2019

Catalyzing Privacy Law

Anupam Chander
Georgetown University Law Center, ac1931@georgetown.edu

Margot E. Kaminski
University of Colorado Law School, margot.kaminski@colorado.edu

William McGeveran
University of Minnesota Law School, billmcg@umn.edu

CATALYZING PRIVACY LAW

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

The United States famously lacks a comprehensive federal data privacy law. In the past year, however, over half the states have proposed broad privacy bills or have established task forces to propose possible privacy legislation. Meanwhile, congressional committees are holding hearings on multiple privacy bills. What is catalyzing this legislative momentum? Some believe that Europe's General Data Protection Regulation (GDPR), which came into force in 2018, is the driving factor. But with the California Consumer Privacy Act (CCPA) which took effect in January 2020, California has emerged as an alternate contender in the race to set the new standard for privacy.

Our close comparison of the GDPR and California's privacy law reveals that the California law is not GDPR-lite: it retains a fundamentally American approach to information privacy. Reviewing the literature on regulatory competition, we argue that California, not Brussels, is catalyzing privacy law across the United States. And what is happening is not a simple story of powerful state actors. It is more accurately characterized as the result of individual networked norm entrepreneurs, influenced and even empowered by data globalization. Our study helps explain the puzzle of why Europe's data privacy approach failed to spur US legislation for over two decades. Finally, our study answers critical questions of practical interest to individuals—who will protect my privacy?—and to businesses—whose rules should I follow?

[*] 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; Privacy Director, 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, and by professors at faculty workshops at 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. Anupam Chander gratefully acknowledges a Google Research Award for related research. We received excellent research help from Shiwen Cai, Lydia Davenport, Xinge He, Romina Montellano Morales, Paige Papandrea, Caroline Schmitz, and librarian Heather Casey. The views herein (and all errors) are the authors' alone.

Table of Contents

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. A month later, California passed the California Consumer Privacy Act ("CCPA"), establishing the nation's most stringent omnibus privacy protections, effective as of January 1, 2020.[2] California, the home of many of the world's largest data-based enterprises, had emerged as a dark horse contender in the privacy regulator race. Then, in the past year, state after state considered broad data privacy legislation,[3] and eleven comprehensive federal privacy bills were introduced in Congress.[4]

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—countries such as Nigeria have joined to make 142 countries and counting with a broad privacy law, often modeled closely on the GDPR.[5] Scholars writing insightfully about the global race to information privacy have

---

[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.

[2] *See* 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; California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. (2018).

[3] See infra Section III(B)(1).

[4] *See* S. 1214: Privacy Bill of Rights Act (Sen. Edward Markey); S. 189: Social Media Privacy Protection and Consumer Rights Act of 2019 (Sen. Amy Klobuchar); S. 806: Own Your Own Data Act (Sen. John Kennedy); H.R. 1282: Data Accountability and Trust Act (Rep. Bobby Rush); H.R. 2013: Information Transparency & Personal Data Control Act (Rep. Suzan DelBene); H.R. 4978: Online Privacy Act (Reps. Anna Eshoo and Zoe Lofgren); S.1116: Balancing the Rights Of Web Surfers Equally and Responsibly Act (Sen. Blackburn); S. 142: American Data Dissemination (ADD) Act (Sen. Marco Rubio); Consumer Online Privacy Rights Act (Sen. Cantwell); S.1578: Do Not Track Act (Sen. Hawley); S.1951: Designing Accounting Safeguards to Help Broaden Oversight and Regulations on Data Act (Sens. Hawley & Warner). *See also* S.3744: Data Care Act of 2018 (Sen. Brian Schatz); Sen. Ron Wyden's Consumer Data Protection Act (Nov. 2018); Sens. Markey & Blumenthal's CONSENT Act (Apr. 2018).

[5] The exact number of countries with comprehensive data protection laws depends on one's characterization of any particular law. While Graham Greenleaf identifies 142 countries and jurisdictions with such laws, Article 19 counts 130. The most recent laws are modeled on the GDPR. *See, e.g.*, Nigeria Data Protection Regulation 2019, https://nitda.gov.ng/wp-content/uploads/2019/01/NigeriaDataProtectionRegulation.pdf. Among other differences, the Nigerian law permits fines up to two percent of global turnover, not the four percent permitted by the GDPR.

tracked the spread of data privacy laws across the world, noting Europe's influence on these developments.[6] In a recent article, Paul Schwartz observes that the European Union pioneered international privacy law to enable commerce across the European Union itself.[7] He argues that other countries have largely adopted the European Union's data privacy model, reflecting its "success in the marketplace of ideas."[8]

Schwartz cites the CCPA as an example of Europe's success.[9] Journalists reporting on the CCPA's enactment, too, have frequently referred to it as "GDPR-lite"[10] and "California's Version of GDPR."[11] And as the push for federal legislation intensifies, many characterize it as a national response to the GDPR.[12]

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

---

[6] 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 & New Delhi*, *25 May 2018*, 18-56 UNSW L. RES. PAPER 8 Pages Posted, 3 (May 24, 2018). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3184548.

[7] Paul Schwartz, *Global Data Privacy: The EU Way*, 94 NYU L. REV. 771, 810 (2019) ("Its 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 that begins with a response to internal political considerations."). Available at https://ssrn.com/abstract=3338954.

[8] *Id.* at 818.

[9] *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 Protection Act (CCPA) of 2018.").

