Rather than deferring to the state of incorporation, many EU states sought to establish where the "real seat" of the corporation lay. Werner F. Ebke, *The Real Seat Doctrine in the Conflict of Corporate Laws*, 36 INT'L L. 1015, 1015–16 (2002). Such an approach would not defer to the mailbox incorporation available in Delaware. *See id.* This rule would still typically result in a single regulator—but this would make gaming the law more difficult. Matthew G. Dore, *Déjà Vu All Over Again? The Internal Affairs Rule and Entity Law Convergence Patterns in Europe and the United States*, 8 BROOK. J. CORP. FIN. & COM. L. 317, 317–18 (2014). One would actually have to locate one's headquarters (the management and control center) in the jurisdiction with the friendliest laws, rather than simply fill out some forms to incorporate via a mailbox. Recent EU caselaw has, however, moved towards the U.S. internal affairs rule, deferring to the jurisdiction of the state of incorporation. *Id.* at 325–29. This opens up the possibility of regulatory competition for corporate law in Europe as well.

39. Cary, *supra* note 32, at 672. According to this view, states such as Delaware might wish to attract incorporations because of the franchise tax—the annual fees corporations pay to maintain their incorporation in that state. Indeed, Delaware has come to fund one-quarter of its budget through this means. STEPHEN M. BAINBRIDGE, CORPORATE GOVERNANCE AFTER THE FINANCIAL CRISIS 24 (2012) ("Delaware generates $740–800 million per year in franchise taxes, which amounts to a quarter of the state's budget."); DEL. OFF. OF MGMT. & BUDGET, FINANCIAL OVERVIEW (2018), https://budget.delaware.gov/budget/fy2018/documents/operating/financial-overview.pdf [https://perma.cc/R7KY-9YK6] (estimating franchise taxes of "$975.0 million for Fiscal Year 2017 and $992.6 million for Fiscal Year 2018").

40. Winter, *supra* note 30, at 257 ("If management is to secure initial capital . . . it must attract investors away from the almost infinite variety of competing opportunities.").

41. *E.g.*, Editors, Comment, *Law for Sale: A Study of the Delaware Corporation Law of 1967*, 117 U. PA. L. REV. 861 (1969).

42. ROBERTA ROMANO, THE GENIUS OF AMERICAN CORPORATE LAW 37–39 (1993).

43. As one Delaware Chancery Court judge noted, "Delaware has a substantial interest in providing an effective forum for litigating disputes involving the internal

competition, seen from this perspective, can occur not just through the content of the governing rules but also through the quality of their adjudication.

The Delaware Effect therefore can be summarized as the emergence of certain jurisdictions as highly influential overseers of particular behavior based on proactive elections made by regulated entities—an opt-in to a particular jurisdiction. If enough regulated entities make the same choice, that jurisdiction may come to dominate the field. Both the substantive law and the regulatory techniques of a jurisdiction may then gain influence outside its borders as other regulators defer to it.[44] While this arrangement could result in a race to the bottom, it could also enable the emergence of highly specialized expert regulatory oversight that then becomes the standard to which other jurisdictions defer.

B. THE CALIFORNIA EFFECT

David Vogel famously challenged a similar hypothesis of a race to the bottom in environmental regulation and consumer protection law. Where many argued that international trade would inevitably lead to the erosion of consumer and environmental regulation, Vogel countered that "under certain circumstances, global economic integration can actually lead to the strengthening of consumer and environmental standards."[45] Instead of a race to the bottom (what he, adopting the traditional view, called a "Delaware Effect") he offered that regulatory competition might result in a "California Effect."[46] This outcome hinged on "the critical role of powerful and wealthy 'green' political

affairs of Delaware corporations." *In re* Activision Blizzard, Inc., 86 A.3d 531, 547 (Del. Ch. 2014). For support for this statement, Vice Chancellor Laster cited Roberta Romano's book *The Genius of American Corporate Law*: "'The most important transaction-specific asset in the chartering relation is an intangible asset, Delaware's reputation for responsiveness to corporate concerns,' which stems from 'a comprehensive body of case law, judicial expertise in corporation law, and administrative expertise in the rapid processing of corporate filings.'" *Id.* at 547 n.7 (citing ROMANO, *supra* note 42, at 38–39).

44. *See, e.g.*, Dore, *supra* note 38, at 325–29 (describing the EU's shift toward the internal affairs rule).

45. David Vogel & Robert A. Kagan, *Introduction: National Regulations in a Global Economy*, *in* DYNAMICS OF REGULATORY CHANGE 1, 1 (David Vogel & Robert A. Kagan eds., 2004); DAVID VOGEL, TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY 5 (2004) ("To the extent that trade liberalization has affected the level of consumer and environmental protection, it has more often strengthened than weakened it.").

46. VOGEL, *supra* note 45, at 5–8.

jurisdictions in promoting a regulatory 'race to the top' among their trading partners."[47]

Unlike the Delaware Effect, in which a jurisdiction tempts companies to opt into its regulatory scheme and other jurisdictions then defer to that one's expertise, the California Effect occurs when one jurisdiction pushes other jurisdictions to improve their own laws.[48] This race to the top is de jure in nature, rather than de facto or deferential; other jurisdictions pass laws that mimic the superregulator jurisdiction.

Vogel identified three conditions under which a California Effect might occur.[49] First, a race to the top is more likely to be triggered if the standards are supported by a coalition of public interest groups with regulated companies that wish to impose the regulatory costs they face on their competitors in other, more lax jurisdictions.[50] Second, the superregulator must have a large market that is sufficiently attractive that companies would rather absorb the cost of regulation than forego the market.[51] Third, a race to the top is more likely to occur if there is a strong institution capable of harmonizing standards across jurisdictions, such as the U.S. federal government or the EU.[52]

The classic example of the California Effect is California's emissions regulations for automobiles. As Ann Carlson explains, from the mid-1960s onward, the state pioneered strong tailpipe emissions standards.[53] When Congress amended the Clean Air Act to preempt state standards for emissions, it grandfathered in "any state" that had emissions controls in place prior to March 30, 1966—a standard applicable only to California, as lawmakers understood perfectly well.[54] The Clean Air Act of 1970 explicitly recognized California as a superregulator: it became the only state allowed to set stricter-than-federal standards, and other states could then opt to follow California's standards.[55] Twelve eastern states and the District of Columbia announced

47. *Id.* at 6.

48. *See id.* at 5–8.

49. *Id.* at 260–68; *see also* Sebastiaan Princen, *Trading Up in the Transatlantic Relationship*, 24 J. PUB. POL'Y 127, 128 (2004) (discussing Vogel's proposed conditions).

50. VOGEL, *supra* note 45, at 260–61.

51. *Id.* at 261–63.

52. *Id.* at 263–68.

53. Ann E. Carlson, *Iterative Federalism and Climate Change*, 103 NW. U. L. REV. 1097, 1111 (2009).

54. *Id.*

55. *See* Rocky Mountain Farmers Union v. Corey, 730 F.3d 1070, 1078–79 (9th Cir. 2013) ("Other states could choose to follow either the federal or the California standards, but they could not adopt standards of their own."); Carlson, *supra* note 53,

in 1994 that they would follow California.[56] Auto emissions rules illustrate all three of Vogel's conditions: a coalition of public interest groups alongside regulated companies, a superregulator with a large and attractive market, and a strong institution (the federal government) capable of harmonizing standards.

The mechanism of the California Effect differs from the Delaware Effect. Under the Delaware Effect, other jurisdictions defer to the regulatory choices of the superregulator, magnifying the impact of those choices.[57] Under the California Effect, other jurisdictions themselves adopt the same rules as the superregulator jurisdiction.[58]

C. THE BRUSSELS EFFECT

In the late twentieth century, as the authority and institutions of the European Union grew, another superregulator emerged: Brussels, the seat of the EU bureaucracy. As Anu Bradford vividly describes it: "Few Americans are aware that EU regulations determine the makeup they apply in the morning, the cereal they eat for breakfast, the software they use on their computer, and the privacy settings they adjust on their Facebook page. And that's just before 8:30 AM."[59]

Where the California Effect depends on jurisdictions racing to strengthen their regulations in response to each other, the Brussels Effect operates principally as a de facto mechanism, when market actors conform their global products to European rules.[60] Bradford observes, "[T]he Brussels Effect is more about one jurisdiction's ability to override others than it is about triggering an upward race."[61]

---

at 1134 (noting California's special status); Nicholas Bryner & Meredith Hankins, *Why California Gets To Write Its Own Auto Emissions Standards: 5 Questions Answered*, CONVERSATION, https://theconversation.com/why-california-gets-to-write-its-own-auto-emissions-standards-5-questions-answered-94379 [https://perma.cc/H7U4-CLJQ]. In 2019, the EPA and NHTSA formally withdrew California's Clean Air Act waiver. Coral Davenport, *Trump To Revoke California's Authority To Set Stricter Auto Emissions Rules*, N.Y. TIMES (Sept. 20, 2019), https://www.nytimes.com/2019/09/17/climate/trump-california-emissions-waiver.html [https://perma.cc/QCL6-TDZ6].

56. Peter P. Swire, *The Race to Laxity and the Race to Undesirability: Explaining Failures in Competition Among Jurisdictions in Environmental Law*, 14 YALE L. & POL'Y REV. 67, 82 (1996).

57. *See supra* Part I.A.

58. *See supra* notes 47–50 and accompanying text.

59. Bradford, *supra* note 28, at 3 (citations omitted).

60. *See id.* ("Unilateral regulatory globalization occurs when a single state is able to externalize its laws and regulations outside its borders through market mechanisms, resulting in the globalization of standards.").

61. *Id.* at 8.

Why might a corporation change its practices outside Europe, adopting stricter codes absent legal compulsion? Bradford explains, "[M]ultinational corporations often have an incentive to standardize their production globally and adhere to a single rule."[62] Of course, sometimes these enterprises do decide to observe different regulatory regimes in different locations. Just as Vogel distilled the conditions for a California Effect, Bradford identifies circumstances under which a Brussels Effect is more likely to occur.[63] First, as with the California Effect, the Brussels Effect is likely to occur only when the unilateral regulator represents a large and attractive market.[64] Second, that superregulator must have significant regulatory capacity, through which it tends to aim strict rules at "inelastic targets" such as consumer markets, thus creating rules that can't be readily evaded.[65] Third, the operations of the firm must be "nondivisible," meaning that it is less costly for a firm to comply with the one higher standard worldwide than to set up different compliance standards.[66]

Unlike the effects named for Delaware and California, the Brussels Effect depends on the choices of the entities subject to regulations, not those of governments or regulators.[67] Indeed, if organizations decide to obey a particular jurisdiction's requirements in all their activities, then that jurisdiction will gain influence even if other jurisdictions might strongly prefer a different rule, so long as the superregulator's demands do not actually violate the law in other places.

While the literature names certain cross-jurisdictional effects after particular superregulators who are especially likely to cause them, it is a mistake to overinterpret these names. As we shall see, superregulators can affect other jurisdictions in various ways.[68] So, for example, when other nations adopt new data protection laws to harmonize their rules with those in the EU, this is a California Effect that happens to emanate from Brussels. When websites began posting globally applicable privacy policies partly in response to a 2003 California statute requiring they do so,[69] this was a Brussels Effect triggered by a California law. We will delve into these catalytic effects in privacy law

62. *Id.* at 6.

63. *Id.* at 10–19; *see also* Schwartz, *supra* note 9, at 780–83 (discussing and applying Bradford's factors).

64. Bradford, *supra* note 28, at 11–12.

65. *Id.* at 12–17.

66. *Id.* at 17–19.

67. *See supra* Parts I.A–B; Bradford, *supra* note 28, at 48–49.

68. *See infra* Part III.

69. California Online Privacy Protection Act of 2003, CAL. BUS. & PROF. CODE §§ 22575–22579 (2018).

more fully below.[70] First, however, we explain the substance of the GDPR and the CCPA, demonstrating in the process both their overlaps and differences and revealing the emergence of California as a contender to be a data privacy superregulator.

II. GDPR VERSUS CCPA

Which data privacy regime is driving the wave of legislative activity related to data privacy across the United States, and what is the mechanism of that influence? To answer this question, we need first to understand the two regimes. This Part reveals both similarities and differences between the GDPR and the CCPA. After all, if the CCPA can be described as a copy of the GDPR, then even if we can show that state legislators and Congress are copying California, Schwartz and others would be correct that the European Union is the ultimate source behind new U.S. privacy proposals.[71] But if, as we argue, the CCPA is a fundamentally different regime—only similar to the GDPR at the surface, while lacking major structural elements of the GDPR—then the question of who the superregulator is becomes one with meaningful consequences for understanding all these federal and state proposals.[72]

A paperback of the GDPR runs some 130 pages, its sections literally divided into chapters.[73] The CCPA, by contrast, is around 25 pages.[74] The two laws were also written on vastly different timelines. If the GDPR is a doctoral thesis, the CCPA is a term paper written the night before the deadline.[75]

In this Part, we compare the two regimes, addressing where they apply, whom they cover, and what they require. We also address differences in the regulatory style, enforcement mechanisms, and legal

70. *See infra* Part III.

71. *See supra* notes 7–14 and accompanying text.

72. *See supra* note 6 (listing data privacy bills proposed in Congress in 2019 and 2020).

73. Eur. Union, *European Data Protection Law: General Data Protection Regulation 2016*, AMAZON, https://www.amazon.com/European-Data-Protection-Law-Regulation/dp/1533170835 [https://perma.cc/2JW7-YDHP].

74. *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–.199 (2018).

75. *Compare* Katelyn Ringrose & Jeremy Greenberg, *California Privacy Legislation: A Timeline of Key Events*, FUTURE PRIV. F. (Aug. 31, 2020), https://fpf.org/blog/california-privacy-legislation-a-timeline-of-key-events [https://perma.cc/C6NC-WVZR], *with* Adam Deakin, *GDPR Timeline: A History of Data Protection*, VUTURE, https://vutu.re/blog/gdpr-timeline--a-history-of-data-protection.aspx [https://perma.cc/2JS2-SHS7].

settings of the GDPR and the CCPA. This understanding of the two systems sets up our analysis in Part III, where we consider the influence of the new European and Californian laws across the United States.

A. EUROPEAN DATA PROTECTION VERSUS U.S. CONSUMER PROTECTION

First, it helps to understand the fundamental differences between a U.S.-style and an EU-style data privacy regime. When discussing data governance, European lawyers do not even use the same language as American lawyers; they refer to statutes that govern the handling of personal data as "data protection" laws, not "privacy" laws.[76] This reflects a fundamental difference in approach: "data protection" is universal in Europe, while most American law focuses on "consumer protection."[77] Data protection laws like the GDPR proceed from the principle that data protection is a fundamental human right safeguarded through constitutional protections in the European Convention on Human Rights and the EU Charter.[78] This places data protection rights on the same plane as free speech or due process.[79] As a result, the default in Europe is that personal information cannot be collected or processed unless there is a specific legal justification for doing so.[80]

In the United States, by contrast, privacy law most often follows a "consumer protection" model, with regulators focused on ensuring that consumers receive the benefit of their bargain in individual business-to-consumer transactions.[81] The consumer protection model frequently relies on the much-criticized premise that disclosure and a right of refusal (so-called "notice and choice") adequately empower

76. *See* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 138, 147 (2017); *see also* CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION 2–3 (2d ed. 2007); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1159–60 (2004); Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 909–10 (2009); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 500–01 (1995).

77. McGeveran, *supra* note 20, at 966 ("[D]ata protection law begins with an assumption that control over personal information is a human right. . . . U.S. regulators, such as the FTC or state attorneys general, regulate privacy by policing the fairness of particular transactions.").

78. Charter of Fundamental Rights of the European Union, arts. 7–8, 2000 O.J. (C 364) 11; Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

79. Charter of Fundamental Rights of the European Union, *supra* note 78, arts. 7, 11.

80. *See id.* art. 8.

81. *See* McGeveran, *supra* note 20, at 966.

consumers.[82] Unlike in Europe, there is no protection in the U.S. Constitution against activities by nongovernmental entities,[83] including the collection of personal data. And unlike a data protection regime, in which protections follow the data, the consumer protection model focuses on governing both a more discrete interaction and a more direct relationship. Until the CCPA, most American law permitted entities to collect and use personal data however they wished by default, absent a specific legal rule forbidding a particular practice.[84]

A second difference between Europe and the United States is that U.S. privacy law has always been fragmented and "sectoral."[85] Different statutes are enforced by different regulators in different sectors such as health care, financial services, education, or credit reporting. A few of these sectoral regimes are constructed like data protection rules, but they apply only within their narrow domains.[86] Most U.S. laws function on the transactional consumer protection model described above. As a final backstop, general-purpose consumer protection regulators, such as the Federal Trade Commission (FTC) and state attorneys general, address a subset of cases falling outside any sectoral rules, again largely following a consumer protection model.[87]

By contrast, in every European nation, specialized data protection regulators have long enforced omnibus statutes applicable to all organizations when they handle any personal data.[88] While these data protection laws contain extra protections for especially sensitive

82. *See, e.g.*, WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 62–67 (2018); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1930 (2013).

83. *See* DeShaney v. Winnebago Cnty. Dep't of Soc. Servs., 489 U.S. 189, 195–96 (1989) ("[N]othing in the language of the Due Process Clause itself requires the State to protect the life, liberty, and property of its citizens against invasion by private actors.").

84. *See* Schwartz & Peifer, *supra* note 76, at 147.

85. *See* Reidenberg, *supra* note 76, at 505–06; Schwartz, *supra* note 76, at 908–13.

86. Health Insurance Portability and Accountability Act, 45 C.F.R. §§ 160, 162, 164 (2020); Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506.

87. Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 748 (2016); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 590 (2014); *see also* McGeveran, *supra* note 20, at 977–78 (describing the "cleanup role" of consumer protection regulators in enforcement of U.S. privacy law).

88. Charter of Fundamental Rights of the European Union, *supra* note 78, art. 8 ("Everyone has the right to the protection of personal data concerning him or her."); Consolidated Version of the Treaty on the Functioning of the European Union art. 16(1), Oct. 26, 2012, 2012 O.J. (C 326) 47 ("Everyone has the right to the protection of personal data concerning them.").

information, their basic human rights frameworks impose uniform requirements every time personal data is collected, processed, or transferred.[89] These rules apply through sweeping definitions of "data controllers" and "data processors" that encompass not only businesses of every size and type but also governments, nonprofit organizations, political campaigns, and even individuals—anyone engaged in the "processing" of personal data.[90]

B. SUBSTANTIVE SIMILARITIES

At first glance, the CCPA may seem more "European" than existing U.S. privacy laws. True, it is the first U.S. statute that has some data protection characteristics without being narrowly sectoral. For example, under the CCPA, legal protections follow personal data, regardless of whether an individual has a direct relationship with the regulated company.[91] This differs from many existing regulatory models in the United States. Because the FTC's general consumer protection authority focuses only on the relationship between individuals and companies, it claims to have little power over data brokers who obtain individual information from other companies or public sources rather than from consumers themselves.[92] The CCPA, by contrast, regulates

89. The European Commission's review of the operation of the GDPR at its second anniversary noted that the EU member states had not offered as much uniformity in their local implementations of the GDPR as might be desired. *Communication from the Commission to the European Parliament and the Council: Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation*, at 12, COM (2020) 264 final (June 24, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264 [https://perma.cc/HSY9-LCUU].

90. GDPR, *supra* note 7, art. 4(2) (defining "processing" as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"); *see* Case C-40/17, Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW e.V., ECLI:EU:C:2019:629 (July 29, 2019) (holding Facebook jointly responsible as a data controller when a third-party website uses a Facebook "Like" button that facilitates user tracking). The first European Court of Justice case dealing with the GDPR's predecessor, the Data Protection Directive, involved a criminal charge against an individual who had posted (seemingly innocuous) information about fellow parishioners to a webpage without their consent. Case C-101/01, Lindqvist v. Åklagarkammaren i Jönköping, 2003 E.C.R. I-12971.

91. CAL. CIV. CODE § 1798.105(d) (Deering 2018).

92. U.S. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/TR62-497D].

data brokers directly—a critical move targeting an industry that has an enormous impact on individuals' privacy.[93]

Some core elements of the CCPA also seem to echo aspects of the GDPR. Both laws define personal information very broadly, far beyond most existing U.S. privacy laws.[94] Both laws foundationally emphasize transparency, reflecting the Fair Information Principles on which many data privacy regimes in both Europe and the United States are built, and both laws share the contours of a number of additional individual rights.[95]

In the past, narrow definitions of personal information have sharply limited the effect of many U.S. privacy laws.[96] Under most U.S. laws, only certain types of information counted as personal data, making the definition limited, technical, and static. The GDPR and CCPA both break with this past by using the real-world potential for identifiability as the touchstone. The GDPR's broad and open definition of personal data includes not just information that directly identifies a person, but also information that renders a person identifiable.[97] The CCPA similarly applies to information that is "capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[98] Both laws provide expansive and open lists of examples of covered personal information, from IP addresses to biometric information.

Another similarity between the GDPR and the CCPA is the central role of transparency. Transparency is a core principle of the GDPR.[99] The GDPR's recitals proclaim it a fundamental tenet of data protection law that people should know that personal data has been collected and be able to understand the extent to which that information is processed.[100] The CCPA likewise focuses on giving people notice and

93. JULIA ANGWIN, DRAGNET NATION 7 (2014) ("Stalkers and rogue employees have consistently found ways to abuse these databases."). The federal Fair Credit Reporting Act, a narrow sectoral statute, does regulate some segments of the data broker industry, but largely within the context of business relationships among credit reporting agencies and the lenders or employers who rely on their products. 15 U.S.C. § 1681.

94. *See* GDPR, *supra* note 7; CAL. CIV. CODE § 1798.

95. GDPR, *supra* note 7; CAL. CIV. CODE § 1798.

96. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814 (2011).

97. GDPR, *supra* note 7, art. 4(1).

98. CAL. CIV. CODE § 1798.140(o)(1).

99. GDPR, *supra* note 7, art. 5(1)(a).

100. *Id.* recital 39.

access rights so that they can trace what is happening to their personal information. The California legislature's articulated intent for the CCPA was to give consumers "an effective way to control their personal information" by giving them "[t]he right . . . to know what personal information is being collected about them," and "[t]he right . . . to know whether their personal information is sold or disclosed and to whom."[101]

Beyond this hortatory language, both laws embed transparency principles in their requirements. Under the GDPR, organizations must provide individuals both notice and access.[102] They must affirmatively provide detailed general notice that includes the purpose of data processing, the recipients of the data, the period for which the data will be stored, and other information.[103] Organizations that collect personal information from a third party must also provide such notice,[104] and all these disclosures must be clear and intelligible.[105]

The GDPR also establishes a right of individual access,[106] building on "subject access rights" that have been in place throughout Europe at least since the 1990s under the Data Protection Directive.[107] In response to an individual's access request, data controllers must disclose, among other things: the purposes of processing, the categories of personal information concerned, the recipients of personal data, retention or storage time, and the source of the data if they have not been collected from the individual.[108] Additionally, they must provide a copy of the data itself in a commonly used electronic form.[109]

The CCPA likewise gives individuals both notice and access rights. Like the GDPR, it requires companies to disclose the purpose of processing, categories of information gathered, and the existence of individual rights with respect to that data (it does not, however, require disclosure of the precise identities of the recipients of the data or the storage period).[110] Such disclosures, according to regulations

101. *See* Assemb. 375, 2018 Leg. § 2(i) (Cal. 2018).

102. GDPR, *supra* note 7, arts. 13–14.

103. *Id.*

104. *Id.* art. 14(1)(d).

105. *Id.* art. 12.

106. *Id.* art. 15.

107. Jef Ausloos & Pierre Dewitte, *Shattering One-Way Mirrors—Data Subject Access Rights in Practice*, 8 INT'L DATA PRIV. L. 4, 4–28 (2018).

108. GDPR, *supra* note 7, art. 15.

109. *Id.* art. 15(3); *see also id.* recital 63 ("Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data.").

110. CAL. CIV. CODE § 1798.185 (2018); CAL. CODE REGS. tit. 11, § 999.305 (2020).

promulgated by California's attorney general, must be "designed and presented in a way that is easy to read and understandable to consumers."[111] The CCPA goes well beyond notice requirements in prior U.S. law, such as a California statute requiring websites to post privacy policies.[112]

Like the GDPR, the CCPA also gives individuals access rights. The statute creates a right for consumers to request both the categories and specific pieces of personal information that a business has collected.[113] Consumers have a right to request disclosure of the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, and the categories of third parties with whom the business shares personal information.[114] Unusually for a U.S. law, the rules apply not just to companies that have a direct relationship with the consumer, but also to companies that collect and sell personal information even if they obtain that information from somebody other than the consumer.[115] CCPA access rights represent a significant advance from very limited rights under previous law, such as access to credit scoring information and the annual free credit report.[116]

The two regimes share, too, the core elements of a number of additional individual rights (though they differ in the details): data portability, opt-out rights, a duty of nondiscrimination, and a right to deletion or erasure. The GDPR contains a right to data portability—that is, a right to receive one's personal data in a format that enables an individual to switch service providers.[117] This right is aimed at giving individuals more control over their data and more choices about IT services[118] but is also understood to potentially enhance competition.[119] The CCPA quietly creates a data portability "right" of its own: personal data delivered electronically in response to an access request "shall be

111. CAL. CODE REGS. tit. 11, § 999.305(2).

112. CAL. CIV. CODE § 22575 (Deering 2014).

113. *Id.* §§ 1798.100(a), .110(a); CAL. CODE REGS. tit. 11, §§ 999.300(q), .308(c)(1), .318.

114. CAL. CIV. CODE § 1798.110(a).

115. Under the CCPA, consumers can request access to certain information from (a) a business that collects personal information and (b) a business that sells personal information or discloses it for a business purpose. *Id.* §§ 1798.100(a), .110(a), .115(a).

116. 15 U.S.C. § 1681(g).

117. GDPR, *supra* note 7, art. 20, recital 68; ARTICLE 29 DATA PROT. WORKING PARTY, GUIDELINES ON THE RIGHT TO DATA PORTABILITY (2017).

118. ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 117, at 3–4.

119. *Id.* at 4.

in a portable and . . . readily usable format."[120] In fact, the CCPA's data portability "right" may be broader than the GDPR's in some ways, as it applies to inferred data about an individual, where the GDPR's right does not.[121]

Both the CCPA and the GDPR contain a right for individuals to "opt out" and deny permission for handling of their personal data in certain ways. The CCPA establishes an opt-out right for consumers to tell a business not to sell their personal information.[122] If a business has actual knowledge that a consumer is sixteen years old or younger, it must obtain affirmative authorization ("opt-in") for any sale of personal information—from the individual themselves if they are between thirteen and sixteen years old or from a parent or guardian if the individual is under thirteen years old.[123] The GDPR, by comparison, establishes three analogous rights: the right to restrict data processing,[124] the right to object to data processing,[125] and the right to withdraw consent.[126] Although the GDPR has broader rights to opt out—they apply well beyond the sale of information—they are also less absolute than those in the CCPA.[127]

Both regimes contain a duty of nondiscrimination: companies cannot "discriminate" against individuals who choose to exercise rights related to personal data.[128] This means that a business cannot, for example, deny goods or services, charge different rates, impose

120. CAL. CIV. CODE § 1798.100(d).

121. ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 117, at 10; CAL. CIV. CODE § 1798.140(o), (*l*), (k), (m).

122. CAL. CIV. CODE § 1798.120. Vermont's new data broker law, H. 764, requires transparency as to whether a data broker allows consumers to opt out of collection or sale of information but does not require a data broker to do so. *See* VT. STAT. ANN. tit. 9, § 2430 (2019).

123. CAL. CIV. CODE § 1798.120(d).

124. GDPR, *supra* note 7, art. 18.

125. *Id.* art. 21, recitals 60, 70.

126. *Id.* art. 7(3).

127. *Id.* art. 2(1). There is also a balancing test specific to scientific or historical research purposes or statistical purposes. *Id.* art. 21(6).

128. CAL. CIV. CODE § 1798.125; GDPR, *supra* note 7, recital 42; EUR. DATA PROT. BD., GUIDELINES 05/2020 ON CONSENT UNDER REGULATION 2016/679 ¶ 48 (2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf [https://perma.cc/PK3G-F7MP] (giving as an example of "consent without detriment" that a company may "show that a service includes the possibility to withdraw consent without negative consequences e.g. without the performance of the service being downgraded to the detriment of the user"); CAL. CODE REGS. tit. 11, § 999.336(a) (2020) ("A financial incentive or a price or service difference is discriminatory, and therefore prohibited . . . if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations.").

penalties, or provide a different level of services to customers who opt out of data transactions. The CCPA regulations, however, contemplate a compensation scheme whereby a business can offer financial incentives or a price or service difference if they are "reasonably related to the value of the consumer's data."[129] This changes the duty of nondiscrimination in at least some circumstances from an absolute duty into an information-forcing mechanism regarding how companies value consumer data.[130]

The GDPR famously contains a right to erasure, also known as the "right to be forgotten."[131] The CCPA creates a more limited right to deletion.[132] The GDPR's right to erasure gives individuals the right to obtain the erasure of personal data both from companies with which they have a direct consumer relationship and from third parties, under certain circumstances.[133] There are exceptions to the right to erasure, including freedom of expression and public interest in the area of public health.[134] As many have noted, this so-called "right to be forgotten" is not absolute but is in large part a balancing test between competing values, outsourced to private companies.[135] The CCPA creates a much narrower right to deletion. Unlike the GDPR's right to erasure, which applies to third parties, the CCPA's right to deletion applies only to businesses that collect information directly from the consumer.[136]

129. CAL. CODE REGS. tit. 11, § 999.336(b).

130. *See id.* § 999.337.

131. GDPR, *supra* note 7, art. 17. *See generally* MEG LETA JONES, CTRL + Z: THE RIGHT TO BE FORGOTTEN (2016).

132. CAL. CIV. CODE § 1798.105 (2018).

133. GDPR, *supra* note 7, art. 17(1)(a)–(f) (permitting an individual to exercise the right to erasure in circumstances including, but not limited to, when the personal data is no longer necessary for the purpose it was originally collected or processed for, the individual withdraws their consent where the organization relied on said consent as the lawful basis of processing, or when the individual objects to the processing of their data for direct marketing purposes).

134. *Id.* art. 17(3)(a), (c).

135. *See* CHRISTINA ANGELOPOULOS, ANNABEL BRODY, WOUTER HINS, BERNT HUGENHOLTZ, PATRICK LEERSSEN, THOMAS MARGONI, TARLACH MCGONAGLE, OT VAN DAALEN & JORIS VAN HOBOKEN, INST. FOR INFO. L., STUDY OF FUNDAMENTAL RIGHTS LIMITATIONS FOR ONLINE ENFORCEMENT THROUGH SELF-REGULATION 52 (2015), https://scholarlypublications.universiteitleiden.nl/access/item%3A2869513/view [https://perma.cc/AAM8-UABW]; *see also* Case C-131/12, Google Spain SL v. AEPD, ECLI:EU:C:2014:317, 16–22 (May 13, 2014); Edward Lee, *Recognizing Rights in Real Time: The Role of Google in the EU Right To Be Forgotten*, 49 U.C. DAVIS L. REV. 1017 (2016); Stefan Kulk & Frederik Zuiderveen Borgesius, Case Note, *Google Spain v. González: Did the Court Forget About Freedom of Expression?*, 5 EUR. J. RISK REGUL. 389, 389–98 (2014).

136. CAL. CIV. CODE § 1798.105(a).

This more restricted scope is an accommodation of First Amendment law and values in the United States, which may constrain erasure requirements imposed on third parties.[137]

In sum, the CCPA moves closer to a data protection regime like the GDPR in certain ways, which helps explain the widespread assumption that it represents a U.S. embrace of the European-style data protection model. While the CCPA's broad definition of personal data, emphasis on transparency, and establishment of some individual rights do go further than previous U.S. law, none of these shifts go nearly as far as the GDPR. As we shall see in the next Section, these similarities are overshadowed by fundamental substantive differences between the two models.

C. SUBSTANTIVE DIFFERENCES

Once an analysis moves beyond these similarities, it becomes clear that the CCPA regime differs sharply from the GDPR. First, and perhaps most importantly, the two laws do not share the same underlying principles, leading to great differences in the scope and nature of the rights and duties imposed by each. Second, while the CCPA is broader than past American sectoral laws, it still regulates a much narrower set of entities than does the GDPR. Third, the two laws have different enforcement mechanisms. Fourth, their regulatory styles contrast, with significant practical and substantive consequences. And finally, California and Europe are each quite distinct in what we call their "legal setting"—the backdrop against which privacy laws exist and will develop over time. We consider each of these differences in order.

First and foremost, for all its moves toward broader coverage and the creation of individual rights, the CCPA does not treat privacy as a human right in the way data protection laws like the GDPR do.[138] It

137. Sorrell v. IMS Health, Inc., 564 U.S. 552, 557 (2011); *see* Anupam Chander & Uyên P. Lê, Free *Speech*, 100 IOWA L. REV. 501, 522 (2015) (arguing that *Sorrell* demonstrates "the seriousness of First Amendment constraints on privacy regulations on information intermediaries"). Cases such as *Florida Star v. B.J.F.*, 491 U.S. 524 (1989), *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975), and *Smith v. Daily Mail Publishing*, 443 U.S. 97 (1979), arguably suggest that once information is legally distributed, the government cannot restrict its use absent state interest of the highest order. However, a number of scholars argue that most privacy laws can pass First Amendment muster. *See, e.g.*, Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501 (2015); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016). *But see* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right To Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000).

138. *Compare* CAL. CIV. CODE § 1798.105, *with* GDPR, *supra* note 7, art. 1.

remains, in the American tradition, a transactional privacy law concerned with protecting *consumers* in their dealings with *commercial* entities. For this reason, the CCPA does not embrace several principles that have been at the core of constitutionally influenced European data protection law since long before the GDPR—back to its predecessor, the 1995 Data Protection Directive,[139] and back even further to national data protection laws in many European countries dating from the 1970s and 1980s.[140]

The GDPR is built around the concept of "lawful processing" of data. That is, personal data cannot be processed unless a data controller has obtained individual consent[141] or one of five other enumerated categories of lawful processing applies.[142] The CCPA does not require that processing be lawful.[143] Rather, it shares the presumption of most other American privacy law that personal data may be collected, used, or disclosed unless a specific legal rule forbids these activities.[144] This is likely the single most meaningful difference between the two regimes.

Moreover, the GDPR imposes multiple additional conditions on all data processing, even when it is authorized by consent or another of the legitimizing conditions.[145] The GDPR requires that personal data may be collected only for "specified, explicit and legitimate purposes," stated at the time of collection.[146] Additional principles include purpose limitation (processing data only for those previously stated purposes), data minimization (collecting no more data than necessary for those purposes), data retention (limiting storage of data to periods justified by those purposes), privacy by design, as well as privacy impact assessments for high risk data processing, among others.[147]

139. Directive 95/46/EC, 1995 O.J. (L 281) 31.

140. *See, e.g.*, Gesetz zum Schutz vor MiBbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG) [Law on Protection Against the Misuse of Personal Data in Data Processing (Federal Data Protection Act)], Jan. 27, 1977, BUNDESGESETZBLATT [BGBI] at 1 201 (W. Ger.); Loi 78-17 du 6 janvier 1978 de informatiqué et libertés [Law 78-17 of January 6, 1978 on Information and Civil Liberties], COMMISION NATIONALE DE L'INFORMATIQUÉ ET DES LIBERTÉS [COMMISSION ON INFORMATION TECHNOLOGY, DATA FILES AND CIVIL LIBERTIES] (Fr.); Data Protection Act 1984, c. 35 (U.K.).

141. GDPR, *supra* note 7, art. 6(1)(a).

142. *Id.* art. 6(1)(a)–(f).

143. CAL. CIV. CODE § 1798.100.

144. *Id.*

145. GDPR, *supra* note 7, art. 5(1).

146. *Id*. art. 5(1)(b).

147. *Id*. art. 5(1)(b)–(f).

The CCPA imposes few requirements concerning the purposes for data collection or the proportionality of data handling to those purposes. The CCPA's text does not even go as far as the Health Insurance Portability and Accountability Act (HIPAA), which requires that downstream disclosures of patient data be the "minimum necessary" to achieve a purpose.[148] Instead, the CCPA requires a business to provide notice if it is "collect[ing] personal information collected for additional purposes."[149] This rule on its face does not stop companies from using data for new purposes—it just requires disclosure if they do so. As in many other places, the CCPA's approach relies on transparency rather than following the GDPR by imposing substantive duties on companies that collect and process personal data. The implementing regulations promulgated by the California attorney general do require that a business "shall not use a consumer's personal information for a purpose materially different than those disclosed in the notice at collection."[150] If a business wishes to use personal information for a new, undisclosed, materially different purpose, it must obtain explicit consent from the consumer for that use. While this is more than mere transparency, it is far from the extensive conditions on all data processing in the GDPR.

The divergence in the two regimes' animating principles also influences their treatment of individual rights. The CCPA, apart from allowing individuals to opt out of sales of their personal data, affords individuals little control. It does nothing to enable individuals to refuse to give companies their data in the first place. The GDPR strives to do so by requiring stringent forms of consent in a number of circumstances[151] and by granting individuals robust rights throughout the life cycle of data processing, including the right to rectification of incorrect information;[152] the right to prevent automated individual decision-making and to receive explanation of any automated decision;[153] and broader rights related to erasure of data and withdrawal

148. 45 C.F.R. §§ 164.502(b), .514(d) (2021).

149. CAL. CIV. CODE § 1798.100(b) (2018).

150. CAL. CODE REGS. tit. 11, § 999.305(a)(5) (withdrawn July 29, 2020).

151. Regarding both particularly sensitive data (special categories of data) and automated decision-making, the GDPR requires the more stringent "explicit consent" if consent is to be the basis of processing. GDPR, *supra* note 7; ARTICLE 29 DATA PROT. WORKING PARTY, GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING AND PROFILING FOR THE PURPOSES OF REGULATION (2017).