[10] *See, e.g.,* Kayvan Alikhani, *Regulatory Disruption: Is Your Business Ready to Comply with the CCPA?*, FORBES (June 6, 2019), https://www.forbes.com/sites/forbestechcouncil/2019/06/06/regulatory-disruption-is-your-business-ready-to-comply-with-the-ccpa/#e5a21e545ee6

[11] *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.

[12] *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), https://www.cnbc.com/2019/05/23/gdpr-one-year-on-ceos-politicians-push-for-us-federal-privacy-law.html.

European antecedent. 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. A subnational jurisdiction, California—itself driven by networked individuals—is now driving privacy in a significant part of the world, seeming to rival the influence of a supranational jurisdiction, the European Union. 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."[13]

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 purportedly irreconcilable regimes.[14] Now we are witnessing what might be characterized as a regulatory race on both sides of the ocean.[15] 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.[16]

This study is also of great practical interest, answering twin questions for individuals and businesses alike: For businesses, whose laws should I follow? For individuals, who will protect my privacy? Answering Studying these questions leads, in turn, to another set of inquiries about the ways 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 these questions have implications not only for the shape of information privacy law, but for understanding inter-jurisdictional regulatory

---

[13] See *infra* note 210 and accompanying text.

[14] *See* Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law: A Study of United States Data Protection 1* (1996); Peter P. Swire & Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce,* and the Europrean Privacy Directive app. A at 213 (1998). *But see* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 281 (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 despite differences in the law on the books).

[15] *See, e.g.*, Sara Merken, *States Follow EU, California in Push for Consumer Privacy Laws (1)*, BLOOMBERG LAW (last updated 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.

[16] 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").

dynamics in the digital economy. While data shares some characteristics with cars, pollution, and corporate charters—all the subject of prior globalizations—it also differs because of its simultaneous global and instantaneous 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, this story 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 the information age.

I. SUPERREGULATORS

US privacy law can be periodized as follows: 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. After the CCPA, Congress and state legislatures across the country saw a huge rush of legislative activity around data privacy.

What is prompting this new interest in privacy lawmaking in the United States? Many point to the 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.[17] The GDPR also prompted global companies to establish expensive compliance programs and infrastructure. 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 Anu Bradford labels the "Brussels Effect."[18] But if this is the case, why did it take so long?[19]

[17] Schwartz, *supra* note 7, at 783.

[18] Mark Scott & Laurens Cerulus, *Europe's new data protection rules export privacy standards worldwide*, POLITICO (Jan. 31 2018), https://www.politico.eu/article/europe-data-protection-

Bradford, after all, coined the phrase in 2012, describing a EU directive promulgated in 1995. 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.[20] Often these effects are named for the places where they were first detected: Delaware, California, or Brussels. 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 greatest depth in corporate law.[21] 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.[22] Some dubbed this the "Delaware Effect," because two thirds of all Fortune 500 companies are incorporated in that state.[23]

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.[24] Thus, a corporation operating principally in

---

privacy-standards-gdpr-general-protection-data-regulation/.

[19] 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).

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

[21] *See, e.g.*, William L. Cary, *Federalism and Corporate Law: Reflections upon Delaware*, 83 YALE L.J. 663, 664 (1974).

[22] 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." Louis K. Liggett Co. v. Lee, 288 U.S. 517, 557–60, 53 S. Ct. 481, 493–94 (1933).

[23] *See* Del. Div. of Corps., *Annual Report Statistics (FY 2018)*, DELAWARE.GOV, https://corp.delaware.gov/stats/. And this does not apply only to large established corporations: in 2017, over 80% of initial public offerings in the U.S. used Delaware as a corporate home. *Id.*

[24] VantagePoint Venture Partners 1996 v. Examen, Inc., 871 A.2d 1108, 1112 (Del. 2005) ("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

California or Kansas can incorporate in Delaware and be assured that relations between its shareholders, directors, and officers will be governed by Delaware law. Without this "internal affairs" rule, a corporation might have to conform to the corporate law 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.[25]

The classic analyses posited that Delaware had cornered the market for incorporations through dubious efforts to favor corporate officers and directors.[26] Ralph Winter famously rejected this claim of an inevitable race to the bottom. Winter argued 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.[27] Where some had derided Delaware's efforts as "law for sale,"[28] Roberta Romano argued that Delaware's efforts were part of the genius of American law. 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. As one Delaware Chancery Court judge noted, "Delaware has a substantial interest in providing

---

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."); Rogers v. Guar. Tr. Co. of New York, 288 U.S. 123, 130 (1933) ("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.").

[25] 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. Such an approach would not defer to the mailbox incorporation available in Delaware. It This rule would still typically result in a single regulator—but this it would make gaming the law more difficult. 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. This opens up the possibility of regulatory competition for corporate law in Europe as well.

[26] William L. Cary, *Federalism and Corporate Law: Reflections Upon Delaware*, 83 YALE L.J. 663 (1974). According to this view, states such as Delaware might wish to attract incorporations because of the franchise tax—the annual fees they pay to maintain their incorporation in that state. Indeed, Delaware would come to fund one-quarter of its budget through this means. STEPHEN M. BAINBRIDGE, CORPORATE GOVERNANCE AFTER THE FINANCIAL CRISIS 24 (2012) (noting that "Delaware generates $740–800 million per year in franchise taxes, which amounts to a quarter of the state's budget"); *Financial Overview (FY 2018)*, DELAWARE.GOV, https://budget.delaware.gov/budget/fy2018/documents/operating/financial-overview.pdf (estimating franchise taxes of $975.0 million for Fiscal Year 2017 and $992.6 million for Fiscal Year 2018).

[27] Ralph Winter, *State Law, Shareholder Protection, and the Theory of the Corporation*, 6 J. LEGAL STUD. 251, 257 (1977) ("If management is to secure initial capital ... it must attract investors away from the almost infinite variety of competing opportunities").

[28] Comment, *Law for Sale: A Study of the Delaware Corporation Law of 1967*, 117 U. PA. L. REV. 861 (1969).

an effective forum for litigating disputes involving the internal affairs of Delaware corporations."[29] Regulatory 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. Both the substantive law and the regulatory techniques of those jurisdictions may then gain influence outside its borders, as other regulators defer to them. While this arrangement could result in a race to the bottom, it could also enable the emergence of highly specialized 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."[30] Instead of a race to the bottom (what he called a "Delaware Effect") he offered that regulatory competition might result in a "California Effect," demonstrating "the critical role of powerful and wealthy 'green' political jurisdictions in promoting a regulatory 'race to the top' among their trading partners."[31] Unlike the Delaware Effect, in which a jurisdiction tempts companies to opt in to 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. 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

---

[29] 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." ROBERTO ROMANO, THE GENIUS OF AMERICAN CORPORATE LAW 38–39 (1993).

[30] DAVID VOGEL & ROBERT KAGAN, DYNAMICS OF REGULATORY CHANGE HOW GLOBALIZATION AFFECTS NATIONAL REGULATORY POLICIES (2004); DAVID VOGEL, TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY (Harvard U. Press 1995) (hereinafter "VOGEL, TRADING UP").

[31] VOGEL, TRADING UP, *supra* note 30, at 6..

occur.[32] First, a race to the top is more likely to be triggered if the standards are supported by a coalition joining public interest groups with regulated companies that wish to impose the same regulatory costs on their competitors in other jurisdictions. 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. 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.

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.[33] 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.[34] The Clean Air Act of 1970 explicitly recognized California as a superregulator: it became the only state allowed set stricter-than-federal standards, and other states could then opt to follow California's standards.[35] Twelve eastern states and the District of Columbia announced in 1994 that they would follow California.[36] Auto emissions rules illustrate all three of Vogel's conditions.

The mechanism of the California Effect differs from the Delaware Effect. Under the Delaware Effect, a second jurisdiction defers to the regulatory choices of the superregulator, magnifying the impact of those choices. Under the California Effect, other jurisdictions themselves adopt the same rules as the superregulator jurisdiction.

C. The Brussels Effect

The formation of the European Union in the late twentieth century saw the emergence of another superregulator: 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

---

[32] VOGEL, TRADING UP, *supra* note 30 at 260–68. *See also* Sebastiaan Princen, *Trading up in the Transatlantic Relationship*, 24 J. PUB. POL. 127, 128 (2004).

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

[34] *Id.*

[35] *See* Rocky Mountain Farmers Union v. Corey, 730 F.3d 1070, 1079 (9th Cir. 2015) ("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 33, at 1134; Nicholas Bryner & Meredith Hankins, *Why California gets to write its own auto emissions standards: 5 questions answered*, THE CONVERSATION (Apr. 6, 2018), https://theconversation.com/why-california-gets-to-write-its-own-auto-emissions-standards-5-questions-answered-94379.

[36] Peter P. Swire, *The Race to Laxity and the Race to Undesirability: Explaining Failures in Competition Among Jurisdictions in Environmental Law*, 14 YALE J. ON REG. 67, 82 (1996).

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."[37]

Where the California Effect depends on jurisdictions racing to raise 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.[38] Bradford observes, "[T]he Brussels Effect is more about one jurisdiction's ability to override others than it is about triggering an upward race."[39]

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."[40] Like Vogel, Bradford identifies conditions under which a Brussels Effect is more likely to occur.[41] First, as with the California Effect, the Brussels Effect is likely to occur only when the unilateral regulator represents a large and attractive market. 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.[42] 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.

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. 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 web sites began posting globally applicable privacy policies partly in response to a 1990s California law requiring they do so, this was a Brussels Effect triggered by a California law. We will delve into these catalytic effects in privacy law more fully below. First, however, we explain the substance of the GDPR and the CCPA, showing that the differences between them mean there is more than one contender to be a data privacy superregulator.

II. GDPR VERSUS CCPA

---

[37] Bradford, *supra* note 19.

[38] *Id.* at 4 ("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 standard Europe's unilateral power to regulate global markets.").

[39] *Id.* at 8.

[40] *Id.* at 6.

[41] *Id.* at 5. *See also* Schwartz, *supra* note 7, at 780.

[42] Bradford, *supra* note 37, at 5.

Which data privacy regime is driving the wave of legislative activity related to data privacy across the U.S., and what is the mechanism of that influence? To answer this question, we need first to understand the two regimes. This Part reveals both the 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. 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 real consequences.

A paperback of the GDPR runs some 130 pages, its sections literally divided into chapters.[43] The CCPA, by contrast, runs around 25 pages. If the GDPR is a doctoral thesis, the CCPA is a term paper written the night before the deadline.