152. GDPR, *supra* note 7, art. 16.

153. *Id.* art. 22; *see also* Margot E. Kaminski, *The Right to Explanation, Explained*, 34 BERKELEY TECH. L.J. 189, 201 (2019).

of consent.[154] Additionally, the GDPR's requirement of lawful processing bestows more individual control than the CCPA.[155] The CCPA relies primarily on transparency, and apart from access and notice rights, grants individuals only the two limited rights discussed above: to opt out of sale and to request deletion.[156]

Fundamentally, then, the CCPA is not a comprehensive European-style data protection regime. The GDPR quintessentially targets compliance from an organizational perspective: it attempts to build up a particular kind of responsible corporate infrastructure, including internal positions and processes.[157] The GDPR's affirmative regulatory requirements range from data minimization to risk assessments to recording requirements, and they are imposed on data collectors even where there is not a corresponding individual right.[158] The CCPA regulations require compliance training and record-keeping,[159] but overall appear to be geared more towards providing transparency into industry practices—in this case, how a company responds to consumer requests under the CCPA—than towards reinforcing good data practices or creating substantive protections for consumers. It remains to be seen if the GDPR will succeed in entrenching more privacy-protective corporate practices, but its aims are far broader, and approach far deeper, than the CCPA's.

A second difference between the GDPR and CCPA relates to regulated entities. As noted earlier, the GDPR covers anyone that processes personal data, including not only companies but also individuals, nonprofit organizations, and governments.[160] The CCPA applies only to businesses, and only to those that meet a complex set of overlapping requirements related to their size or the extent of their involvement in personal data trade.[161] Here again, the two laws reflect the

154. GDPR, *supra* note 7, art. 17.

155. *Id.* art. 6(1)(a).

156. CAL. CIV. CODE § 1798.120 (2018).

157. *See* Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529, 1596 (2019).

158. GDPR, *supra* note 7, art. 5(2); *see also* Kaminski, *supra* note 157.

159. CAL. CODE REGS. tit. 11, § 999.317 (2020).

160. GDPR, *supra* note 7, art. 2(1).

161. CAL. CIV. CODE §§ 1798.100, .105, .110, .115, .120. The CCPA targets three kinds of commercial entities as "businesses." *Id.* § 1798.140(c). It targets (1) larger businesses (with over twenty-five million dollars in annual gross revenue) that collect California residents' personal data, regardless of how many people are impacted by this collection; (2) for-profit businesses of any size that buy, receive, sell, or share personal information concerning a significant number of residents (50,000 or more); and (3) businesses that derive half or more of their annual revenues from selling personal information—regardless of their size or how many people are affected by this activity.

dominant approach on each side of the Atlantic. A data protection model inherently aims to be comprehensive. The CCPA, while broader than many sectoral U.S. privacy laws of the past, still limits its aim to protecting consumers from certain data handling practices within a specific context defined by commerciality, geography, and scale.

The regimes' respective enforcement mechanisms are a third area of divergence. Both provide for monetary penalties for non-compliance. The GDPR authorizes administrative fines issued by national data protection regulators of up to 4% of a company's annual worldwide revenue, while the CCPA includes civil penalties of up to $2,500 per violation or $7,500 per intentional violation, a number that can exact enormous sums when multiplied by the number of people affected in many privacy violations.[162] However, there is no private right of action for affected individuals to enforce most elements of the CCPA. This is in keeping with the trend for U.S. privacy laws of at least the last twenty years, including the FTC Act,[163] HIPAA,[164] and the Children's Online Privacy Protection Act (COPPA).[165] There have been proposals in the California legislature to authorize private CCPA lawsuits, but for now only the state attorney general may enforce most provisions of the law.[166] In Europe, a constitutionally guaranteed right of redress for violations of individual rights means the GDPR can be enforced by individual complaints.[167] While class actions are largely unfamiliar in European law, the GDPR does allow a claims representation model so that individuals do not have to file claims on their own behalf only. There is also a well-developed regulatory structure in the GDPR, with specialized data protection regulatory authorities in each EU country and coordination of their efforts through a European Data Protection Board.[168] Although the recently enacted California Privacy Rights Act (CPRA) establishes a new privacy-specific regulator,[169] there is no tradition of dedicated data protection regulators in the United States, which instead relies on agencies with numerous other

162. GDPR, *supra* note 7, art. 83; CAL. CIV. CODE § 1798.155(a)–(b).

163. Federal Trade Commission Act, 15 U.S.C. §§ 41–58.

164. Health Insurance Portability and Accountability Act, 45 C.F.R. § 160.203 (2002).

165. 15 U.S.C. §§ 6501–6506.

166. The CCPA does, however, authorize private lawsuits for a narrow set of claims related to data security breaches.

167. GDPR, *supra* note 7, arts. 77–79.

168. *Id.* arts. 51–59.

169. *See* Lydia de la Torre & Glenn Brown, *What Is the California Privacy Protection Agency?*, IAPP (Nov. 23, 2020), https://iapp.org/news/a/what-is-the-california-privacy-protection-agency [https://perma.cc/QL6A-CYDP].

obligations, including the FTC, state attorneys general, and sectoral regulators in areas such as health, banking, or education.

Fourth, the regulatory styles of the two regimes differ greatly. This can create both substantive and cultural gaps. The CCPA establishes limited but granular requirements that California's attorney general has fleshed out further in recently promulgated regulations.[170] The GDPR, on the other hand, consists of broad standards in its text and relies heavily on cooperation with companies and various forms of guidance (including the GDPR's Recitals, European Data Protection Board Guidelines, and interpretations from individual national data protection authorities) to fill in the details.[171] In other words, the GDPR's approach to regulation exemplifies collaborative governance, also known as "coregulation" or "new governance."[172] The GDPR's vagueness is arguably deliberate. EU authorities wanted to allow companies and sectors to fill in details of how to comply with the law over time, whether formally by establishing codes of conduct or certification mechanisms (although these have yet to materialize more than two years after the GDPR came into force),[173] or informally through self-regulation, recording and reporting, impact assessments, and ongoing conversations with regulators.[174] By contrast, the CCPA's granularity appears, in places, to value detail and certainty over adaptability.

For example, where the GDPR simply states that it requires clarity and intelligibility in its access and notice rights, the statutory text of the CCPA specifies that companies provide a toll-free telephone number and website address for consumers to make access requests.[175] For those businesses subject to the CCPA's opt-out, the CCPA mandates a clear and conspicuous link titled "Do Not Sell My Personal Information" and a description of the consumer's right to opt out of the sale of personal data.[176] The CCPA regulations go into even more detail about the precise mode and content required for notice at

170. *Final Text of Proposed Regulations*, *Cal. Code Regs. tit. 11, §§ 999.300–.337*, CAL. OFF. ATT'Y GEN., https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf [https://perma.cc/CT9M-4G7M].

171. *See* Kaminski, *supra* note 157; McGeveran, *supra* note 20.

172. *See, e.g.*, Jody Freeman, *Collaborative Governance in the Administrative State*, 45 UCLA L. REV. 1, 31 (1997); Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L. REV. 342, 349 (2004).

173. GDPR, *supra* note 7, arts. 40, 42.

174. *See* Kaminski, *supra* note 157; McGeveran, *supra* note 20.

175. CAL. CIV. CODE § 1798.130(a)(1) (2018).

176. CAL. CODE REGS. tit. 11, § 999.305(f)(1) (2020).

collection, notice of opt-out, notice of financial incentive, and privacy policies.[177] These examples demonstrate a stylistic difference between the two laws that could have real consequences for businesses trying to comply with both. For certain obligations, the CCPA and its regulations offer a clear, if inflexible, roadmap for compliance. Often, however, it is so detailed that it creates the possibility of divergence from the GDPR—even where in broad strokes the two laws might appear similar.

Finally, the backdrop against which these two privacy laws were enacted, or what we call their legal setting, differs significantly. While the CCPA is constrained by increasingly deregulatory First Amendment doctrine, the GDPR is backed by European courts that have increasingly recognized the importance of both privacy and data protection as fundamental rights.[178] In recent years, these courts have applied the right to be forgotten to search engines,[179] found the Data Retention Directive to violate fundamental rights,[180] and twice invalidated the primary mechanism for transferring data to the United States because of fears that American national security surveillance would trample on Europeans' rights.[181]

Crucially, European constitutional structures enforce affirmative rights against private conduct, not just against state actors as in the United States.[182] And, while European constitutional traditions safeguard the right to freedom of expression, it is usually balanced against other rights, and it can and does often lose out to constitutional data protection rights.[183] By contrast, the U.S. Supreme Court in recent years has interpreted free speech doctrine to restrict both data privacy regulations and other consumer protection disclosure regimes.[184] Some observers worry that the First Amendment is becoming an increasingly blunt tool, subjecting many regulations concerning

177. *Id.* §§ 999.305–.308.

178. Schwartz & Peifer, *supra* note 76.

179. Case C-131/12, Google Spain SL v. AEPD, ECLI:EU:C:2014:317, 22 (May 13, 2014).

180. Case C-293/12, Digit. Rts. Ir. Ltd. v. Minister for Commc'ns, Marine & Nat. Res., ECLI:EU:C:2014:238, 19 (Apr. 4, 2014).

181. Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, 10–31 (Oct. 6, 2015); Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd., ECLI:EU:C:2020:559 (July 16, 2020).

182. *See* Schwartz & Peifer, *supra* note 76, at 126, 155.

183. Alec Stone Sweet & Jud Mathews, *Proportionality Balancing and Global Constitutionalism*, 47 COLUM. J. TRANSNAT'L L. 73, 90–149 (2008); Bilyana Petkova, *Privacy as Europe's First Amendment*, 25 EUR. L.J. 140, 152 (2019).

184. *See infra* Part III.D.2.

privacy and other topics to often-fatal strict scrutiny.[185] Additionally, the Supreme Court has been skeptical of data privacy harms, in cases addressing both privacy damages and standing to sue.[186] The U.S. Constitution contains no explicit data privacy right, and the Fourth Amendment protects only against state action, not the actions of private parties.[187]

Overall, these five differences overshadow the similarities. Asserting that the CCPA is remotely equivalent to a data protection regime like the GDPR overstates the importance of a few resemblances. It is true that the CCPA departs from some common characteristics of previous U.S. privacy law and that it overlaps with some aspects of the GDPR. But the California law's motivations, mechanisms, scope, and legal setting keep it well within the consumer protection tradition of American privacy law. The question now is which of these two fundamentally different laws is catalyzing the recent legislative activity around privacy in Congress and state legislatures.

III. CATALYZING PRIVACY

The standard account of transatlantic privacy describes two fundamentally incompatible privacy regimes reflecting deep philosophical divides between legal cultures. According to this story, a laissez-faire approach to data privacy in the United States reflects broader liberal norms that prioritize individual autonomy in the face of big government, while the more interventionist EU approach reflects "social-protection norms" aimed at protecting human dignity.[188] Researchers (including one of us) have argued that this conventional wisdom oversimplifies matters by focusing on disparities in law-on-the-books and ignoring similarities in practices-on-the-ground.[189] Nonetheless, the EU and United States have been unable, or at least

185. *See, e.g.*, Margot E. Kaminski, *Privacy and the Right To Record*, 97 B.U. L. REV. 167, 173 (2017); Scott Skinner-Thompson, *Recording as Heckling*, 108 GEO. L.J. 125, 146 (2019); Richards, *supra* note 137, at 1524. *See generally* Amanda Shanor, *The New* Lochner, 2016 WIS. L. REV. 133.

186. *See* Doe v. Chao, 540 U.S. 614 (2004); FAA v. Cooper, 566 U.S. 284 (2012); Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013); Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016); Frank v. Gaos, 139 S. Ct. 1041 (2019).

187. Some state constitutions do, however, provide an explicit right to privacy, even against private parties. *See, e.g.*, CAL. CONST. art. 1, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending . . . privacy.").

188. *See* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1343 (2000); Whitman, *supra* note 76, at 1161.

189. Bamberger & Mulligan, *supra* note 20, at 260; McGeveran, *supra* note 20, at 960.

disinclined, to come to an international consensus on data privacy, instead forging *sui generis* and unstable bilateral arrangements governing data transfers between the two regimes.[190]

The CCPA and the GDPR herald a possible paradigm shift for data privacy. Rather than two fundamentally incompatible frameworks, one European and one American, we identify the emergence of a race between California and the European Union as regulatory catalysts, driving the U.S. states, and possibly the U.S. federal government, to enact new data privacy laws.[191]

This Part first outlines the argument that the GDPR has been the dominant influence on both de facto and de jure spread of privacy law worldwide. We argue that the United States represents an exception to this narrative—a narrative that largely, and in our view mistakenly, adheres to a notion of nation-states (and supranational entities) as unitary actors rather than considering the various players within them.[192]

We then examine a number of recently proposed and several recently enacted state and federal data privacy laws, aiming to answer the question: which jurisdiction is driving this race to propose and enact new privacy rules? We find that although the commonly accepted narrative credits new strong European rules as the driver,[193] in fact, the proposals in U.S. states have largely copied California. And although the CCPA does not always provide the substantive content for recently proposed federal legislation, it has been the impetus behind those bills. California, not Europe, is catalyzing the recent and ongoing development of U.S. data privacy law.

The story of the CCPA and its imitators, we argue, is not the commonly assumed story about the unilateral power of Brussels. It

190. *See* cases cited *supra* note 181.

191. Sara Merken, *States Follow EU, California in Push for Consumer Privacy Laws (1)*, BLOOMBERG L. (Feb. 6, 2019, 3:02 PM), https://news.bloomberglaw.com/privacy-and-data-security/states-follow-eu-california-in-push-for-consumer-privacy-laws-1.

192. *See, e.g.*, Harold Hongju Koh, *How Is International Human Rights Law Enforced?*, 74 IND. L.J. 1397, 1401–09 (1999) (contrasting five theories of how international human rights law is enforced: power, self-interest, liberal explanations, communitarian explanations, and legal process explanations—and noting the role of "transnational norm entrepreneurs" in legal process (in contrast to state-centric theories such as realism)); Anne-Marie Slaughter, *A Liberal Theory of International Law*, 94 AM. SOC'Y INT'L L. PROC. 240, 241 (2000) (describing liberal IR theory as "a view that preserves an important role for states but deprives them of their traditional opacity" in contrast to traditional IR theory, "which conceive[s] of the international system as composed of unitary, identical state actors with fixed preferences (the billiard ball model)").

193. *See supra* notes 10–14 and accompanying text.

demonstrates instead how networked individuals can harness processes at the state and local level to promote the adoption of new legal norms.[194] Rather than causing a race to the bottom, the backdrop of what we call "data globalization" both influences and empowers norm entrepreneurs advocating for stricter requirements.[195]

Why are other states now copying the CCPA? We posit a number of reasons. First, in an echo of the Delaware Effect, California may have established itself nationally as an expert jurisdiction on data privacy law, through both the CCPA and numerous earlier statutes regulating data privacy.[196] Second, since so many data-centered companies have a significant presence in California, other states may be presuming a California-driven "Brussels" Effect: that is, many companies already complying with the CCPA with respect to California residents would de facto comply with, or be readily able to comply with, CCPA-like requirements in other states. Third, state legislators motivated to enact privacy protections are far more likely to model their laws on a roughly twenty-page law from a U.S. jurisdiction than a foreign law consisting of 99 articles and 173 recitals.

We do not deny that the GDPR influenced the direction of American privacy law. It certainly reduced the costs of compliance with new American privacy law for multinationals that were already bringing themselves into compliance with the GDPR. The strong new European law also brought attention to the comparative deficit in U.S. law. But the effect from the EU has been more circumscribed than generally reported, and it is clearly secondary to a very real California Effect.

We will close Part III with some cautious predictions. We examine some of the countervailing forces unique to the United States that may contain the spread of privacy rules from one jurisdiction to the next, including the dormant commerce clause, the possibility of federal preemption, and the First Amendment. We hypothesize, however, that the spread of data privacy law in the United States will continue, with the CCPA as the new minimum threshold for protection. A new data privacy equilibrium is being established in the United States, whether it progresses state-by-state, encourages development of

194. *See supra* note 192.

195. For an argument of how to curtail the race to the bottom with respect to online service providers, see ANUPAM CHANDER, THE ELECTRONIC SILK ROAD: HOW THE WEB BINDS THE WORLD IN COMMERCE 166–69 (2013).

196. *See, e.g.*, CAL. BUS. & PROF. CODE § 22580 (California "Eraser Law" allowing minors the right to delete Internet content under certain circumstances); CAL CIV. CODE §§ 1798.80–.84 (California's pioneering data breach notification law); CAL. BUS. & PROF. CODE §§ 22575–22579 (California Online Privacy Protection Act of 2003, which required online privacy policies and other disclosures about handling of personal data).

model state legislation, results in a uniform federal law, or some combination of the above.

A. BRUSSELS AS THE WORLD'S PRIVACY CATALYST

As Paul Schwartz and others have observed, the GDPR is driving the enactment of new data privacy laws around the world.[197] This matches what we described in Part I as a (de jure) "California" Effect.[198]

The EU has strictly limited the export of personal data outside of the EU since the 1995 Data Protection Directive came into effect, and this policy continued in the GDPR.[199] Both the Directive and the GDPR allow crossborder transfers of personal data only in one of three ways. Two of the methods are cumbersome, requiring individual companies to go through complex, inflexible, and often bureaucratic processes to adopt either "binding corporate rules" or "model contract clauses."[200] The third method is the "adequacy mechanism," which operates on the national level instead of at the level of an individual organization. If the European Commission declares a foreign country's data protection laws and enforcement to offer an "adequate level of protection,"[201] then data can flow to any organization in that country with no further constraint. Because an adequacy ruling greatly simplifies data transfer in comparison to the more onerous options, many countries have sought to modify their laws to obtain such a ruling.[202]

The adequacy process can thus be characterized as a deliberate legal export strategy. By making it much easier for companies doing business in the EU to transfer data across borders if their home jurisdictions adopt data protection laws that satisfy European authorities, the EU deployed the Brussels Effect (de facto compliance) to cause a California Effect (de jure regulatory changes). As Schwartz cautions, the dynamic is more complicated in reality, because other jurisdictions have pushed back against the adequacy process, resulting in

197. *See generally* Schwartz, *supra* note 9, at 771 ("The cornerstone of EU law in this area, the General Data Protection Regulation (GDPR), is now widely regarded as a privacy law not just for the EU, but for the world.").

198. *See supra* Part I.B.

199. *See* GDPR, *supra* note 7, art. 45; Directive 95/46/EC, art. 25, 1995 O.J. (L 281).

200. GDPR, *supra* note 7, arts. 46–47 (describing binding corporate rules and standard contractual clauses, among other mechanisms); Directive 95/46/EC, art. 25 (outlining procedures for derogations from Article 25 limitations on cross-border transfers).

201. Directive 95/46/EC, art. 25(1).

202. *See* Schwartz, *supra* note 9, at 786–95 (comparing UK, Japan, U.S. and noting that Israel and others have received adequacy determinations).

more of a give-and-take than pure export.[203] But at the end of the day, the laws of other countries do look much more like EU law than they did before their adequacy determinations.

The GDPR also demonstrates a (de facto) Brussels Effect, spurring many multinational companies to comply with its provisions worldwide, even where other jurisdictions do not adjust their laws, and not only for operations dealing with European persons. Some enterprises decided to avoid GDPR exposure by excluding Europe altogether.[204] For example, the *Los Angeles Times* and the *Chicago Tribune* disabled access for Internet users in the EU.[205] National Public Radio took a different approach: "Users could either agree to the new terms, or decline and be taken to a plain-text version of the site, looking for all the world like it had last been updated in 1996."[206] Chinese smart-home manufacturer Yeelight disabled Internet-connected lightbulbs in the European Union.[207] For these firms, even the potential benefits of serving the huge European market could not justify the costs of compliance or the risks of non-compliance. And surely many smaller organizations disregard GDPR requirements because their exposure to Europe is minor.