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 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 E.U.-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.[44] This reflects a fundamental difference in approach: "data protection" is universal in Europe, while most American law focuses on "consumer protection."[45] 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

[43] https://www.amazon.com/European-Data-Protection-Law-Regulation/dp/1533170835

[44] *See* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEORGETOWN L. J. 115, 138, 147 (2017); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004). *See also* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 505–06 (1995); Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 905 (2009); CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION 2–3 (2d ed. 2007).

[45] McGeveran, *supra* note 14, 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").

on Human Rights and the E.U. Charter. This places data protection rights on the same plane as free speech or due process.[46] 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.

In the U.S., by contrast, privacy law usually follows a "consumer protection" model, with regulators focused on ensuring that consumers receive the benefit of their bargain in individual business-to-consumer transactions. The consumer protection model often relies on the much-criticized premise that disclosure and a right of refusal (so-called "notice and choice") adequately empower consumers.[47] 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 presupposed that entities may collect and use personal data however they wish by default, unless a specific legal rule forbids a particular practice.

A second difference between Europe and the United States is that U.S. privacy law has always been fragmented and "sectoral."[48] Different statutes are enforced by different regulators in different areas 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.[49] 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, largely following a consumer protection model.[50] 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. While these data protection laws contain extra protections for especially sensitive information, their basic human rights frameworks impose uniform requirements every time personal data is collected, processed, or transferred. 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

---

[46] European Convention on Human Rights, Art. 8; Charter of Fundamental Rights of the European Union, Arts. 7, 8.

[47] *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).

[48] *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 505–06 (1995); Schwartz, *Preemption and Privacy*, *supra* note 44.

[49] Health Insurance Portability and Accountability Act, 45 C.F.R. § Parts 160, 162, and 164; Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501 et seq.

[50] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016).

individuals—anyone engaged in the "processing" of personal data.[51]

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. This differs from many existing regulatory models in the United States. For example, because the FTC's general consumer protection authority focuses on the relationship between individuals and companies, it has little power over data brokers who obtain individual information from other companies or public sources rather than from consumers themselves.[52] The CCPA directly regulates data brokers independent of their commercial relationships—a critical move targeting an industry that has great potential for abuse.[53]

At first glance, too, some core elements of the CCPA echo aspects of the GDPR. Both laws define personal information very broadly, far beyond most existing U.S. privacy laws. Both laws foundationally emphasize transparency, reflecting the Fair Information Principles (FIPS) on which many data privacy regimes in both Europe and the U.S. are built. And both laws share the contours of a number of additional individual rights.

In the past, narrow definitions of personal information have sharply limited the effect of many U.S. privacy laws.[54] Under most U.S. laws, only

---

[51] General Data Protection Regulation 2016/679, art. 4(2), 2016 O.J. (L 119) (EU) (hereinafter "GDPR") (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* Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW e.V., C-40/17 (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, Bodil Lindqvist v. Åklagarkammaren i Jönköping, 2003 E.C.R. I-12971.

[52] Fed. Trade Comm'n, *Data Brokers: A Call for Transparency and Accountability* (2014).

[53] 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 et seq.

[54] 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*

certain types of defined 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.[55] 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."[56] 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.[57] The GDPR's recitals proclaim it a fundamental tenet of data protection law that people should know that their data have been collected, and be able to understand the extent to which that information is processed.[58] The CCPA likewise focuses on giving people notice and 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."[59]

Beyond this hortatory language, both laws embed transparency principles in their requirements. Under the GDPR, organizations must provide individuals both notice and access. 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.[60] Organizations that collect personal information from a third party must provide such notice as well.[61] And all these disclosures must be clear and intelligible.[62] The GDPR also establishes a right of individual access,[63] building on "subject access rights" that have been in place at least since the 1990s throughout Europe under the Data Protection Directive.[64] In response to an individual's access request, data controllers must disclose, among other things:

New Concept of Personally Identifiable Information, 86 N.Y.U. L.Q. REV. 1814 (2011).

[55] GDPR, *supra* note 51, art. 4(1).

[56] CAL. CIV. CODE § 1798.140(o)(1).

[57] GDPR, *supra* note 51, art. 5(1)(a).

[58] GDPR, *supra* note 51, Recital 39.

[59] See Cal. A.B. 375 Sec. 2(i).

[60] GDPR, *supra* note 51, art. 13, 14.

[61] *Id.* art. 14(1)(d).

[62] *Id.* art. 12.

[63] GDPR, *supra* note 51, art. 15.

[64] Jef Ausloos & Pierre Dewitte, *Shattering One-Way Mirrors. Data Subject Access Rights in Practice*, INTERNATIONAL DATA PRIVACY LAW (2018) 8(1), pp.4–28.

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.[65] Additionally, they must provide a copy of the data itself, in a commonly used electronic form.[66]

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 (but not the recipients of the data or the storage period). This mandate goes well beyond notice requirements in prior U.S. law, such as a California statute requiring web sites to post privacy policies.[67] And like the GDPR, the CCPA 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.[68] Additionally, 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.[69] 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.[70] This represents a significant advance from very limited rights under previous law, such as access to credit scoring information and the annual free credit report.[71]

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/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.[72] This right is aimed at giving individuals more control over their data and more choices about IT services[73] but is also understood to potentially

---

[65] GDPR, *supra* note 51, art. 15.

[66] *Id.* art. 15 (3). *See also* Rec. 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").

[67] CAL. CIV. CODE § 22575.

[68] *Id.* at §§ 1798.100(a) and 1798.110(a).

[69] *Id.* at § 1798.110(a).

[70] 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 CAL. CIV. CODE §§ 1798.100(a); 1798.110(a); 1798.115(a).

[71] 15 U.S.C. § 1681g.

[72] GDPR, *supra* note 51, art. 20, Recital 68; Article 29 Working Party Guidelines on the Right to Data Portability (2017) (hereafter "WP29 Portability Guidelines").

[73] WP29 Portability Guidelines, *supra* note 72, at 3–4.

enhance competition.[74] The CCPA quietly creates a data portability "right" of its own: personal data delivered electronically in response to an access request "shall be in a portable and… readily usable format."[75] 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.[76]

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.[77] If a business has actual knowledge that a consumer is 16 years old or younger, it must obtain affirmative authorization ("opt-in") for any sale of personal information.[78] The GDPR, by comparison, establishes three analogous rights: the right to restrict data processing,[79] the right to object to data processing,[80] and the right to withdraw consent.[81] 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.[82] Both regimes contain, too, a duty of nondiscrimination: companies cannot discriminate against individuals who choose to exercise the right to opt out.[83] This means that a business cannot, for example, deny goods or services, charge different rates, impose penalties, or provide a different level of services to customers who opt out of data transactions.

The GDPR famously contains a right to erasure, also known as the "right to be forgotten."[84] The CCPA, too, creates a right to deletion.[85] The GDPR's right to erasure gives individuals the right to obtain the erasure of personal

---

[74] *Id.* at 4.

[75] CAL. CIV. CODE § 1798.100(d).

[76] WP29 Portability Guideline, *supra* note 72, at 10; CAL. CIV. CODE § 1798.140(o), (1), (k), (m).

[77] 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* 9 V.S.A. ch. 62, subch. 5 (Vt.).

[78] CAL. CIV. CODE § 1798.120(d). That opt-in consent must come from a parent or guardian if the individual is under 13 years old, minors between 13 and 16 years old may provide their own opt-in consent. *Id.*

[79] GDPR, *supra* note 51, art. 18.

[80] *Id.* art. 21, Recital 60, 70.

[81] *Id.* art. 7(3).

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

[83] CAL. CIV. CODE § 1798.125; GDPR, *supra* note 51, Recital 42; Guidelines on Transparency under Regulation 2016/679, at 11, 2018 O.J. (WP260) (EC) ("giving as an example of "consent without detriment" that a company may "show that a service includes the possibility to withdraw without negative consequences, e.g. without the performance of the service being downgraded to the detriment of the user").

[84] General Data Protection Regulation 2016/679, art. 17, 2016 O.J. (L 119) (EU). *See generally* MEG LETA JONES, CTRL + Z: THE RIGHT TO BE FORGOTTEN (2016).

[85] CAL. CIV. CODE § 1798.105

data both from companies with which they have a direct consumer relationship and from third parties, under certain circumstances.[86] There are exceptions to the right to erasure, including freedom of expression and public interest in the area of public health.[87] 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.[88] The CCPA, by contrast, creates a 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.[89] This more restricted scope may be a nod to First Amendment law and values in the United States, which may constrain erasure requirements imposed on third parties.[90]

In sum, the CCPA moves closer to a data protection regime like the GDPR in certain ways, which help explain the 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, however, none of these shifts goes nearly as far as the GDPR—and as we shall see in the next section, all of them are overshadowed by important substantive differences between the two models.

C. Substantive Differences

Once an analysis moves beyond these basic similarities, however, it

---

[86] GDPR, *supra* note 51, 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 invididual 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).

[87] *Id.* art. 17(3)(a), (c).

[88] *See* Case C–131/12, *Google Spain SL v. AEPD*, 2014 E.C.R. 317; 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); S. Kulk & F.Z. Borgesius, *Google Spain v. González: Did the Court Forget about Freedom of Expression?*, 5 EUROPEAN J. OF RISK REG. 3, 389–98 (2014). [Note: add IVIR research when complete.]

[89] CAL. CIV. CODE § 1798.105(a).

[90] Sorrell v. IMS, 564 U.S. 552 (2011). *See* Anupam Chander, Free *Speech*, 100 IOWA L. REV. 501, 522 (arguing that *Sorrell* demonstrates "the seriousness of First Amendment constraints on privacy regulations on information intermediaries"). *Cases such as* Florida Star v. BJF, 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 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).

becomes clear that the CCPA regime differs sharply from the GDPR. First and perhaps most important, 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. It 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,[91] and back even further to national data protection laws in many European countries dating from the 1970s and 1980s.[92]

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,[93] or the processing falls under one of the other five enumerated categories of lawful processing.[94] The CCPA does not require that processing be lawful. 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. This is likely the single most meaningful practical 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.[95] The GDPR requires that personal data may be collected only for "specified, explicit and legitimate purposes," stated at the time of collection.[96] 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

---

[91] Directive 95/46/EC, 1995 O.J. (L 281) (EU).

[92] *See, e.g.* 1978 Bundesdatenschutzgesetz, (Germany); Stat. no. 78-17 of 6 Jan. 1978 (France); Data Protection Act 1984 (U.K.).

[93] *Id.* art. 6(1)(a).

[94] *Id.* art. 6(1)(a)-(f).

[95] *Id.* art. 5(1).

[96] *Id.* art. 5(1)(b).

(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.