Nonetheless, when the GDPR went into effect in May 2018, people across the world, including Americans, begin receiving a fusillade of messages from companies updating their privacy policies. Some companies have adopted the compliance infrastructure required in the GDPR—designating data protection officers, running impact assessments, baking in some form of privacy by design—throughout their international operations. Just as the scholarship on the Brussels Effect anticipates, these companies have found it desirable to maintain a unified firm-wide compliance architecture and adhered to the more

203. *Id.* (illustrating negotiations between the EU and external countries to allow personal data to flow freely between economies).

204. Rebecca Sentance, *GDPR: Which Websites Are Blocking Visitors from the EU?*, ECONSULTANCY (May 31, 2018), https://econsultancy.com/gdpr-which-websites-are-blocking-visitors-from-the-eu-2 [https://perma.cc/9A2Y-XEHA].

205. Alex Hern & Martin Belam, *LA Times Among US-Based News Sites Blocking EU Users due to GDPR*, GUARDIAN (May 25, 2018), https://www.theguardian.com/technology/2018/may/25/gdpr-us-based-news-websites-eu-internet-users-la-times [https://perma.cc/76J5-5G2C] (noting that U.S. papers such as the *New York Daily News*, the *Baltimore Sun*, *Orlando Sentinel*, and the *San Diego Union-Tribune* also disabled access).

206. Alex Hern & Jim Waterson, *Sites Block Users, Shutdown Activities and Flood Inboxes as GDPR Rules Loom*, GUARDIAN (May 24, 2018), www.theguardian.com/technology/2018/may/24/sites-block-eu-users-before-gdpr-takes-effect [https://perma.cc/4FYJ-PL5S].

207. *Id.*

stringent GDPR requirements. A few companies have gone even further by adopting aspects of the GDPR other than its compliance rules; Microsoft, for example, announced that it would "extend the rights that are at the heart of GDPR to all of our consumer customers worldwide."[208]

Through both the Directive and the GDPR, EU authorities successfully exported their approach to data protection to many places around the globe, both through national responses to the adequacy mechanism and institutional efforts to unify data compliance operations. But the influence of EU privacy law has been much more limited in other respects, starting with its capacity to catalyze legal change in the United States.

B. BUT SEE THE UNITED STATES

While the GDPR's adequacy mechanism and its direct effect on global companies may entice other jurisdictions worldwide to enact or amend data privacy law, it is not the catalyst for recently proposed laws in the United States. Indeed, as Part II shows, the CCPA is not modeled on the GDPR, though both share similarities founded in the long-established Fair Information Practice Principles. The forces behind both the CCPA and its counterparts across the United States do not seek an adequacy ruling from the European Union. Nearly a quarter century of European data protection law did not prompt the United States to take up a broad law of its own.

Why has the United States gone its own way? We will note later that the exceptional American approach to free expression, and its tension with some portions of the GDPR framework, are likely inhibiting factors. But we believe that an earlier moment of norm entrepreneurship was equally critical.

The EU prohibition on cross-border data transfers became effective in 1998 under the Data Protection Directive. Faced with the near certainty that U.S. law would not be found adequate for unrestricted data flow from the European Union,[209] the Clinton administration set

208. Julie Brill, *Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data*, MICROSOFT BLOG (May 21, 2018), https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data [https://perma.cc/2MG5-AJ49].

209. An adequacy determination would not have been forthcoming from the EU without dramatic legal and regulatory changes in the U.S. *See Opinion 1/99 of the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data: Concerning the Level of Data Protection in the United States and the Ongoing Discussions Between the European Commission and the United States Government*, at 2, art. 29 (Jan. 26, 1999), https://ec.europa.eu/justice/article-29/documentation/opinion

out to negotiate an exception because U.S. companies wanted to avoid using the more cumbersome mechanisms for data transfer available under the European law. Bolstered by its close relationship to Europe as well as America's economic and other soft power, the Clinton administration worked out a bespoke exemption from the European rules. American and European diplomats worked for years to negotiate a separate data trade agreement applicable only to their bilateral relationship. In 2000, the Clinton administration and the European Commission signed the "U.S.-EU Safe Harbor Agreement," which allowed U.S. companies to certify annually that they adhered to a narrow set of general data protection principles in order to transfer personal data from the EU.[210]

The U.S. thus inoculated itself against any catalyzing effect from EU data protection law, of either the de facto or de jure variety. The European Commission (effectively the EU's executive branch) ratified the Safe Harbor as consistent with EU data protection law.[211] But in a 2015 decision, the Court of Justice of the European Union, citing the revelations of Edward Snowden about the scope of U.S. national security surveillance, struck down the Safe Harbor.[212]

Even then, the response was not for the U.S. to conform its law to the EU adequacy standard, or even to concede that American data controllers would need to use one of the other mechanisms for cross-border data transfers. Instead, the two sides returned to the negotiating table and reached a new compromise, known as the "EU-U.S. Privacy Shield."[213] The carrot of adequacy that enticed countries from Argentina to Thailand to change their data privacy laws still failed to

-recommendation/files/1999/wp15_en.pdf [https://perma.cc/NR47-MKFU] ("[T]he current patchwork of narrowly-focussed sectoral laws and voluntary self-regulation cannot at present be relied upon to provide adequate protection in all cases for personal data transferred from the European Union."). *But see* Christopher Wolf, *Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers*, 43 WASH. U. J.L. & POL'Y 227 (2014) (making an admittedly contrarian argument that U.S. law could be judged adequate under the Data Protection Directive).

210. *See Welcome to the U.S.-EU Safe Harbor*, EXPORT.GOV (Jan. 12, 2017), https://2016.export.gov/safeharbor/eu/eg_main_018365.asp [https://perma.cc/EKJ6-XFHY].

211. *See* Commission Decision 2000/520, 2000 O.J. (L 215) 7.

212. Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 (Oct. 6, 2015).

213. *See Privacy Shield Overview*, INT'L TRADE ADMIN., https://www.privacyshield.gov/Program-Overview [https://perma.cc/TA5G-KRVU].

move U.S. privacy law.[214] In 2020, the EU's highest court once again invalidated the special transatlantic arrangement as still inconsistent with EU law.[215] It remains to be seen how the EU and U.S. will respond this time. But there is little indication that American jurisdictions have become any more inclined to harmonize U.S. law with the GDPR model.

We now turn to examine the recent extensive state and federal legislative activity in the United States. Our close comparison of the GDPR and the CCPA in Part I and our examination below of various state and federal privacy bills shows that the CCPA, not the GDPR, has played the leading role in the legislative response across the United States. The various state bills are often modeled on provisions of the CCPA. Federal bills in turn are the political response to state legislative activity prompted by the CCPA.

1. State Laws

Since the advent of the GDPR and the CCPA, the United States has seen an unprecedented volume of legislative proposals that would regulate data privacy at the state level. According to the National Conference of State Legislatures, in 2019 alone, consumer privacy bills were introduced or filed in at least twenty-five states and Puerto Rico.[216] Legislatures in nearly half of the states (twenty-one by our count) considered or enacted data security bills in 2018 and 2019.[217]

214. In a rare exception to this rule, as part of the negotiations leading to the adoption of the Privacy Shield, the U.S. Congress passed the Judicial Redress Act in 2015, 5 U.S.C. § 552a, to help assure Europeans that they would have the ability to bring claims under the Privacy Act of 1974, 5 U.S.C. § 552a, against U.S. governmental intrusions.

215. Case C-311/18, Data Prot. Comm'n v. Facebook Ir. Ltd., ECLI:EU:C:2019:1145 (Dec. 19, 2019).

216. *2019 Consumer Data Privacy Legislation*, NAT'L CONF. ST. LEGISLATURES (Jan. 3, 2020), http://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy/calif.aspx [https://perma.cc/6WNL-RX4P].

217. *See, e.g.*, Alabama Data Breach Notification Act of 2018, ALA. CODE § 8-38-1 (2018); Act Amending Title 44, Chapter 11, Arizona Revised Statutes, by Adding Article 2 Relating to Consumer Household Goods, ARIZ. REV. STAT. ANN. §§ 44-1611 to -1616 (2019); California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1789.175 (West 2019); Act Concerning Strengthening Protections for Consumer Data Privacy, COLO. REV. STAT. ANN. §§ 6-1-713, 6-1-716 (West 2019); S. 240, 101st Gen. Assemb., 1st Reg. Sess. (Ill. 2019) (introduced as Consumer Credit Reporting Agency Registration and Cybersecurity Program Act); Act To Amend and Reenact R.S. 51:3073(2) and (4)(a) and 3074, Relative to the Database Security Breach Notification Law, LA. STAT. ANN. §§ 51:3073 to :3074 (2019) (requiring organizations to destroy information and expands definition of PII); S. 786, 439th Gen. Assemb. (Md. 2019); H.R. 904, 2019 Gen. Assemb., 2019 Sess. (N.C. 2019); NEB. REV. STAT. ANN. §§ 87-801, 87-806 (West 2019); S. 176, 54th Leg., 1st Sess. (N.M. 2019); S. 5575, 2019 Leg., 2019–2020 Reg. Sess. (N.Y.

Data privacy and data security are related but not identical issues,[218] although legislators frequently conflate them—evidenced by Colorado's "data privacy" law, which focuses on data security matters. At least ten states considered privacy laws aimed at Internet service providers (ISPs), presumably in response to Congress's 2017 repeal of the Federal Communications Commission's broadband privacy rules.[219] And legislators in many states proposed narrower privacy laws, on topics from student privacy to the protection of biometric or geolocation information.[220]

2019); Security Breach Notification Act, OKLA. STAT. ANN. tit. 24, §§ 162–166 (West 2008); Act Relating to Actions After a Breach of Security that Involves Personal Information, OR. REV. STAT. ANN. §§ 646A.602, .604, .606, .608, .610, .622 (West 2011); H.R. 1181, 2019–20 Gen. Assemb., 2019 Sess. (Pa. 2019); Insurance Data Security Act, S.C. CODE ANN. §§ 38-99-10 to -100 (2019); Act To Provide for the Notification Related to a Breach of Certain Data and To Provide a Penalty Therefor, S.D. CODIFIED LAWS §§ 22-40-19 to -26 (2019); Act To Amend Tennessee Code Annotated, Title 47, Relative to Release of Personal Information, TENN. CODE ANN. § 47-18-2107 (West 2019); Act Relating to the Privacy of Personal Identifying Information and the Creation of the Texas Privacy Protection Advisory Council, H.R. 4390, 86th Leg., Reg. Sess. (Tex. 2019); S. 156, 2017–2018 Gen. Assemb., 2018 Sess. (Vt. 2018); H.R. 1071, 66th Leg., 2019 Reg. Sess. (Wash. 2019); Act To Amend the Code of Virginia by Adding a Section Numbered 58.1-341.2, Relating to Notification of Tax Return Data Breach, VA. CODE ANN. § 58.1-341.2 (2018). Virginia also introduced a bill in 2018 to amend and reenact section 59.1-200 related to the Virginia Consumer Protection Act. The bill died in committee. H.D. 1588, 2018 Gen. Assemb., Reg. Sess. (Va. 2018).

218. *See* Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667, 668–69 (2013) ("While legal scholars tend to conflate privacy and security, they are distinct concerns."); William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1141 (2019) ("*Data security* is just one element of the broader concept of *data privacy*; the latter also relates to the collection, use, and disclosure or personal data in addition to its secure storage.").

219. Brian Fung, *Trump Has Signed Repeal of the FCC Privacy Rules. Here's What Happens Next.*, WASH. POST (Apr. 4, 2017, 6:42 AM), https://www.washingtonpost.com/news/the-switch/wp/2017/04/04/trump-has-signed-repeal-of-the-fcc-privacy-rules-heres-what-happens-next [https://perma.cc/RK25-UD2A]; *see* H.R. 230, 30th Leg., 1st Sess. (Ala. 2017); H.R. 232, 30th Leg., 1st Sess. (Ala. 2017); H.R. 277, 30th Leg., 2d Sess. (Ala. 2018); S. 160, 30th Leg., 2d Sess. (Ala. 2018) (these four Alaska bills died); H.R. 80, 29th Leg., 2018 Reg. Sess. (Haw. 2018) (introducing a task force on ISP privacy); S. 243, 2019 Gen. Assemb., Reg. Sess. (Ky. 2019); S. 275, 129th Leg., 1st Reg. Sess. (Me. 2019); H.D. 1655, 2018 Gen. Assemb., Reg. Sess. (Md. 2018); H.D. 141, 2020 Gen Assemb., Reg. Sess. (Md. 2020); H.R. 382, 191st Gen. Ct., Reg. Sess. (Mass. 2019); H.R. 1030, 91st Leg., Reg. Sess. (Minn. 2019); S. 1553, 90th Leg., Reg. Sess. (Minn. 2018); H.R. 457, 66th Leg., 2019 Sess. (Mont. 2019) (failed in committee); S. 2641, 218th Leg., Reg. Sess. (N.J. 2018); Gen. Assemb. 3711, 218th Leg., Reg. Sess. (N.J. 2018); Gen. Assemb. 1927, 218th Leg., Reg. Sess. (N.J. 2018); Gen. Assemb. 1527, 218th Leg., Reg. Sess. (N.J. 2018); S. 5245, 242d Leg., 2019–2020 Reg. Sess. (N.Y. 2019); H.R. 246, 2019–20 Gen. Assemb., 2019 Reg. Sess. (Pa. 2019).

220. *See, e.g.*, H.R. 2354, 87th Gen. Assemb., Reg. Sess. (Iowa 2018); Geolocation Privacy Protection Act, H.R. 2785, 101st Gen. Assemb., 1st Reg. Sess. (Ill. 2019); H.R.

Our focus here is on the unprecedented flurry of comprehensive data privacy legislation. Restricting the focus to comprehensive data privacy laws, we count at least seventeen states in addition to California and Puerto Rico that considered or enacted comprehensive data privacy laws in 2018 and 2019.[221] Five states established task forces with the goal of proposing data privacy legislation.[222] Including task forces, there were in 2018 and 2019 at least nineteen states (and Puerto Rico) considering or enacting comprehensive data privacy legislation.[223] In California, the California Privacy Rights Act (CPRA), enacted via ballot initiative in November 2020 but with most provisions not going into effect until January 2023, establishes the new California Privacy Protection Agency, a privacy-specific regulator in that state.[224] In addition to these individual state proposals, the Uniform Law Commission (ULC) is developing a proposed uniform law that would establish "a comprehensive legal framework for the treatment of data privacy," guided to a large degree by the scope of the CCPA.[225] The ULC

536-FN, 2019 Gen. Ct., Reg. Sess. (N.H. 2019) (adding biometric information to the consumer protection act); H.R. 2866, 80th Legis. Assemb., 2019 Reg. Sess. (Or. 2019) (adding geolocation info); H.R. 352, 111st Gen. Assemb., Reg. Sess. (Tenn. 2019) (making unauthorized use or distribution of personal health information a violation of consumer protection law); S. 110, 2019–2020 Gen. Assemb., 2020 Sess. (Vt. 2020) (student privacy law); H.D. 2535, 2019 Gen. Assemb., Reg. Sess. (Va. 2019) (requiring sites to let minors request to remove information).

221. *See* S. 418, 30th Leg., Reg. Sess. (Haw. 2019); H.R. 3358, 101st Gen. Assemb., Reg. Sess. (Ill. 2019); H.R. 465, 2019 Leg., Reg. Sess. (La. 2019); S. 275, 129th Leg., 1st Reg. Sess. (Me. 2019); H.D. 901, 2019 Gen. Assemb., Reg. Sess. (Md. 2019); S. 120, 191st Gen. Ct., Reg. Sess. (Mass. 2019); H.R. 2917, 91st Leg., Reg. Sess. (Minn. 2019); H.R. 592, 100th Gen. Assemb., 1st Reg. Sess. (Miss. 2019); S. 220, 80th Sess., Reg. Sess. (Nev. 2019, codified at Chap. 211); Gen. Assemb. 4640, 218th Leg., Reg. Sess. (N.J. 2018); Gen. Assemb. 4902, 218th Leg., Reg. Sess. (N.J 2019); S. 176, 54th Leg., 1st Sess. (N.M. 2019); Assemb. 7736, 2019–2020 Leg. Sess., Reg. Sess. (N.Y. 2019); S. 5642, 2019–2020 Leg. Sess., Reg. Sess. (N.Y. 2019); H.R. 1049, 2019–2020 Gen. Assemb., Reg. Sess. (Pa. 2019); H.R. 5930, 2019 Gen. Assemb., Reg. Sess. (R.I. 2019); H.R. 4518, 86th Leg., Reg. Sess. (Tex. 2019); H.R. 764, 2017–2018 Gen. Assemb., Reg. Sess. (Vt. 2018); S. 5376, 66th Leg., 2019 Reg. Sess. (Wash. 2019).

222. S. 1108, 2019 Gen. Assemb., Jan. Sess. (Conn. 2019); H.R. 225, 30th Leg., Reg. Sess. (Haw. 2019); H.R. 249, 2019 Leg., Reg. Sess. (La. 2019); H.R. 1485, 66th Leg. Assemb., Reg. Sess. (N.D. 2019); H.R. 4390, 86th Leg., Reg. Sess. (Tex. 2019) (establishing the Texas Privacy Protection Advisory Council).

223. North Dakota and Connecticut are each counted once in our analysis, as both states proposed comprehensive data privacy legislation and ultimately instead established a task force.

224. *See* de la Torre & Brown, *supra* note 169.

225. Katie Robinson, *New Drafting and Study Committees To Be Appointed*, UNIF. L. COMM'N (July 24, 2019, 4:37 PM), https://www.uniformlaws.org/committees/community-home/digestviewer/viewthread?MessageKey=bc3e157b-399e-4490-9c5c-608ec5caabcc&CommunityKey=d4b8f588-4c2f-4db1-90e9-48b1184ca39a&

has drafted and promoted hundreds of model statutes, from the Uniform Commercial Code to the Uniform Trade Secrets Act. Once the ULC votes to publish model bills, it is up to individual state legislatures to adopt them.[226]

We focus here on a few of these proposals to identify their intellectual origins in either the CCPA or the GDPR. We find that, despite popular claims to the contrary, the catalysis for data privacy proposals in state legislatures is emanating not from Brussels, but from California.

Take, for example, Connecticut's proposed comprehensive data privacy bill, SB 1108. The original version of the bill, introduced in January 2019, effectively copied the CCPA, with minor edits. The definition of "personal information" was identical; the definition of a covered "business" was identical.[227] Like the CCPA, the proposed Connecticut bill granted individuals access rights,[228] a right to deletion,[229] and a right to opt out of the sale of one's data.[230] Like the CCPA, the proposed Connecticut bill prohibited businesses from discriminating against consumers for exercising their rights.[231] The proposed bill so closely tracked the CCPA's requirements that it, too, required a toll-free number for requesting access, and a conspicuous "Do Not Sell My Personal Information" link for opting out of sale.[232] Ultimately, however, legislators replaced the bill with a substitute act establishing a task force concerning consumer privacy, signed into law on July 9, 2019.[233] The Act instructs the task force to "examine what information businesses in this state should be required to disclose to

tab=digestviewer#bmbc3e157b-399e-4490-9c5c-608ec5caabcc [https://perma.cc/98JG-TQQ3].