The CCPA imposes few requirements concerning the purposes for data collection or the proportionality of data handling to those purposes. The CCPA does not even go as far as HIPAA, which requires that disclosures of patient data be the "minimum necessary" to achieve a purpose.[97] Instead, the CCPA requires a business to provide notice if it is "using personal information collected for additional purposes."[98] This rule doesn't 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 divergence in their animating principles influences the two laws' treatment of individual rights as well. 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[99] and by granting individuals robust rights throughout the life cycle of data processing, including: the right to rectification of incorrect information;[100] the right to prevent automated individual decision-making and to receive explanation of any automated decision;[101] and broader rights related to erasure of data and withdrawal of consent. Additionally, the GDPR's requirement of lawful processing bestows more individual control than the CCPA.[102] The CCPA relies primarily on transparency, and grants individuals only the two limited rights discussed above: to opt out of sale and to request deletion.

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

---

97 45 C.F.R. §§ 164.502(b), 164.514(d).

98 CAL. CIV. CODE § 1798.100(b).

99 And 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 51; Article 29 of the Data Protection Working Party, Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation, 17/EN. WP 251rev.01 (Oct. 3, 2017) (hereinafter "A29WP, Guidelines on Automated Individual Decision-making").

100 GDPR, *supra* note 51, art. 16..

101 *Id.* art. 22. *See also* Margot E. Kaminski, *The Right to Explanation, Explained*, 34 BERK. TECH. L. J. 189, 201 (2019).

102 GDPR, *supra* note 51, art. 6(1)(a).

processes.[103] Whether it will succeed is another question, but its aims are far broader, and approach far deeper, than the CCPA's. The CCPA lacks the GDPR's affirmative regulatory requirements—ranging from data minimization to risk assessments to recording requirements—imposed on companies even where there is not a corresponding individual right.[104] Four other differences listed below further demonstrate that the CCPA is not the same sort of law as the GDPR.

The second difference 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.[105] The CCPA applies only to businesses, and then 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.[106] Here again, the two laws reflect the 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.[107] 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, HIPAA and the Children's Online Privacy Protection Act (COPPA). There have been proposals in the California Legislature to add authorize private CCPA lawsuits, but for now only the state Attorney General may enforce the most portions of

---

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

[104] GDPR, *supra* note 51, art. 5(2). *See also* Kaminski, supra note 103.

[105] GDPR, *supra* note 51, art. 2(1).

[106] CAL. CIV. CODE §§ 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, *et seq*. The CCPA targets three kinds of commercial entities as "businesses." CAL. CIV. CODE § 1798.140(c). It targets 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. It targets 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 it targets 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.

[107] GDPR, *supra* note 51, art. 83; CAL. CIV. CODE § 1798.155(a), (b).

the law.[108] Spurred by a constitutionally guaranteed right of redress for violations of individual rights, the GDPR does enable individual rights of action[109] as well as enforcement by national data protection regulatory authorities and coordination of their efforts through a European Data Protection Board.[110]

Fourth, the regulatory styles of the two regimes differ greatly. This can create both substantive and cultural gaps. While the CCPA creates limited but granular requirements, and tasks the state AG with providing more details, the GDPR largely regulates by issuing broad standards and then relying on various forms of guidance (the Recitals, European Data Protection Board Guidelines) and cooperation with companies to fill in the details.[111] In other words, the GDPR's approach to regulating largely constitutes collaborative governance, also known as "co-regulation" or "new governance."[112] The GDPR's vagueness is arguably deliberate. It allows companies and sectors to fill in details of how to comply with the law over time, whether formally through establishing codes of conduct or certification mechanisms,[113] or informally through self-regulation, recording and reporting, impact assessments, and ongoing conversations with regulators.[114] By contrast, the CCPA's granularity appears, in places, to value detail and certainty over flexibility.

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 number and website address for access requests.[115] 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 sale of personal data. This example demonstrates a stylistic difference between the two laws that could have real consequences for businesses trying to comply with both. Often, the CCPA is so detailed that it creates the possibility of divergence between the laws, even where in broad strokes the two might appear similar.

Finally, the two laws differ greatly in the backdrop against which they were each enacted, or what we call the legal setting. While the CCPA is constrained by increasingly deregulatory First Amendment doctrine, the GDPR is backed

---

[108] The CCPA does authorize private lawsuits for a narrow set of claims related to data security breaches.

[109] GDPR, *supra* note 51, art. 77–79.

[110] *Id.* art. 51–59.

[111] *See* Kaminski, *supra* note 103; McGeveran, *supra* note 14.

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

[113] GDPR, *supra* note 51, art. 40, 42.

[114] *See* Kaminski, *supra* note 103; McGeveran, *supra* note 14.

[115] CAL. CIV. CODE § 1798.130(a)(1). [Note: check status of amendment on this point]

by European courts that have increasingly recognized the importance of both privacy and data protection as fundamental rights.[116] In recent years, these courts have applied the right to be forgotten to search engines;[117] found the Data Retention Directive to violate fundamental rights;[118] and invalidated the primary mechanism for transferring data to the United States because of fears that American national security surveillance would trample on Europeans' rights.[119]

Crucially, European constitutional structures enforce affirmative rights against private conduct, not just against state actors as in the U.S..[120] 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.[121] 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.[122] Some observers worry that the First Amendment is becoming an increasingly blunt tool, subjecting many regulations concerning privacy and other topics to often-fatal strict scrutiny. Additionally, the Supreme Court has been skeptical of data privacy harms, in cases about both privacy damages and standing to sue.[123] The U.S. Constitution contains no explicit data privacy right, and the Fourth Amendment protects only against state action, and not the actions of private parties.

Thus, 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.

---

116 Schwartz & Peifer, *supra* note 44.

117 Case C–131/12, *Google Spain SL v. AEPD*, 2014 E.C.R. 317.

118 Case C-293/12, Digital Rights Ireland Ltd. V. Minister for Communications, Marine and Natural Resources, 2014 E.C.R. 238.

119 Case C–362/14, *Schrems v. Data Protection Commissioner*, Curia, Court of Justice (Oct. 6, 2015) (hereinafter "*Schrems*").

120 *See* Schwartz & Peifer, *supra* note 44.

121 Alec Stone Sweet & Jud Mathews, *Proportionality Balancing and Global Constitutionalism*, 47 COLUM. J. TRANSNAT'L L. at 68-149 (2008); Bilyana Petkova, *Privacy as Europe's First Amendment*, 25 EUR. L. J. 140 (2019).

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

123 *See* Doe v. Chao, 540 U.S. 614 (2004); FAA v. Cooper, 132 S. Ct. 1441 (2012); Clapper v. Amnesty Int'l, 133 S. Ct. 1138 (2013); Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016); Frank v. Gaos, No. 17-961, 2018 U.S. LEXIS 2658 (Apr. 30, 2018).

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 U.S. 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.[124] Researchers (including one of us) have argued this conventional wisdom oversimplifies matters by focusing on disparities in law-on-the-books and ignoring similarities in practices-on-the-ground.[125] Nonetheless, the EU and U.S. have been unable, or at least 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.[126]

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 United States federal government, to enact new data privacy laws.[127]

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, however, 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 as unitary actors rather than considering the various players within them.[128]

---

[124] *See* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1343 (1999); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161 (2004).

[125] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 260 (2011); McGeveran, *supra* note 14, at 960.

[126] *Schrems*, *supra* note 119, at 93–94; [update with cite to *Schrems II* when decided]

[127] Sara Merken, *States Follow EU, California in Push for Consumer Privacy Laws (1)*, BLOOMBERG LAW (last updated 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.

[128] See, e.g., Harold Hongju Koh, *How is International Human Rights Law Enforced?*, 74 INDIANA 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*, AM. SOC. OF INT'L LAW, PROCEEDINGS OF THE ANNUAL MEETING 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

We then examine a number of recently proposed (and several recently enacted) state and federal data privacy laws, towards the goal of answering the question: which jurisdiction is driving this race to propose and enact new privacy rules? We find that although the commonly accepted narrative has credited new strong European rules as the driver,[129] in practice U.S. states largely copied California. And although the CCPA does not necessarily provide the substantive content for recently proposed federal laws, it has been the impetus behind those congressional bills. California, not Europe, is catalyzing the 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 demonstrates instead how networked individuals can harness processes at the state and local level to promote the adoption of new legal norms.[130] Rather than causing a race to the bottom, the backdrop of data globalization both influences and empowers norm entrepreneurs advocating for stricter requirements.

As to why other states are now copying the CCPA, we posit a number of reasons. First, California may have established itself nationally as an expert jurisdiction on data privacy law, through both the CCPA and earlier law—a sort of variant Delaware effect. Second, since so many companies have a significant presence in California, other states may be presuming a California-driven "Brussels" effect: that is, that 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 nationwide. 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 European law consisting of 99 Articles and 173 Recitals. This is not to say, however, that the GDPR has played no role. We note that Europe may be functioning as a quieter, but still significant, privacy catalyst. But this effect from the EU is more subtle than has been argued, and secondary to a very real California Effect.

Finally, we close 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 its floor. Whether it progresses state-by-state, spurs adoption of model state legislation, or results in a uniform federal law, a new data privacy equilibrium is fast being established in the United States.

---

theory, "which conceive[s] of the international system as composed of unitary, identical state actors with fixed preferences (the billiard ball model")).

[129] See *supra* notes 9-12 and accompanying text.

[130] *See supra* note 128.

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.[131] This matches what we described in Part I as a "California" Effect (de jure). The EU has strictly limited the export of personal data outside of the EU at least since the 1995 Data Protection Directive came into effect, and this policy continued in the GDPR.[132] The 1995 Directive envisioned that such crossborder transfers would be available only in one of three ways (and the same three were retained in the GDPR). 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."[133] The third is the "adequacy mechanism," which would operate 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,"[134] 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.[135]

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 regulate upwards, 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 more of a give-and-take than pure export.[136] But at the end of the day, the laws of other countries did look much more like EU law after these adequacy determinations than they did before.

The GDPR also demonstrates a Brussels Effect, spurring many multinational companies to comply with its provisions worldwide, not only for operations dealing with European persons. 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

---

131 *See generally* Schwartz, *supra* note 7.

132 *See* GDPR, *supra* note 51, art. 45; Directive 95/46/EC, art. 25.

133 GDPR, *supra* note 51, art. 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 crossborder transfers).

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

135 *See* Schwartz, *supra* note 7, at 786–95(comparing UK, Japan, U.S. and noting that Israel, others have receive adequacy determinations).

136 *Id.* at __.