226. *See FAQs*, UNIF. L. COMM'N, https://www.uniformlaws.org/aboutulc/faq [https://perma.cc/8XGL-CALF]. One of the authors of this Article, William McGeveran, previously served as the reporter for the committee drafting this model legislation; another of the authors of this Article, Margot Kaminski, serves as research director for the Developments in Privacy Law Committee.

227. *Compare* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.140(c) (defining "business"), *and id.* § 1798.140(o) (defining "personal information"), *with* S. 1108 § 1(3), 2019 Gen. Assemb., Jan. Sess. (Conn. 2019) (defining "business"), *and id.* § 1(15) (defining "personal information").

228. Conn. S. 1108 §§ 2, 4, 6.

229. *Id.* § 3.

230. *Id.* § 7.

231. *Id.* § 8.

232. *Id.* §§ 9(1), 10(1).

233. *See generally Substitute for Raised S.B. No. 1108 Session Year 2019*, CONN. GEN. ASSEMB., https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&which_year=2019&bill_num=Sb+1108 [https://perma.cc/A6F7-NZF2].

consumers . . . [s]uch examination shall include, but not be limited to, the California Consumer Privacy Act of 2018, as amended, to consider what provisions could be implemented in this state."[234]

Massachusetts's proposed data privacy bill, S. 120, provides another clear example of this mimicry.[235] Also introduced in January 2019, S. 120 contains language identical to the California law in multiple places. Like the CCPA, the proposed Massachusetts bill applies to "businesses," and like the CCPA, this includes both businesses with gross revenues over a certain threshold (ten million dollars in Massachusetts, twenty-five million dollars in California) and businesses that derive fifty percent or more of annual revenue from the disclosure of personal information. S. 120's exception for publicly available information, too, almost perfectly adopts CCPA language.[236] While S. 120 does not contain the CCPA's exhaustive list of examples of personal information, its core definition of personal information differs by just one word.[237] The proposed Massachusetts bill would establish notice, access, and deletion requirements that largely correspond to those in the CCPA.[238] Like the CCPA, the rights are not waivable.[239]

In some places, the proposed Massachusetts bill is stronger than the CCPA. It gives consumers the right to opt out of not just the sale of personal information, but also of third-party disclosure.[240] And unlike the CCPA, it provides for a private right of action, with statutory

234. Substitute S. 1108 § 1(a), 2019 Gen. Assemb. (Conn. 2019).

235. Mark D. Quist, *Comprehensive Data Privacy Legislation Introduced in Massachusetts – Includes Private Right of Action Without a Need To Prove Harm*, MONDAQ (Feb. 15, 2019), http://www.mondaq.com/unitedstates/x/781198/Data+Protection+Privacy/Comprehensive+Data+Privacy+Legislation+Introduced+In+Massachusetts+Includes+Private+Right+Of+Action+Without+A+Need+To+Prove+Harm [https://perma.cc/CZ8S-QK2M].

236. *Compare* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.140(o)(2) (2018), *with* S. 120 § 1(m)(1), 191st Gen. Ct. (Mass. 2019).

237. *Compare* Mass. S. 120 § 1(m)(1) (defining "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer *or the consumer's device*" (emphasis added)), *with* CAL. CIV. CODE § 1798.140(v)(1) (defining "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer *or household*" (emphasis added)).

238. Mass. S. 120 § 2 (requiring disclosure of categories of personal info, business purpose, consumer rights, and more); *id.* § 3 (establishing the right to request specific pieces of personal info, names of third parties to whom disclosed, sources, and business purpose); *id.* § 5 (covering the right to delete info collected from the consumer); *id.* § 6 (including the right to opt out of third-party disclosure instead of sale).

239. *Compare* CAL. CIV. CODE § 1798.192, *with* Mass. S. 120 § 14.

240. Mass. S. 120 § 6.

damages of $750 per consumer per incident, plus attorney fees.[241] Mirroring the CCPA, it directs the state attorney general to write regulations and empowers that office to enforce the new privacy rules.[242]

Also, in January 2019, North Dakota introduced data privacy legislation[243] with significant similarities to the CCPA. That legislation seems to have been inspired by a news report about European privacy law that one of the drafters watched.[244] Despite this inspiration, when the time came to draft a bill, North Dakota also looked to California for substantive language.[245] The bill defined a covered business nearly word-for-word identically to the CCPA's definition.[246] The definition of "personal information," too, closely tracked that in the CCPA.[247] It created a right of access similar to the CCPA's.[248] Unlike the CCPA, however, in a few provisions, the North Dakota bill emulated a more

241. *Id.* § 9.

242. *Id.* §§ 10–11.

243. H.R. 1485, 66th Leg. Assemb. (N.D. 2019).

244. *See* Sara Merken, *States Follow EU, California in Push for Consumer Privacy Laws (1)*, BLOOMBERG L. (Feb. 6, 2019, 3:02 PM), https://news.bloomberglaw.com/privacy-and-data-security/states-follow-eu-california-in-push-for-consumer-privacy-laws-1 [https://perma.cc/8A8X-9MUW] ("North Dakota Rep. Jim Kasper (R) told Bloomberg Law that he decided to introduce legislation after watching a '60 Minutes' program about the new rights the EU's General Data Protection Regulation provides to EU citizens.").

245. *Id.* (noting that some states have "largely follow[ed] the lead of California" in drafting consumer privacy laws).

246. *Compare* N.D. H.R. 1485, § 51-37-01 ("[A] [c]overed entity . . . a. Has annual gross revenues in excess of twenty-five million dollars; b. Annually buys, receives, sells, or shares personal information of at least fifty thousand consumers, households, or devices; or c. Derives at least fifty percent of its annual revenues from selling personal information."), *with* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.140(c) (West 2018) (defining business as "[a] sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that . . . (A) Has annual gross revenues in excess of twenty-five million dollars . . . (B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices. (C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.").

247. *Compare* N.D. H.R. 1485 § 51-37-01 ("'Personal information' means information that identifies, describes, or could reasonably be linked with a particular individual. The term does not include publicly available information lawfully made available to the general public from federal, state, or local government records."), *with* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.140(o)(1) (West 2018) ("'Personal information' means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.").

248. N.D. H.R. 1485 § 51-37-03 (providing that upon "request from an individual, a covered entity shall disclose" the content of personal data that it possesses).

European approach; for example, it would have prohibited disclosure of personal information without express written consent (more of an opt-in than an opt-out) and it would have created a private right of action.[249] On the other hand, other departures from the CCPA took it further from the GDPR, because it lacked a notice requirement or a right to deletion. Ultimately, the bill was replaced by a proposal for a legislative study of data privacy laws.[250]

These three states are just a sampling of this dynamic. We find proposals in at least seven other states that could similarly be characterized as CCPA clones to a large degree.[251] Bills in Mississippi, Pennsylvania, and Rhode Island, like those in Connecticut and Massachusetts, copied portions of the CCPA wholesale.[252] One proposed Texas bill largely tracked the CCPA as well.[253] Texas ultimately enacted a different bill into law, the Texas Privacy Protection Act; while initially it too was a broad data protection law, it was ultimately amended to create a council to report back on proposed statutory changes.[254] In Illinois, the proposed Data Transparency and Privacy Act would apply the CCPA definition of "businesses" and would grant consumers both notice and access rights and a right to opt out of sale, although it

249. *Id.* § 51-37-02 ("Prohibition against disclosure of personal information except upon written consent."); *id.* § 51-37-05 ("If an individual's personal information is purchased, received, sold, or shared by a covered entity in violation of this chapter, the individual may bring a civil action in a court of this state . . . .").

250. N.D. H.R. 1485; *see also* N.D. LEGIS. COUNCIL, DISCLOSURE OF CONSUMERS' PERSONAL DATA—BACKGROUND MEMORANDUM (2019), https://www.legis.nd.gov/files/resource/committee-memorandum/21.9058.01000.pdf [https://perma.cc/7U2L-7BLV] (noting that "House Bill No. 1485 was amended to provide for a mandatory Legislative Management study on protections, enforcements, and remedies regarding the disclosure of consumers' personal data, and both chambers passed the bill as a mandatory study").

251. *See* Rachel R. Marmor, Maryam Casbarro, Monder "Mike" Khoury & Nancy Libin, *"Copycat CCPA" Bills Introduced in States Across Country*, DAVIS WRIGHT TREMAIN LLP (Feb. 8, 2019), https://www.dwt.com/blogs/privacy—security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou [https://perma.cc/E6NB-XAFU] ("Legislators in nine states have introduced draft bills that would impose broad obligations on businesses to provide consumers with transparency and control of personal data.").

252. H.R. 1253, 2019 Leg. (Miss. 2019); H.R. 1049, 2019 Gen. Assemb. (Pa. 2019); H.R. 5930, 2019 Gen. Assemb. (R.I. 2019).

253. H.R. 4518, 86th Leg. (Tex. 2019). By contrast, H.R. 4390, 86th Leg. (Tex. 2019) takes a more blended CCPA-GDPR approach.

254. Tex. H.R. 4390; *see* Emily Bruemmer, Davis Wright Tremaine LLP, *State and Federal Privacy Legislation Stalls*, JD SUPRA (June 28, 2019), https://www.jdsupra.com/legalnews/state-and-federal-privacy-legislation-63216 [https://perma.cc/D2GZ-5P9H] (noting that House Bill 4390 created an advisory council to study data privacy laws in Texas and other jurisdictions).

carved out the use of data for advertising and other exemptions.[255] Maryland's bill and Hawaii's original bill (later replaced with a task force) offered a set of rights for data subjects similar to the CCPA, though they differ in some significant respects.[256]

Nevada is one of the only states to not just consider but actually enact new data privacy law in this period. The new law, expanding on previously existing protections, went into effect in 2019.[257] Nevada law had already required websites and online services that collect certain personal information to provide notice to consumers.[258] While not directly importing language from the CCPA, the new Nevada law echoes the conceptual core of the CCPA by prohibiting companies from selling consumer information on receipt of a "verified request" from the consumer to opt out.[259] That said, the new Nevada law proves considerably less ambitious in scope than the CCPA: it covers a narrower definition of personal information, and a narrower subset of businesses, and requires less of them (no access requests, no deletion).[260] It also defines "sale" less broadly than does the CCPA.[261] But its focus on an opt-out for restricting sale of personal data is distinctly Californian, and not European.[262]

In summary: a considerable number of states are mimicking the precise language of the CCPA, while others are adopting its core consumer-oriented framework. No state has proposed adopting European-style comprehensive data protection law. We found very few state proposals that even focused on GDPR-like compliance obligations in addition to individual consumer rights, including Washington's recently failed Privacy Act[263] (discussed further below) and one of the two bills proposed in Texas.[264] One of New York's proposals reflects a third competing concept of data privacy, which we introduce and discuss in the next Section.[265] But our close analysis clearly shows

255. H.R. 3358, 101st Gen. Assemb. (Ill. 2019).

256. S. 418, 30th Leg., Reg. Sess. (Haw. 2019); S. 613, 2019 Gen. Assemb., Reg. Sess. (Md. 2019); *see also* Marmor et al., *supra* note 251 (describing the differences between the states' draft laws).

257. S. 220, 80th Sess. (Nev. 2019).

258. NEV. REV. STAT. § 603A.340 (2019).

259. Nev. S. 220, § 2.2 (codified at NEV. REV. STAT. § 603A.345).

260. Nev. S. 220.

261. *Id.* § 1.6.1.

262. *Id.* § 2.2.

263. Washington Privacy Act, S. 5376, 66th Leg., Reg. Sess. (Wash. 2019).

264. H.R. 4390, 86th Leg. (Tex. 2019).

265. S. 5642, 2019–2020 Leg. Sess, Reg. Sess. (N.Y. 2019); *see* Issie Lapowsky, *New York's Privacy Bill Is Even Bolder Than California's*, WIRED (June 4, 2019),

that California, not Europe, is catalyzing comprehensive data privacy legislation in states around the country.

2. Federal Laws

While state bills are typically modeled on the CCPA, many proposed federal privacy bills may not look much like the CCPA at all. Yet, we argue, they are clearly drafted in response to it. There were by our count at least ten federal data privacy proposals introduced in 2018 and 2019.[266] New federal bills continue to be introduced all the time.[267] We compare several of these proposed federal laws to show how they differ from both the GDPR and the CCPA—and note how a third model has also emerged. We close this Section by explaining why, nonetheless, the CCPA can be understood as the primary catalyst of federal data privacy proposals.

We compare below the following proposed legislation to the CCPA and GDPR: Senator Ron Wyden's Consumer Data Protection Act,[268] Senator Marco Rubio's American Data Dissemination Act,[269] and Senator Brian Schatz's Data Care Act.[270] We conclude that the substantive provisions of several of the bills draw from older privacy laws or from academic proposals, not the GDPR or the CCPA. At least among

https://www.wired.com/story/new-york-privacy-act-bolder [https://perma.cc/HMH4-EEGM] (describing the New York Privacy Act).

266. *See supra* note 6 (listing comprehensive privacy bills currently being considered in Congress). *See generally* Cameron F. Kerry, *Breaking Down Proposals for Privacy Legislation: How Do They Regulate?*, BROOKINGS (Mar. 8, 2019), https://www.brookings.edu/research/breaking-down-proposals-for-privacy-legislation-how-do-they-regulate [https://perma.cc/2XML-YBRU] (discussing how different data privacy proposals may interact with existing regulatory framework); Tim Peterson, *Circling Closer to a Federal Privacy Law, Congress Has Introduced 7 Privacy Bills This Year*, DIGIDAY (June 25, 2019), https://digiday.com/marketing/cheatsheet-know-7-privacy-bills-congress-introduced-year [https://perma.cc/GC3V-ERD6] (describing different federal data privacy proposals).

267. *See, e.g.*, Zack Whittaker, *A New Senate Bill Would Create a U.S. Data Protection Agency*, TECH CRUNCH (Feb. 13, 2020, 4:00 AM), https://techcrunch.com/2020/02/13/gilliband-law-data-agency [https://perma.cc/9568-6NNH] (discussing a new bill proposed by Senator Kirsten Gillibrand called the Data Protection Act); Geoffrey A. Fowler, *Nobody Reads Privacy Policies. This Senator Wants Lawmakers To Stop Pretending We Do*, WASH. POST (June 18, 2018, 7:00 AM), https://www.washingtonpost.com/technology/2020/06/18/data-privacy-law-sherrod-brown [https://perma.cc/87D2-7LMW] (discussing a new bill proposed by Senator Sherrod Brown called the Data Accountability and Transparency Act).

268. S. SIL18B29, 115th Cong. (2018).

269. S. 142, 115th Cong. (2019).

270. S. 3744, 115th Cong. (2018).

the bills analyzed here, only Senator Wyden's bill shows direct signs of influence from both the CCPA and GDPR.

The proposed Consumer Data Privacy Act (CDPA),[271] introduced by Senator Wyden in November 2018, incorporates language and concepts from both the CCPA and GDPR, yet differs from both. For example, like the CCPA, the CDPA's definition of personal information focuses on whether information is not just individually identified but "reasonably linkable" to an individual.[272] Like the CCPA, the CDPA does not cover businesses below a certain size, as long as they meet other restrictions.[273] The CDPA, however, would incorporate a number of aspects of the GDPR: it would require reporting in some circumstances;[274] create access rights,[275] including with respect to companies that lack a direct relationship with consumers;[276] create a right of correction;[277] and require impact assessments for automated decision-making.[278] Unlike either the GDPR or CCPA, however, the CDPA would build enforcement around a robust consumer right to opt out of data sharing with third parties.[279] The CDPA directs the FTC to promulgate regulations, and houses enforcement with the FTC, to which it allocates considerable additional resources.[280] It does not preempt state regulation.

The proposed Data Care Act (DCA) introduced in December 2018 by Senator Schatz with fourteen cosponsors, differs fundamentally

271. S. SIL18B29, 115th Cong. (2018).

272. *Compare id.* § 2.12 (defining "personal information" as "any information, regardless of how the information is collected, inferred, or obtained that is reasonably linkable to a specific consumer or consumer device"), *with* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.140(o)(1) (West 2018) (defining "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household").

273. *Compare* S. SIL18B29, 115th Cong. § 2.5(B)(i) (2018) (excluding companies with less than fifty million dollars in average annual gross receipts and requiring that they not collect information on over one million people and devices and are not data brokers), *with* CAL. CIV. CODE § 1798.140(1)(A) (2018) (excluding companies with less than twenty-five million dollars in annual gross revenues).

274. S. SIL18B29, 115th Cong. § 5 (2018).

275. *Id.* § 7(b)(1)(D).

276. *Id.* § 7(b)(1)(D)(iii); *see* GDPR, *supra* note 7, art. 14 ("Information to be provided where personal data have not been obtained from the data subject").

277. S. SIL18B29 § 7(b)(1)(F).

278. *Id.* § 7(b)(1)(G).

279. *Id.* § 7(b)(1)(D)(iii).

280. *See generally id.*

from both the CCPA and GDPR.[281] The DCA would impose duties of care, loyalty, and confidentiality on online service providers.[282] The DCA focuses on duties owed by companies with a direct relationship to consumers, not on data brokers or other third parties.[283] Thus, the DCA advances a consumer protection rather than data protection model of privacy and does not impose any of the transparency requirements that are central to both the California and EU regimes. The DCA embodies an emerging strain of thought about privacy among U.S. scholars who advocate redefining privacy as a matter of "trust" or "fiduciary-like duty" on the part of large-scale data collectors.[284] The "information fiduciary" model of data privacy has not been limited to Senator Schatz's federal proposal; the recent New York Privacy Act was modeled on the concept.[285] This shows the possibility of a third potential catalyst on the field—the concept of an "information fiduciary," stemming from a number of academic proposals—and indicates perhaps an upcoming battle of the norm entrepreneurs, discussed further below.

281. Data Care Act of 2018 (DCA), S. 3744, 115th Cong. (2018). The DCA would put enforcement in the hands of the FTC, already responsible for enforcing aspects of U.S. data privacy under its consumer protection authority. *Id.* § 4(a). The Act would not preempt state privacy laws, although state attorneys general would be prevented from bringing enforcement actions during an FTC enforcement action. *Id.* § 5.

282. *Id.* § 3.

283. *Id.*

284. *See* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018) (advocating for a data privacy model based upon a context of trust); Balkin, *supra* note 137, at 1186 (discussing "the concept of an *information fiduciary*"); Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE L. REV. 1057, 1087–106 (2019) (arguing that fiduciary duties should be applied to data collectors); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1219–23 (2017) (reviewing FINN BRUNTON & HELEN NISSENBAUM, OBFUSCATION: A USER'S GUIDE FOR PRIVACY AND PROTEST (2015), and discussing how to promote trust in a digital world and hold data collectors responsible); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 434 (2016) ("If we want a sustainable digital society, we need strong, trusted information relationships [between consumers and data collectors]."); Tim Wu, *An American Alternative to Europe's Privacy Law*, N.Y. TIMES (May 30, 2018), https://www.nytimes.com/2018/05/30/opinion/europe-america-privacy-gdpr.html [https://perma.cc/49ZK-87WG] ("[T]he United States may need to . . . rely on judges and state law to establish that the legal concept of 'fiduciary duty' can apply to technology companies."). For a critique, see Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497 (2019), which identifies issues with the theory of information fiduciaries.

285. S. 5642, 2019–2020 Leg. Sess, Reg. Sess. (N.Y. 2019); *see* Bruemmer et al., *supra* note 254 ("[T]he New York Privacy Act included the concept of a 'data fiduciary'. . . ."); Lapowsky, *supra* note 265 ("[T]he New York bill would . . . require businesses to act as so-called 'data fiduciaries' . . . .").

The proposed American Data Dissemination Act (ADD), introduced by Senator Rubio in January 2019, directs the FTC to propose privacy rules "substantially similar, to the extent practicable, to the requirements applicable to agencies" under the 1974 Privacy Act.[286] Unlike the Privacy Act,[287] which applies only to the federal government, these rules would apply to private sector actors that collect certain types of personal information.[288] The ADD resembles the GDPR and CCPA only to the extent that those two regimes, like the 1974 Privacy Act, build on Fair Information Practice Principles.[289] It directs the FTC to adopt regulations that restrict disclosures of records;[290] create an access right;[291] and create a correction right of sorts, or at least a means to amend and dispute inaccurate records based on process established under the Fair Credit Reporting Act.[292] Thus, the ADD draws on neither the CCPA nor the GDPR directly, but instead uses existing federal privacy law as its model. The ADD would preempt state privacy laws.[293]

While the three federal bills do not mimic the CCPA to the extent state laws do, the CCPA laid the groundwork for federal legislation in two key ways. First, because U.S. corporations with national reach will likely find themselves having to comply with the CCPA (and possibly also the GDPR), a federal rule presents less of a regulatory burden for U.S. corporations than it would have in the absence of the CCPA. Second, many hope to limit the potential regulatory burden of multiple, varying state laws by enacting a federal law that preempts state laws. Given the flurry of activity in state houses across the country, a federal law seems to many businesses like the "least worst" option. In this sense, the federal response may well be a backlash against the CCPA rather than an embrace of it.

286. American Data Dissemination Act of 2019, S. 142, 115th Cong. § 4(a)(2) (2019).

287. Privacy Act of 1974, 5 U.S.C. § 552a.

288. S. 142, 115th Cong. § 2(a)(5) (2019) (defining "covered providers").

289. *Fair Information Practice Principles*, INT'L ASS'N PRIV. PROS., https://iapp.org/resources/article/fair-information-practices/#:~:text=(1)%20The%20Collection%20Limitation%20Principle,2)%20The%20Data%20Quality%20Principle [https://perma.cc/EY8C-92GD] (describing the eight principles).

290. American Data Dissemination Act of 2019, S. 142, 115th Cong. § 4(b)(1)(B) (2019).

291. *Id.* § 4(b)(1)(C).

292. *Id.* § 4(b)(1)(D)–(E).

293. *Id.* § 6.

C. CALIFORNIA AS U.S. PRIVACY CATALYST

The above analysis—in Part II comparing the CCPA and GDPR, and in this Part above analyzing in detail a number of recent state and federal proposals—leads us to a new understanding of what is happening in the race to influence U.S. data privacy law. The true story is more complex, and more interesting, than the conventional narrative of a long-armed, unilateral Brussels. California, not Europe, has been catalyzing privacy proposals across the United States.

In this Section, we offer this alternative story. We begin with a discussion of how our departure from the GDPR-centric narrative is more than just a shift in location from Brussels to Sacramento. The story of California as the U.S. data privacy catalyst involves not just state government actors but also tightly networked norm entrepreneurs, acting against backdrop forces of what we call "data globalization." The spread of the CCPA to other states, we posit, reflects a number of overlapping dynamics, and the influence of the GDPR is only one of them. This version of the story may be messier than a pure Brussels Effect, but it is more accurate and leads to several insights about the near future of U.S. data privacy law.

The theories of regulatory catalysis that we discussed in Part I are essentially realist or rational choice theories of lawmaking. That is, the Brussels Effect largely conceives of States (and states) as unitary actors, using power to achieve compliance on an international stage or balancing sticks with carrots to drive both government and private entities towards rationally choosing a regulatory goal.

The story of the CCPA, when examined in greater detail, is far more complex. It is not the story of California as a unified state actor but of a collection of individual norm entrepreneurs that harnessed the state legislative process to produce the law. In this sense, it is a legal process story made up not just of governments but of individuals, issue networks, and interpretative communities, one that reflects Harold Koh's characterization of vertical legal process in style if not in transnational nature.[294]

If the origin story of the CCPA teaches anything, it is that individuals and networks of individuals play significant roles in the process of regulatory catalysis. Before 2018, California, like every other U.S.

294. *See generally* Koh, *supra* note 192, at 1406 (explaining compliance with international law norms in part through "the *vertical process* whereby transnational actors interact in various fora, generate and interpret international norms, and then seek to internalize those norms domestically"); Harold Hongju Koh, *Transnational Legal Process*, 75 NEB. L. REV. 181 (1996) (providing a broad overview of transnational legal process and its significance in international legal scholarship).

state and the federal government, had no comprehensive data privacy law. Real estate developer Alastair Mactaggart wanted to enact such law in California.[295] Mactaggart and his friend Rick Arney, who had worked in the California legislature, knew they could use California's referendum process to avoid being tangled up by lobbying in the legislature.[296] Mactaggart befriended Mary Stone Ross, who had worked for the CIA and the House Intelligence Committee.[297] They collaborated on drafting the ballot initiative through a group they named Californians for Consumer Privacy, the political committee that then pushed the bill (although Ross and Mactaggart later had a falling out).[298] Mactaggart looked up privacy experts, and contacted UC Berkeley Professor Chris Jay Hoofnagle, who put him in touch with former FTC Chief Technologist Ashkan Soltani.[299] Mactaggart then hired Soltani to help revise the proposed ballot initiative, the bones of which became the CCPA.[300] Then, as Soltani has put it, "Mactaggart . . . offered Silicon Valley a take-it-or-leave-it privacy policy—the same kind that Silicon Valley usually offered everyone else."[301]

By using the California ballot initiative process, Mactaggart and his allies forced the state legislature's hand.[302] The California legislature, fearing the practical difficulties of a ballot initiative that would become nearly unchangeable law with immediate effect,[303] scrambled

295. *See* Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley—and Won*, N.Y. TIMES MAG. (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html [https://perma.cc/PG7Y-A9FM].

296. *Id.*

297. Kashmir Hill, *How a Woman Disappears from the History Books*, JEZEBEL (Aug. 20, 2018), https://jezebel.com/how-a-woman-disappears-from-the-history-books-1828393645 [https://perma.cc/J7C9-2CHP].

298. *See id.* (noting "personality conflicts" between Mactaggart and Ross).

299. Confessore, *supra* note 295.

300. *Id.*

301. *Id.*

302. *Id.* The initiative gathered some 629,000 signatures. *Id.*

303. Amending an initiative approved by the voters "would require a 70 percent vote of each house and signature by the governor," and any amendment would have to be "consistent with, and further the intent of, the act." Edward R. McNicholas, Colleen Theresa Brown, Amy Lally, Michael Mallow & Ash Nagdev, *California's GDPR? Sweeping California Privacy Ballot Initiative Could Bring Sea Change to U.S. Privacy Regulation and Enforcement*, SIDLEY AUSTIN LLP (June 26, 2018), https://datamatters.sidley.com/californias-gdpr-sweeping-california-privacy-ballot-initiative-could-bring-sea-change-to-u-s-privacy-regulation-and-enforcement [https://perma.cc/KZ9G-RNH2]; Kristen J. Mathews & Courtney M. Bowman, *The California Consumer Privacy Act of 2018*, PROSKAUER ROSE LLP (July 13, 2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018 [https://

to draft a bill that would persuade the initiative's sponsors to withdraw it.[304] State Assembly member Ed Chau and State Senator Robert Hertzberg, both from districts neighboring Los Angeles, introduced the bill.[305] The enactment of the CCPA does not represent the action of a legislature that independently recognized a social problem it could help address or a response spurred by companies advocating for legislation under the pressures of the GDPR. Instead, it was the legislature's reaction to leverage exerted by highly motivated, connected, and—at least in Mactaggart's case—wealthy individuals.[306]

Rather than causing a race to the bottom, the backdrop of data globalization appears to have both influenced and empowered these norm entrepreneurs. First, news stories about the effects of data globalization enabled Mactaggart to frame the importance of the initiative, as he repeatedly pointed to the story of the British consulting firm Cambridge Analytica using U.S. persons' data to allegedly manipulate voters in the 2016 election.[307] In the preamble to the CCPA, the California legislature eventually echoed this motivation.[308] Second, data

perma.cc/8A87-JZJW] ("[I]t can be very difficult to amend [California] ballot initiatives once they are voted into law.").

304. *See* Confessore, *supra* note 295 ("[Mactaggart] . . . told California lawmakers that he would drop his campaign if they could pass a reasonable privacy bill by June 28, the legal point of no return for formally withdrawing his initiative from the ballot."); Assemb. 375, 2018 Leg. § 2(g) (Cal. 2018) (enacted) ("In March 2018, it came to light that tens of millions of people had their personal data misused by a data mining firm called Cambridge Analytica.").

305. *See* Assemb. 375, 2018 Leg. § 2(g) (Cal. 2018) (enacted) (enacting the California Privacy Act of 2018).

306. To some extent, aspects of the GDPR reflect this dynamic, too. *See* Case C–362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 (Oct. 6, 2015) (invalidating the EU Safe Harbor arrangement in favor of privacy advocate Schrems).

307. Cambridge Analytica LLC, Docket No. 9383, 2019 WL 6724446 (FTC Nov. 25, 2019); *see* Casey Newton, *How a Wiley Californian Beat Google and Facebook's Influence Operation*, VERGE (Aug. 15, 2018), https://www.theverge.com/2018/8/15/17691004/california-data-privacy-law-alastair-mactaggart-regulation [https://perma.cc/9CZY-WDKG] ("Mactaggart benefited from increased skepticism about tech companies broadly, but he also got an unexpected gift this spring: the Cambridge Analytica data privacy scandal."). For an argument that the actual impact of the Cambridge Analytica misuse of information on the 2016 U.S. election was "likely exaggerated," see YOCHAI BENKLER, ROBERT FARIS & HAL ROBERTS, NETWORK PROPAGANDA: MANIPULATION, DISINFORMATION, AND RADICALIZATION IN AMERICAN POLITICS 277 (2018).

308. Assemb. 375, 2018 Leg. § 2(g) (Cal. 2018) ("In March 2018, it came to light that tens of millions of people had their personal data misused by a data mining firm called Cambridge Analytica. A series of congressional hearings highlighted that our personal information may be vulnerable to misuse when shared on the Internet. As a result, our desire for privacy controls and transparency in data practices is heightened.").

globalization may have lowered some of the bigger hurdles to privacy lawmaking in California (and possibly Congress) by imposing GDPR compliance costs on the large Silicon Valley enterprises, almost all of which have a substantial European presence. Faced with significant privacy compliance costs from the GDPR, the marginal cost of a state privacy statute to their business model was now much lower. Third, data globalization enabled the GDPR itself to touch U.S. citizens in the form of both updated privacy policies and news stories about protective European privacy law.[309] This affected both public opinion and elite responses, whether causing U.S. citizens to wonder why Europeans should get privacy protections that we do not, or inspiring lawmakers like the North Dakota legislator to take action on a privacy bill.[310]

What happened next—the spread of the CCPA—was intended and predicted by its originators, who hypothesized that, like California emissions standards, a baseline data privacy law would spread.[311] We offer four explanations, beyond the usual dynamics of the California Effect, as to why this is happening.

First, even prior to the CCPA, California established itself nationally as an expert jurisdiction on data privacy law, given both previous pioneering legislation and the presence of Silicon Valley within its borders. California has been a forerunner in laws governing online data privacy and data security for over fifteen years. The California Online Privacy Protection Act (CalOPPA) was enacted in 2003 and went into effect in 2004.[312] It was the first U.S. law "to require commercial

309. *See, e.g.*, Adam Satariano, *GDPR, a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. TIMES (May 25, 2018), https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html ("[T]he European Union . . . enacts the world's toughest rules to protect people's online data.").

310. *See, e.g.*, Brooke Auxer, 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/QN3J-EX93] ("[A] majority of Americans report being concerned about the way their data is being used by companies . . . .").

311. Confessore, *supra* note 295 (noting how Mactaggart compares privacy legislation to auto-emission legislation).

312. CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2014).

websites and online services to post a privacy policy."[313] In the intervening years, privacy policies have become ubiquitous across the Internet.[314]

Also, in 2003, California enacted a data breach notification law: legal rules requiring companies that have suffered a qualifying data security breach to notify users whose information may have been compromised.[315] Prior to California's intervention, few companies voluntarily disclosed security breaches of their customers' personal information, fearing the public relations disaster of such a revelation.[316] At first, some companies limited their compliance with the new data breach notification law to the borders of California. In 2004, the data broker ChoicePoint suffered a huge data breach.[317] Initially, it reported that breach to Californians only, as the state's law required.[318] However, observers quickly noted how odd it would be if a data breach at an Atlanta-based nationwide operation affected only Californians. Faced with intense criticism for failing to inform customers outside California, ChoicePoint voluntarily issued a nationwide notice to all Americans whose information had been compromised.[319]

313. *California Online Privacy Protection Act (CalOPPA)*, CONSUMER FED'N CAL. EDUC. FOUND. (July 29, 2015), https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3 [https://perma.cc/QL8G-499H].

314. *See, e.g.*, *supra* note 208 and accompanying text.

315. CAL. CIV. CODE § 1798.82 (West 2003) (providing disclosure requirements for any person or business in California who owns or licenses computerized data, including personal information, when there is a security breach of the system).

316. SAMUELSON L., TECH. & PUB. POL'Y CLINIC, UNIV. CAL.-BERKELEY SCH. L., SECURITY BREACH NOTIFICATION LAWS: VIEWS FROM CHIEF SECURITY OFFICERS 15 (2007), https://www.law.berkeley.edu/files/cso_study.pdf [https://perma.cc/5BG7-8VDN] (conducting interviews with businesses and noting that "all the organizations interviewed noted concerns that a public notification of a breach would damage their organizations' reputation and the trust behind their name").

317. Tom Zeller Jr., *Breach Points Up Flaws in Privacy Laws*, N.Y. TIMES (Feb. 24, 2005), https://www.nytimes.com/2005/02/24/business/breach-points-up-flaws-in-privacy-laws.html [https://perma.cc/G6MH-GWJW] (noting that the data breach allowed con artists to access "personal data of nearly 145,000 people").

318. *See id.* ("ChoicePoint informed only 35,000 Californians that their information might have been compromised in [breach] because California is currently the only state that requires companies to make such disclosures.").

319. ChoicePoint explained its delay in notifying non-Californians as follows: "The company said it first notified consumers in California because that was where most of the victims lived, and then prepared more notices when investigators suggested that residents in nearly every state were affected." *Id.* Most analysts discredit this explanation. *See, e.g.*, Ronald I. Raether, Jr., *There Has Been a Data Security Breach: But Is Notice Required?*, A.B.A. (Aug. 31, 2011), http://apps.americanbar.org/buslaw/blt/content/2011/08/article-raether.shtml [https://perma.cc/E57W-NQLT] ("ChoicePoint decided initially to notify only California consumers. The backlash was swift and

This notification also resulted in an enforcement action by the FTC. ChoicePoint, a provider of credit reporting services, had violated the federal Fair Credit Reporting Act by allowing access to some 163,000 consumer reports to persons who were not duly authorized to receive access.[320] So far, this story resonates with our account of the Brussels Effect: a large business found it unwise to compartmentalize its compliance efforts based on the law of particular jurisdictions and was forced to provide a higher level of protection across its operations.

By 2005, the California breach notification law had unleashed a "wave" of additional reported security breaches in the state.[321] These notifications in California alerted consumers nationally of breaches that might have affected them but remained unreported under their own states' laws. Very swiftly, in a textbook de jure California Effect, dozens of other states adopted their own notification laws.[322] Today, all fifty states have enacted data security breach notification laws.[323] The laws that followed California's not only copied but also both expanded[324] and contracted[325] California's model. And in 2018, the

immediate. ChoicePoint quickly modified its decision and notified all affected consumers regardless of their state of residency.").

320. Natalie Kim, *Three's a Crowd: Towards Contextual Integrity in Third-Party Data Sharing*, 28 HARV. J.L. & TECH. 325, 330 (2014); *see* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 923 (2007) (describing ChoicePoint's settlement with the FTC). The FTC-ChoicePoint settlement also authorized the FTC to monitor compliance by "[p]osing as consumers and suppliers" of ChoicePoint. *See* Stipulated Final Judgement & Order at 19, United States v. ChoicePoint Inc., No. 1:06-cv-0198 (N.D. Ga. Jan. 26, 2006), https://www.ftc.gov/sites/default/files/documents/cases/2006/01/0523069stip.pdf [https://perma.cc/P9N9-3T9U].

321. Satish M. Kini & James T. Shreve, *Notice Requirements: Common Themes and Differences in the Regulatory and Legislative Responses to Data Security Breaches*, 10 N.C. BANKING INST. 87, 87 (2006).

322. *See* SAMUELSON L., TECH. & PUB. POL'Y CLINIC, *supra* note 316, at 3 ("At least 36 states have enacted legislation requiring organizations that possess sensitive personal information to warn individuals of security breaches. California led the way in the creation of these laws, driven by concerns about identity theft and lax information security. In following California's lead, other states have expanded upon the requirements of the California statute by, for example, requiring that organizations report breaches to a state regulatory agency.").

323. *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (July 17, 2020), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/3ZXZ-WA2C].

324. *See* SAMUELSON L., TECH. & PUB. POL'Y CLINIC, *supra* note 316, at 9 ("[M]any states have expanded the definition to include various others forms of personal information . . . .").

325. *Id.* at 44 ("[M]any states have also narrowed California's notification trigger by exempting notification to consumers only if, upon a reasonable investigation, the organization reasonably determines that harm is not likely to result to individuals

GDPR introduced security breach notification into European law, explicitly borrowing from California's innovation.[326]

This history of following California law lays the groundwork for states to imitate the CCPA. And California may be seen as an expert jurisdiction on digital data policy for other reasons. If a state legislature is going to copy another state and wants to strike a balance between individual rights and business needs, California law represents an appealingly pre-packaged compromise from the state that houses both a generally pro-consumer electorate and Silicon Valley industry.

Second, we believe states may be copying California because they presume that the CCPA will create a Brussels Effect of de facto compliance, originating in California. This is probably part of what caused the copycat data breach notification statutes. Lawmakers in other states should anticipate that companies are less likely to oppose a bill if it tracks the contours of a California law that those businesses must obey already. Even though the CCPA protects only California residents, companies may find it difficult to partition that data or may calculate the cost is low enough to extend their compliance infrastructure to consumers in other states. This makes those companies with exposure to the CCPA, but not to the GDPR, less likely to fight a local law that mimics the CCPA.

Third, compared to the GDPR, the CCPA is a better legal meme for U.S. legislators.[327] The GDPR contains 99 articles and 173 recitals, and it harnesses an existing complex regulatory system against the backdrop of European court decisions and constitutional doctrine. The GDPR is long, complicated, and foreign.[328] The CCPA's relative brevity and simplicity, however, likely make it more appealing to state legislatures. A state could only "copy" the GDPR after condensing it and transposing it into an American legal setting. A state can copy the CCPA simply by cutting and pasting.

Fourth, while not directly catalyzing U.S. privacy law, the GDPR continues to play an important role. For the most part the GDPR has not had a (de jure) "California Effect" on the U.S. federal government or U.S. states, but it has had a (de facto) "Brussels Effect" on companies

whose information is compromised by the breach. Vermont requires that, if an organization makes such a determination, the organization must provide notice and an explanation to the Attorney General or to the applicable department of banking, insurance, securities and health care administration.").

326. *See* GDPR, *supra* note 7, art. 33 ("Notification of a personal data breach to the supervisory authority.").

327. We thank Christina Mulligan for this insightful characterization.

328. *See supra* note 73 and accompanying text.

operating in U.S. jurisdictions. This may lower the resistance of global companies to both state and U.S. data privacy law. While many of the companies most affected by the GDPR were already shouldering regulatory costs under the prior Data Protection Directive, the GDPR has heavier obligations, more explicit extraterritorial reach, and more severe penalties, all of which have dramatically increased corporate investment in GDPR compliance over the levels under the Directive.

A clear example of this dynamic is the proposed Washington Privacy Act, which has twice come relatively close to passage only to fail late in the process.[329] This bill had more similarities with the GDPR than other state legislation.[330] It used GDPR terminology such as "controller" and "processor."[331] It would have established "GDPR lite" requirements for notice, access, correction, deletion, and restriction of processing requirements, and would have imported aspects of the EU concept of lawful processing.[332] Unlike other proposed state laws, the Washington bill included privacy risk assessments, another idea borrowed from the GDPR.[333] It even drew on the GDPR's limitations on automated decision-making.[334]

The key to understanding why the Washington proposal borrowed so many elements of the GDPR may be one of the state's largest companies: Microsoft.[335] Microsoft has declared that it complies with

329. S. 5376, 66th Leg., Reg. Sess. (Wash. 2019).

330. *Id.*

331. *See generally id.*; GDPR, *supra* note 7, art. 33 (using the terms "controller" and "processor").

332. Wash. S. 5376 § 7 (requiring controllers to provides consumers a privacy notice that includes: the categories of personal data collected, purposes for which that data is used, rights that consumers may exercise, categories of personal data shared with third parties, and whether it sells personal data to data brokers).

333. *Compare id.* § 8(4) ("The controller must make the risk assessment available to the attorney general upon request. Risk assessments are confidential and exempt from public inspection and copying."), *with* GDPR, *supra* note 7, art. 35 ¶ 7 ("Data protection impact assessment.").

334. Washington Privacy Act, H.R. 5376, 66th Leg., Reg. Sess. §§ 6(7), (14)(1) (Wash. 2019) ("A consumer must not be subject to a decision based solely on profiling which produces legal effects concerning such consumer or similarly significantly affects the consumer . . . Controllers using facial recognition for profiling must employ meaningful human review prior to making final decisions based on such profiling where such final decisions produce legal effects concerning consumers or similarly significant effects concerning consumers.").

335. *Microsoft Corporation (MSFT)*, YAHOO FIN. (Jan. 17, 2021), https://finance.yahoo.com/quote/MSFT/ [https://perma.cc/K68U-3STV] (showing Microsoft's market capitalization as of January 17, 2021, as $1.608 trillion).

the GDPR worldwide.[336] With over 451,000 employees in the state, the company has a significant voice in Washington.[337] The company actively promoted adoption of the Washington statute; Microsoft President Brad Smith described it as "build[ing] on the best aspects of approaches elsewhere."[338] In introducing the bill, Washington Chief Privacy Officer Alex Alben tellingly explained that "companies that already comply with Europe's General Data Protection Regulation . . . shouldn't have a hard time complying with the proposed law in Washington."[339]

The Brussels Effect on Microsoft may thus be driving it to push for state privacy legislation that more closely maps on to the GDPR and therefore does not raise regulatory costs for Microsoft—but may raise regulatory costs for non-GDPR-compliant local competitors. Microsoft also gains by assuring users that their information is well-protected, with legal sanctions for failures.

After sailing through the state senate by a vote of 46-1,[340] the Washington bill foundered amid controversy in 2019. After portions of the original legislation were stripped out, the state ACLU and

336. Julie Brill, *Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data*, MICROSOFT ON ISSUES (May 21, 2018), https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data [https://perma.cc/P5D2-TZZ8] ("That's why today we are announcing that we will extend the rights that are at the heart of GDPR to all of our consumer customers worldwide. Known as Data Subject Rights, they include the right to know what data we collect about you, to correct that data, to delete it and even to take it somewhere else.").

337. Monica Nickelsburg, *Amazon Surpasses Microsoft in Number of Seattle Region Employees Amid Big Growth Plans Across US*, GEEKWIRE (Sept. 9, 2019), https://www.geekwire.com/2019/amazon-surpasses-microsoft-number-seattle-region-employees-amid-big-growth-plans-across-us [https://perma.cc/6RZT-AG7L].

338. Brad Smith, *Next Generation Washington: Our Priorities for 2019*, MICROSOFT ON ISSUES (Feb. 11, 2019), https://blogs.microsoft.com/on-the-issues/2019/02/11/next-generation-washington-our-priorities-for-2019 [https://perma.cc/M3MR-VZEM]; Wendy Davis, *Microsoft Endorses Washington State Proposed Privacy Bill*, MEDIAPOST: DIGIT. NEWS DAILY (Feb. 11, 2019), https://www.mediapost.com/publications/article/331814/microsoft-endorses-washington-state-proposed-priva.html [https://perma.cc/H36D-C7HJ].

339. Monica Nickelsburg, *Washington State Considers New Privacy Law To Regulate Data Collection and Facial Recognition Tech*, GEEKWIRE (Jan. 22, 2019), https://www.geekwire.com/2019/washington-state-considers-new-privacy-law-regulate-data-collection-facial-recognition-tech [https://perma.cc/JRL5-6ZJZ] (paraphrasing Alben's remarks).

340. *Senate Passes Carlyle's Washington Privacy Act*, WASH. SENATE DEMOCRATS (Feb. 14, 2020), https://senatedemocrats.wa.gov/carlyle/2020/02/14/senate-passes-carlyles-washington-privacy-act [https://perma.cc/TY6U-57MX].

consumer advocacy organizations opposed the bill as too weak.[341] Critics objected that the bill's departure from elements of the GDPR, especially in its enforcement mechanisms, would make it ineffective; they also complained that industry lobbyists had too much influence over a legislative process they considered opaque.[342] After working to mend fences with privacy advocates and expand industry support, the bill's sponsors reintroduced it in 2020, with most of the same core features, but again fell short at the end of the legislative session.[343] Microsoft's chief privacy officer, former FTC commissioner Julie Brill,[344] has signaled that the company will continue to support legislation modeled at least loosely on the GDPR, declaring, "We believe privacy is a fundamental human right."[345]

This story of the Washington Privacy Act displays the GDPR's Brussels Effect in action. But again, it also underscores the power of individual or corporate norm entrepreneurs. A global company that already complies with the GDPR has good reason to want to impose costs on its competitors while publicly promoting stronger privacy rights for its users and thus enhancing their trust in that company. In addition, Brill, a former FTC commissioner who was well regarded among privacy advocates, appears to be driving the agenda and bringing in compliance norms from a U.S. government agency.

341. *Coalition Letter in Opposition to SB 5378*, ACLU WASH. (Apr. 16, 2019), https://www.aclu-wa.org/docs/coalition-letter-opposition-sb-5376 [https://perma.cc/5UVT-8T23]; *Washington State Privacy Bill Fails To Advance; Consumer Reports Says Weak Bill Did Not Provide Meaningful Protections*, CONSUMER REPS. ADVOC. (Apr. 18, 2019), https://advocacy.consumerreports.org/press_release/washington-state-privacy-bill-fails-to-advance-consumer-reports-says-weak-bill-did-not-provide-meaningful-protections [https://perma.cc/V6WS-AMH8]; *see also* Lucas Ropek, *Why Did Washington State's Privacy Legislation Collapse?*, GOV. TECH. (Apr. 19, 2019), https://www.govtech.com/policy/Why-Did-Washington-States-Privacy-Legislation-Collapse.html [https://perma.cc/L6RK-C67U].

342. Ropek, *supra* note 255.

343. Lucas Ropek, *Washington Privacy Law Once Again Fails To Materialize*, GOV. TECH. (Mar. 13, 2020), https://www.govtech.com/policy/Washington-Privacy-Law-Once-Again-Fails-to-Materialize.html [https://perma.cc/JC9N-UC2G].

344. *Former Commissioners*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/biographies/former-commissioners [https://perma.cc/5F66-ZGDJ].

345. *See* Julie Brill, *The New Washington Privacy Act Raises the Bar for Privacy in the United States*, MICROSOFT ON ISSUES (Jan. 24, 2020), https://blogs.microsoft.com/on-the-issues/2020/01/24/washington-privacy-act-protection [https://perma.cc/NA9L-VMAU]; Julie Brill, *Our Support for Meaningful Privacy Protection Through the Washington Privacy Act*, MICROSOFT ON ISSUES (Apr. 29, 2019), https://blogs.microsoft.com/on-the-issues/2019/04/29/our-support-for-meaningful-privacy-protection-through-the-washington-privacy-act [https://perma.cc/3TWA-GHYD].

Finally, the GDPR may be playing an important framing role in policy discussions, acting to rhetorically normalize and ground current conversations around data privacy. The publicity accompanying the advent of the GDPR may have stoked American public interest in data privacy. The GDPR may be leading U.S. citizens—including the North Dakota legislator mentioned above[346]—to wonder why EU persons get stronger privacy rights than Americans, and to question the longstanding narrative that imposing digital privacy regulation will break the Internet or otherwise kill innovation.[347]

Some may doubt the sincerity of California as a privacy regulator. Data protection rules, critics will observe, encumber some of its leading corporations. They may assume that these corporations will hobble any real regulatory enforcement by the state. But California's economy is far bigger than Silicon Valley alone. Of course, diffuse voices fare poorly against actors with concentrated interests, as Mancur Olson observed.[348] But Mary Stone Ross, Alastair MacTaggart, and others demonstrated that California's initiative process could be leveraged to tap into a widely shared desire to protect privacy that could overcome even concentrated industry opposition. Indeed, MacTaggart and his organization led the successful campaign to pass CCPA revisions by ballot measure.[349] This time, however, Mary Stone Ross opposed the ballot measure, arguing that "the initiative would roll

346. *See supra* note 244 and accompanying text.

347. For a description of the role of privacy law in the rise of U.S. Internet companies, see Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639, 642 (2014), which states that "legal innovations in the 1990s that reduced liability concerns for Internet intermediaries, coupled with low privacy protections, created a legal ecosystem that proved fertile for the new enterprises of what came to be known as Web 2.0."

348. MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS 2 (1965) ("[U]nless the number of individuals in a group is quite small, or unless there is coercion or some other special device to make individuals act in their common interest, rational, self-interested individuals will not act to achieve their common or group interests.").

349. *See* Allison Grande, *What's at Stake as Calif. Privacy Law Revamp Goes to Voters*, LAW360 (Oct. 23, 2020, 9:12 PM), https://www.law360.com/articles/1313938/what-s-at-stake-as-calif-privacy-law-revamp-goes-to-voters [https://perma.cc/RBL8-JNAK]; Sidney Fussell, *One Clear Message from Voters This Election? More Privacy*, WIRED (Nov. 4, 2020, 8:26 PM), https://www.wired.com/story/one-clear-message-voters-election-more-privacy [https://perma.cc/7N4A-RE3E].

For the full text of the California Privacy Rights and Enforcement Act of 2020, see *The California Privacy Rights Act of 2020,* CAL. DEP'T JUST. (Nov. 4, 2020), https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf [https://perma.cc/CWP9-C85F].

back the CCPA's protections and weaken core definitions of the law, while making the biggest companies even more powerful."[350]

Vogel argues that the California Effect requires that "nonstate actors in rich and powerful political jurisdictions prefer stronger regulatory standards."[351] Content-based industries based in Los Angeles have long complained that Silicon Valley enterprises are insufficiently attentive to intellectual property claims. The CCPA's principal authors[352] both represent districts bordering Los Angeles.[353] Many Silicon Valley enterprises themselves support data privacy law, though some suggest that the support is a strategic effort to undermine California's privacy law with a weaker, preemptive federal law.[354] There is a reason for responsible Silicon Valley enterprises to embrace privacy law. Silicon Valley enterprises depend on users' confidence that revealing more and more of themselves to their electronic assistants will not create privacy risks. Companies that violate that trust undermine trust for other companies as well.[355] Ultimately, whether Californians or those outside the state trust the state's privacy regulators will depend on their performance.[356]

There are many more individual norm entrepreneurs at work here in the spread of the CCPA to other states, and the federal response to it, than we have thus far allowed. As mentioned above, the Uniform Law Commission's new project to draft model state legislation represents one of the most formal such networks: commissioners from every state consciously seek to replicate successful innovations across state boundaries in a uniform way. Individual federal

350. Grande, *supra* note 349.

351. VOGEL, *supra* note 45, at 268.

352. Assemblymember Ed Chau and Senator Robert Hertzberg introduced the CCPA. Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (June 28, 2018, 5:57 PM), https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill [https://perma.cc/LPW2-CW6B].

353. Chau represents the 49th Assembly District and Hertzberg represents the 18th Senate District. ED CHAU, https://a49.asmdc.org [https://perma.cc/NBG3-GUY9]; SENATOR ROBERT HERTZBERG, https://sd18.senate.ca.gov [https://perma.cc/Q4SK-9DYQ].

354. Russell Brandom, *Tim Cook Wants a Federal Privacy Law—but So Do Facebook and Google*, VERGE (Oct. 24, 2018, 4:12 PM), https://www.theverge.com/2018/10/24/18018686/tim-cook-apple-privacy-law-facebook-google-gdpr [https://perma.cc/QDP5-3NH5].

355. *See* Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIA. L. REV. 559, 598 (2015); *see also* Balkin, *supra* note 137; Richards & Hartzog, *supra* note 284, at 435.

356. *Cf.* Ann E. Carlson, *Regulatory Capacity and State Environmental Leadership: California's Climate Policy*, 24 FORDHAM ENV'T L. REV. 63, 65–66 (2012) (describing success of California's environmental policy agency).

representatives are catalysts for change. Senator Wyden, for example, has been a privacy advocate for years and may be taking advantage of current dynamics to push for changes to federal law.[357] Civil society groups such as the Center for Democracy and Technology have proposed discussion legislation in hopes of influencing the federal debate.[358] The North Dakota legislator who watched a GDPR documentary, too, can be characterized as a norm entrepreneur. David Hoffman at Intel Corporation, characterized as a longtime "industry leader on privacy," developed a draft federal proposal that Intel released for comments.[359] These stories likely represent the tip of a very large iceberg of individuals and knowledge networks working to harness existing forces to propagate new law.

This suggests the early growth of what we call "catalysis networks." Paul Schwartz has noted the existence of "harmonization networks" (a term coined by Anne-Marie Slaughter) in privacy law—networks of "regulators in different countries [who] work together to harmonize or otherwise adjust different kinds of domestic law."[360] What we are seeing here is not solely attempts by various actors to harmonize U.S. and EU law on the ground (although it is certainly in the interest of global companies to minimize disparities). We predict that we are seeing the emergence of both individuals and networks taking advantage of the moment to drive both broader geographic coverage and perhaps new forms of law.

In one version of this story, the CCPA becomes not just a catalyst but a floor of protection nationwide. There are certainly plenty of reasons to believe this might be the case. That said, we turn now to several potential limits on Californian catalysis.

D. CONSTRAINTS ON CALIFORNIAN CATALYSIS

There are at least three possible constraints on the nationwide spread of CCPA-like privacy law. First, the complex relationship between state and federal sovereignty in the U.S. constitutional order interacts substantially with the ability of state laws like the CCPA to operate or spread nationally. Both the dormant commerce clause and

357. *See* Sara Morrison, *The Year We Gave Up on Privacy*, VOX (Dec. 23, 2020, 8:00 AM), https://www.vox.com/recode/22189727/2020-pandemic-ruined-digital-privacy; Kerry, *supra* note 266.

358. *CDT's Privacy Legislation*, CTR. FOR DEMOCRACY & TECH., https://cdt.org/campaign/federal-privacy-legislation [https://perma.cc/4AZG-K8EF].

359. Kerry, *supra* note 266.

360. Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1967 (2013).

potential federal preemption of state law could limit the reach of state law and the catalytic effect of the CCPA.[361] Second, while it is beyond the scope of this Article to address these arguments at length, recent First Amendment doctrine may create problems for the CCPA and similar laws.[362] Finally, we note the possibility that new models, notably including "trust" or "fiduciary" concepts, may take root and out-race both the GDPR and the CCPA to become the dominant catalyst for new privacy law.

1. The Dormant Commerce Clause

Because Internet regulation inevitably spills over jurisdictional lines, the dormant commerce clause plays an important role in disciplining any individual state's Internet regulation. As the Supreme Court has explained, "By prohibiting States from discriminating against or imposing excessive burdens on interstate commerce without congressional approval, [the dormant commerce clause] strikes at one of the chief evils that led to the adoption of the Constitution, namely, state tariffs and other laws that burdened interstate commerce."[363]

The dormant commerce clause imposes two separate conditions on regulatory spillovers: (1) the regulation at issue must not discriminate against interstate commerce,[364] and (2) it must not impose excessive burdens on interstate commerce.[365] The Supreme Court has offered a general principle: "Where [a] statute regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits."[366]

361. One of the authors of this Article has spoken to attorneys who are already planning to challenge the CCPA under the dormant commerce clause.

362. For an account of the ways that the First Amendment has limited U.S. privacy law, see Chander & Lê, *supra* note 137, at 516–22.

363. Comptroller of the Treasury v. Wynne, 135 S. Ct. 1787, 1794 (2015).

364. Dep't of Revenue v. Davis, 553 U.S. 328, 338 (2008) ("Under the . . . protocol for dormant Commerce Clause analysis, we ask whether a challenged law discriminates against interstate commerce.").

365. *Id.* ("A discriminatory law is virtually per se invalid, and will survive only if it advances a legitimate local purpose that cannot be adequately served by reasonable nondiscriminatory alternatives." (citations omitted) (internal quotation marks omitted)).

366. Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970). A finding that a statute is discriminatory could "be overcome by a showing that the State has no other means to advance a legitimate local purpose." United Haulers Ass'n v. Oneida-Herkimer Solid

Early cases challenging state Internet regulation on commerce clause grounds met with some success. Among the first was a 1997 decision in *American Library Ass'n v. Pataki*, overturning a New York statute that prohibited the transmission of obscene content to minors.[367] Into the early twenty-first century, a number of courts followed the lead of *Pataki* when evaluating similar statutes.[368] However, courts in other contexts have departed from *Pataki*'s approach, upholding, for example, state anti-spam statutes against commerce clause challenges.[369] A California appeals court "reject[ed] *Pataki*'s holding that any State regulation of Internet use violates the dormant commerce clause."[370]

A federal district court case from California seems particularly relevant. That case considered a dormant commerce clause challenge to an earlier California privacy law. In 2014, two Californians filed a class action against Omni Hotels, alleging a violation of the California Invasion of Privacy Act, a 1967 statute that makes it illegal to record a conversation without consent of both parties. Omni Hotels had set up its call center in Nebraska and complied fully with Nebraska law. Nebraska offered "an employer friendly law that exempts business from state wiretap statutes and gives employers the right to intercept, disclose and use e-mails in the ordinary course of business."[371] Omni argued that practically speaking, to comply with California law, it would have to notify all callers to its customer service about the recording, not just Californians, and that this constituted a per se violation of the commerce clause.[372]

Waste Mgmt. Auth., 550 U.S. 330, 338 (2007) (citing Maine v. Taylor, 477 U.S. 131, 138 (1986)).

367. Am. Librs. Ass'n v. Pataki, 969 F. Supp. 160, 169 (S.D.N.Y. 1997) ("[T]he Internet is one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether."). For a critique of this decision, see Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785, 786–87 (2001).

368. *See* ACLU v. Johnson, 194 F.3d 1149, 1161 (10th Cir. 1999); PSINet, Inc. v. Chapman, 362 F.3d 227 (4th Cir. 2004); Am. Booksellers Found. v. Dean, 342 F.3d 96, 104 (2d Cir. 2003); Se. Booksellers Ass'n v. McMaster, 282 F. Supp. 2d 389, 396 (D.S.C. 2003); Cyberspace Commc'ns, Inc. v. Engler, 142 F. Supp. 2d 827, 831 (E.D. Mich. 2001).

369. Washington v. Heckel, 24 P.3d 404, 413 (Wash. 2001); Ferguson v. Friendfinders, Inc., 115 Cal. Rptr. 2d 258, 268–69 (Ct. App. 2002).

370. *Ferguson*, 115 Cal. Rptr. 2d at 265.

371. Ades v. Omni Hotels Mgmt. Corp., 46 F. Supp. 3d 999, 1009–10 (C.D. Cal. 2014) (citation omitted).

372. *Id.* at 1012 ("Omni asserts that because the portability of mobile phone numbers makes it unfeasible to distinguish between Californian and non-Californian calls,

The court decided that the California law did not discriminate against out-of-state providers and went on to consider whether the statute unduly burdened interstate commerce.[373] It concluded, "Overall, the Court finds that the interests of California in the privacy of its consumers would be affected more by the application of Nebraska law than Nebraska's pro-business interests would be affected by the application of California law."[374] If Omni had prevailed, then Nebraska would have, wittingly or not, created the ideal conditions for a privacy race to the bottom: locate your call center in Nebraska and ignore privacy laws in the other jurisdictions where your callers reside. The district court's ruling avoided that result.

The CCPA does not appear to facially discriminate against interstate commerce.[375] The statute is written broadly to cover all businesses that deal with the private information of California residents, regardless of where they are located. As long as the California attorney general does not enforce the law against foreign companies in a discriminatory fashion, the CCPA would likely survive at least this prong of the doctrine.

The more realistic potential basis for a challenge would be the contention that the CCPA poses an "excessive burden" on interstate commerce. While it is possible that enforcement of the CCPA would occur in a manner that leads to such an excessive burden, a federal court may well conclude that the important interests at stake justified the CCPA's reasonable interventions across state lines. While businesses will complain of heightened compliance costs (as Omni complained of the California recording law), California's interests in protecting its residents' privacy may well justify those additional costs (as the court concluded in the Omni litigation).[376] However, uncertainty may yet deter other states from following the CCPA's lead, at least until any commerce clause challenge is resolved.

compliance with § 632.7 would force Omni to warn all callers, even those from single-consent states, that they could be recorded.").

373. *Id.*

374. *Id.*

375. As the Supreme Court has explained this aspect of dormant commerce clause doctrine, "'discrimination' simply means differential treatment of in-state and out-of-state economic interests that benefits the former and burdens the latter." United Haulers Ass'n v. Oneida-Herkimer Solid Waste Mgmt. Auth., 550 U.S. 330, 338–39 (2007) (quoting Or. Waste Sys. v. Dep't of Env't Quality, 511 U.S. 93, 99 (1994)).

376. *Omni Hotels Mgmt. Corp.*, 46 F. Supp. 3d at 1015.

2. Preemption

The CCPA could face another federalism-based challenge to its catalytic effect on other states, coming not from the courts but from Congress. State laws may be preempted when compliance with both state and federal mandates is impossible, and thus the introduction of a comprehensive federal privacy law could lead to preemption of part or all of the CCPA.[377] In many domains, Congress has adopted federal statutes that explicitly preempt state law in the same area, thus establishing uniform national standards on a topic.[378] A new federal statute with an express preemption clause would unravel the CCPA and any potential imitators at the state level. The sudden support of many industry groups for federal privacy law is likely motivated by the desire for just this outcome.[379]

Who should regulate privacy in the United States? Should states regulate privacy, should the federal government, or should both? There are thoughtful arguments for federal preemption of stricter state regulation, but we conclude that, on balance, the federal government should establish a national minimum, not a national maximum, for data privacy. This is what William Buzbee has called "floor preemption," allowing a one-way ratchet for standards—upwards—across the United States.[380] In fact, preemption may be the issue that kills proposed federal data privacy law, as powerful Californians and Democrats line up against the industry and Republicans. House Speaker Nancy Pelosi has vowed not to support any federal privacy law that provides fewer protections than the CCPA or indeed that preempts state law at all.[381] However, industry will be less interested in any federal law if it would not supersede the CCPA.

377. *See* Fla. Lime & Avocado Growers, Inc. v. Paul, 373 U.S. 132, 142–43 (1963).

378. *See, e.g.*, 17 U.S.C. § 301 (federal preemption provision of the Copyright Act of 1976); 21 U.S.C. § 343-1 (preempting state law concerning food labeling); 29 U.S.C. § 1144 (federal preemption provision of ERISA). *See generally* S. Candice Hoke, *Preemption Pathologies and Civic Republican Values*, 71 B.U. L. REV. 685, 700 (1991).

379. Writing of this dynamic in other contexts, Roderick Hills Jr. explains this apparent contradiction: "[F]ederal regulation frequently results from lobbying efforts by industry interests that oppose regulation. The apparent paradox of this statement dissolves when one takes into account industry's desire for uniformity of regulation." Roderick M. Hills, Jr., *Against Preemption: How Federalism Can Improve the National Legislative Process*, 82 N.Y.U. L. REV. 1, 20 (2007).

380. We borrow here the federal regulation framework set out by William Buzbee. William Buzbee, *Asymmetrical Regulation: Risk, Preemption, and the Floor/Ceiling Distinction*, 82 N.Y.U. L. REV. 1547, 1549 (2007).

381. Darius Tahir, *Pelosi Puts Privacy Marker Down*, POLITICO (Apr. 15, 2019, 10:00 AM), https://www.politico.com/newsletters/morning-ehealth/2019/04/15/pelosi-puts-privacy-marker-down-424986 [https://perma.cc/GJ39-7J9J] ("'We

There are virtues of a single national standard.[382] A national privacy law would establish uniformity across the region—rather than promising higher or lower protections depending on where a person is or where their data is processed or held.[383] It would facilitate data flows across state borders without requiring legal review of the laws of multiple jurisdictions. It would avoid the possibility of inconsistent mandates such as inconsistent notice requirements. Compliance costs likely would go down with only one legal standard.

But a federal preemption ceiling raises substantial concerns. It risks establishing a minimal level of privacy—one lower than that a state such as California could have demanded. Second, it may reduce existing enforcement capacity and expertise by sidelining state attorneys general who currently engage in significant enforcement of data privacy and data security law.[384] States have a long history of regulating privacy, much of it developed through the common law.[385] As Peter Swire has documented, existing federal privacy legislation generally serves as a regulatory floor, not a ceiling, including sector-specific preemption provisions adopted since the mid-1990s.[386] This reflects what Buzbee observes, that "[i]n most areas focused on regulation of risks . . . such as discrimination and efforts to enhance public welfare through regulation of environmental, occupational, and product risks, the protective 'one way ratchet' of floor preemption . . . has been the

cannot accept anything—for example, the Republicans would want preemption of state law. Well, that's just not going to happen,' [Pelosi] said. 'We in California are not going to say, "You pass a law that weakens what we did in California." That won't happen.'").

382. *See* Schwartz, *supra* note 76, at 423–27; Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868, 890–99 (2009).

383. Bellia, *supra* note 382, at 897.

384. Citron, *supra* note 87, at 798–99 (observing important role of states in privacy protection). To avoid this problem, any federal preemption could expressly retain an enforcement role for state attorneys general. *See* Peter Swire, *US Federal Privacy Preemption Part 2: Examining Preemption Proposals*, IAPP (Jan. 10, 2019), https://iapp.org/news/a/us-federal-privacy-preemption-part-2-examining-preemption-proposals [https://perma.cc/KQS5-KUV4].

385. *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 386–87 (1960).

386. Peter Swire, *US Federal Privacy Preemption Part 1: History of Federal Preemption of Stricter State Laws*, IAPP (Jan. 9, 2019), https://iapp.org/news/a/us-federal-privacy-preemption-part-1-history-of-federal-preemption-of-stricter-state-laws [https://perma.cc/R3WR-KF8C]. Both HIPAA and GINA serve as floors for state regulation, not ceilings. *See* 45 C.F.R. §§ 160.203–.205 (2019) (HIPAA); Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, § 2(5), 122 Stat. 881, 882–83. While the Fair Credit Reporting Act preempts some causes of action, it permits states to regulate identity theft. *See* Fair Credit Reporting Act, 15 U.S.C. § 1681t(a).

legislative and regulatory norm."[387] Most importantly, a federal preemption ceiling risks losing the regulatory innovation that continued state legislation in the area might supply.[388]

New federal privacy law could provide a nationwide floor, permitting states to intervene only to the extent that they raise privacy standards further. This allows for state innovations and experimentation. Writing of an earlier narrow California law that permits minors to delete certain information they uploaded to Internet sites, Heather Gerken and James Dawson argue that "[i]f the experiment proves workable, California's 'eraser' law may serve as a model for future regulation; if the experiment fails, policy-makers will be all the wiser."[389] Of course, a national floor sacrifices the uniformity of a single national standard, increasing compliance costs. But if any state offers a too-strict privacy rule—one that is too difficult to comply with given its business model—a corporation might simply refuse to provide it the relevant product or service.

Yet an additional option, raised previously by Paul Schwartz, might be a Clean Air Act model for data privacy: Congress could designate California as a kind of superregulator, granting it the exclusive right to deviate upwards from the federal privacy standard.[390] This would allow California alone the opportunity to innovate in the area and permit other states to choose either California's or the federal government's rules. It would lower regulatory compliance costs but preserve some room for upward regulation. However, it would forego the possibility of experimentation in other states, which might regulate differently, more clearly, or more stringently than California.[391] For example, this approach could destroy the prospect of a new "trust" model emerging from legislation such as the bill proposed in New York.[392]

Regulating in the face of substantial uncertainty will require a dynamic approach. Because of the pace of change in data gathering and processing, information privacy is a study in surprising turns. Data can be used in unexpected ways; its benefits and drawbacks are yet to

387. Buzbee, *supra* note 380, at 1552.

388. *See* Schwartz, *supra* note 76, at 917 (describing states as "laboratories for innovations in information privacy law").

389. Heather K. Gerken & James T. Dawson, *Living Under Someone Else's Law*, 36 DEMOCRACY J. 42, 47 (2015).

390. Schwartz, *supra* note 76, at 935 (referencing Ann Carlson's scholarship).

391. *See* VT. STAT. ANN. tit. 9, § 2453 (2017); 201 MASS. CODE REGS. 17 (2009); OR. REV. STAT. §§ 646A.600–.628 (2007).

392. *See supra* note 217 and accompanying text.

be fully discovered. The last handful of years have brought us tracking pixels, facial recognition, deep fakes, robot dogs, and even omnipresent satellites.[393] If a federal bill ossifies the rules, we may not be able to generate the regulations needed for yet more surprising turns. Of course, the federal government is capable of more agile versions of governance such as collaborative governance or responsive regulation, including through a regulatory agency like the FTC.[394]

If a federal law preempts state information privacy law, the CCPA might be lost to history, a mere footnote in the centuries of evolution of privacy law. Yet we believe it would still have served a critical role: prompting an omnibus federal privacy law for the first time since the dawn of the Internet age. As Gerken and Dawson observe, "By creating a spillover, a single innovative state can put an item on the national agenda even if nearly everyone else—Congress, interest groups, and other states—would prefer that the issue go away."[395] This would be a significant and long-lasting California Effect, indeed.

3. The First Amendment

Another potential constraint on the enactment of state and federal laws, and indeed the survival of the CCPA, is the First Amendment. Discussed above in the context of the differing regulatory settings of the European Union and United States, the First Amendment potentially poses constraints on drafters of U.S. privacy law. While in-depth coverage of these constraints—and their limitations—is outside of this Article's scope, we outline a few basic concepts here.

393. Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org [https://perma.cc/RB45-VME5]; Ry Crist, *Yes, the Robot Dog Ate Your Privacy*, CNET (June 28, 2019, 8:21 AM), https://www.cnet.com/news/yes-the-robot-dog-ate-your-privacy [https://perma.cc/ZZT8-W3CK]; Christopher Beam, *Soon, Satellites Will Be Able To Watch You Everywhere All the Time*, TECH. REV. (June 26, 2019, 8:21 AM), https://www.technologyreview.com/s/613748/satellites-threaten-privacy [https://perma.cc/2BAY-PCNT].

394. Charles Sabel and his coauthors argue for the virtue of a "rolling-rule regime" where "regulators use reports on proposals and outcomes to periodically reformulate minimum performance standards, desirable targets, and paths for moving from the former to the latter." Charles Sabel, Archon Fung & Bradley Karkkainen, *Beyond Backyard Environmentalism*, 24 BOS. REV. 4, 4 (1999). For other agile governance models, see Dennis D. Hirsch, *Going Dutch? Collaborative Dutch Privacy Regulation and the Lessons It Holds for U.S. Privacy Law*, 2013 MICH. ST. L. REV. 83, 151–60; McGeveran, *supra* note 20, at 979–85; and Lauren E. Willis, *Performance-Based Consumer Law*, 83 U. CHI. L. REV. 1309, 1330–35 (2015).

395. Gerken & Dawson, *supra* note 389, at 46.

The First Amendment protects freedom of speech. It also protects expressive activity (speech mixed with action) and penumbral activity necessary for speech to take place (such as the placement of newspaper kiosks to distribute newspapers or the purchase of pen and paper).[396] A series of First Amendment cases on public records established significant limitations on laws restricting the distribution of lawfully obtained information.[397] More recently, the Supreme Court applied the First Amendment to find unconstitutional a Vermont law regulating the sale of prescription drug user data.[398] And in 2018, the Supreme Court found unconstitutional a series of disclosure requirements aimed at protecting patients from pro-life organizations posing as abortion providers in a decision that could have consequences for other disclosure-based consumer protection regimes.[399]

Recently, the expansive coverage and protection of First Amendment doctrine has led some to decry its potential deregulatory effects.[400] On the other hand, privacy scholars have noted that the First Amendment also provides arguments for effective privacy law, as a lack of privacy can chill free expression.[401] Commentators disagree on

396. *See* Margot E. Kaminski, *Privacy and the Right To Record*, 97 B.U. L. REV. 167, 189 (2017).

397. Cox Broad. Corp. v. Cohn, 420 U.S. 469, 493–95 (1975); *see also* Volokh, *supra* note 137, at 1116–17.

398. Sorrell v. IMS Health, Inc., 564 U.S. 552 (2011); *see* Chander, *supra* note 137 (arguing that *Sorrell* demonstrates "the seriousness of First Amendment constraints on privacy regulations on information intermediaries"). Cases such as *Florida Star v. B.J.F.*, 491 U.S. 524 (1989), *Cox Broadcasting Corp.*, 420 U.S. 469, and *Smith v. Daily Mail Publishing*, 443 U.S. 97 (1979), can be read to stand for the principle that once information is legally distributed, government cannot restrict its use absent state interest of the highest order. However, a number of scholars argue that privacy laws can pass First Amendment muster. Balkin, *supra* note 137, at 1189. *But see* Volokh, *supra* note 137, at 1051.

399. *See* Amy Howe, *Opinion Analysis: Divided Court Rules for Anti-Abortion Pregnancy Centers in Challenge to California Law*, SCOTUSBLOG (June 26, 2018, 4:02 PM), https://www.scotusblog.com/2018/06/opinion-analysis-divided-court-rules-for-anti-abortion-pregnancy-centers-in-challenge-to-california-law [https://perma.cc/Q7WJ-VFZB].

400. *See* Shanor, *supra* note 185, at 133; MARY ANNE FRANKS, THE CULT OF THE CONSTITUTION 105 (2019).

401. *See, e.g.*, Marc Jonathan Blitz, *Constitutional Safeguards for Silent Experiments in Living: Libraries, the Right To Read, and a First Amendment Theory for an Unaccompanied Right To Receive Information*, 74 UMKC L. REV. 799, 800 (2006); Julie E. Cohen, *A Right To Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1003–19 (1996); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 393–94 (2008); Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 467 (2015); Skinner-Thompson, *supra* note 185; Anupam Chander, *Youthful*

how much of data privacy law might survive First Amendment challenges.[402] Through court challenges or through its expanding cultural penumbra, the First Amendment may chill the spread of the CCPA.

CONCLUSION

What does all of this mean for our privacy? The end result of the race between the GDPR and the CCPA may well be a hybrid of both. The de facto privacy law governing global corporations may be the strictest aspects of both California and European law—a figurative, but not literal, highest common denominator.[403] Thanks to a Brussels Effect, some large global enterprises would adhere to GDPR norms. But thanks to a California Effect in one of the various forms we have described, that state would have outsized influence on the substance of U.S. privacy law—as Alastair Mactaggart has boasted, "Under [the CCPA], the attorney general of California will become the chief privacy officer of the United States of America."[404] Many corporations will find themselves comporting with both regimes simultaneously, rather than configuring their services or offerings by jurisdiction. Call this hybrid the "CDPR"—the CCPA + the GDPR.

But this de facto reality only goes so far. Those outside either jurisdiction will not be able to assert those rights directly with either regulators or courts. Both regimes grant individual rights only to their own residents. For example, the much-embattled facial recognition company Clearview provides only Californians and European Union residents the opportunity to opt out.[405]

We predict that within the United States, the CCPA will yet continue to drive both businesses and legislatures. The CCPA, both de facto and de jure, will likely call the tune for the march of a new American data privacy spreading to other jurisdictions. California, not Brussels, has emerged as the superregulator of U.S. privacy law.

Indiscretion in an Internet Age, *in* THE OFFENSIVE INTERNET 124, 134 (Saul Levmore & Martha Nussbaum eds., 2010).

402. For a sampling of this extensive debate, see Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 60–61 (2014); Richards, *supra* note 137, at 1521–22; and Volokh, *supra* note 137, at 1050–51.

403. A more mathematical analogy might be two curves mapping out various issues on the *x* axis with *y* being the level of strictness for each issue, resulting in a third operational curve consisting of the highest peaks between the two curves.

404. Confessore, *supra* note 295.

405. *Privacy Request Forms*, CLEARVIEW.AI, https://clearview.ai/privacy/requests [https://perma.cc/BU9L-8MG7] (including a separate reference to the UK necessitated by Brexit).