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 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."[137]

Not all companies have conformed their global operations to the GDPR, however. Some enterprises decided to avoid GDPR exposure by excluding Europeans entirely.[138] For example, the *Los Angeles Times* and the *Chicago Tribune* disabled access for internet users in the EU.[139] 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."[140] Chinese smart-home manufacturer Yeelight disabled internet-connected lightbulbs in the European Union.[141] 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.

B. But See United States

While the GDPR's adequacy mechanism and its direct effect on global companies may be enticing other jurisdictions worldwide to enact 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 certainly have shared 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 a strong adequacy ruling from the European Union. Nearly a quarter century of European data

---

[137] 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/.

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

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

[140] *Id.*

[141] *Id.*

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, may be an inhibiting factor. But we believe that another moment of norm entrepreneurship was equally critical. The EU prohibition on crossborder data transfers became effective in 1998 under the Data Protection Directive. Faced with the near certainty that United States law would not be found adequate for unrestricted data flow from the European Union,[142] the Clinton Administration set 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.

The resulting "U.S.-EU Safe Harbor Agreement," signed in 2000 between the Clinton Administration and the European Commission, allowed U.S. companies to certify annually that they adhered to a set of rather vague data protection principles in order to transfer personal data from the EU.[143] 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.[144] In 2015, the Court of Justice of the European Union, citing the revelations of Edward Snowden, struck down the Safe Harbor.[145] 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 mechanism for crossborder data transfers. Instead, the two sides returned to the negotiating table and

---

[142] An adequacy determination would not have been forthcoming from the EU without dramatic legal and regulatory changes in the U.S. *See* Article 29 Working Party, WP 15, Op. 1/99, *Concerning the Level of Data Protection in The United States and the Ongoing Discussions Between the European Commission and the United States Government* 2 (1999) ("[T]he current patchwork of narrowly-focused sectoral laws and voluntary selfregulation 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).

[143] *See* Intl. Trade Admin, *Welcome to the U.S.-EU Safe Harbor Agreement* (Jan, 12, 2017), https://2016.export.gov/safeharbor/eu/eg_main_018365.asp.

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

[145] Schrems v. Commissioner, Case C-362/14 (CJEU 2015).

reached a new compromise, known as the "EU-U.S. Privacy Shield."[146] This arrangement is now being challenged in EU courts as well.[147] But the adequacy provision that spurred countries from Argentina to Thailand to change their law failed to move U.S. privacy law.[148]

The GDPR's rules on crossborder transfer are the same as their forerunners in the Directive. And the Privacy Shield continues to apply to crossborder trnasfers of personal data under the new regime. Thus, the adequacy mechanism seems unlikely to have catalyzed legislative activity in the U.S. the way it has in the rest of the world. We now turn to examine the that extensive state and federal legislative activity in the United StatesOur close comparison of the GPDA and the CCPA in Part I and our examination below of various state and federal privacy bills shows that the CCPA, not the GDPR, 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

Over the last year, the United States has seen an unprecedented volume of legislative proposals regulating data privacy at the state level. This burst of interest has manifested in multiple types of laws: on data security, on internet service provider (ISP) privacy, on specific types of data, and on comprehensive data privacy. Our focus here is on comprehensive data privacy, but we start with a short overview of legislative activity in the broader space, to give a better sense of just how active state legislators have been.

Legislatures in nearly half of the states (twenty-one at our count) considered or enacted data security bills in 2018–2019.[149] Data privacy and

---

[146] *See* Intl. Trade Admin, Privacy Shield Overview, https://www.privacyshield.gov/Program-Overview (last visited June 14, 2019).

[147] Facebook Ireland and Schrems, Case C-311/18 (CJEU 2019).

[148] In a rare exception to this rule, as part of the negotiations leading to the adoption of the Privacy Shield, the United States Congress passed the Judicial Redress Act in 2015, 5 U.S.C. § 552a note, 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.

[149] *See e.g.*, Alabama Data Breach Notification Act, ALA. CODE § 8-38-1 (1975) (passed March 27 2018); Act Amending Title 44, Chapter 11, Arizona Revised Statutes, By Adding Article 2; Relating to Consumer Household Goods, ARIZ. REV. STAT. ANN. §§ 44-1611-1616 (2019) (passed May 2017); California Consumer Privacy Act, 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) (passed May 29 2018); S.B. 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, 3074 (2019) (passed May 20, 2018) (requires organizations to destroy info, expands

data security are not identical policy discussions.[150] Yet the rush to enact data security law shows the growing appetite for these issues, which are often conflated by legislators—evidenced by Colorado's "data privacy" law, which is largely focused not on privacy but on data security. According to the National Conference of State Legislatures (NCSL) in 2019 alone, consumer privacy bills were introduced or filed in at least 25 states and Puerto Rico.[151] 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.[152] And legislators in many states proposed narrower privacy laws, on topics from protection of

---

definition of PII); S.B. 786, 439th Gen. Assemb. (Md. 2019); H.B. 904, 2019 Gen. Assemb., 2019 Reg. Sess. (N.C. 2019); Consumer Protection–Data Security Act, NEB. REV. STAT. ANN. §§ 87-801, 87-806 (West 2019) (signed into law Feb 28 2018); S.B. 176, 54th Leg. Sess., 1st Sess. (N.M. 2019); Act of July 25, 2019, Ch. 117 (S. 5575-B), 2019 N.Y. Sess. Laws (McKinney); Security Breach Notification Act, OKLA. STAT. ANN. tit. 24, §§162-166 (West 2019); Act relating to actions after a breach of security that involves personal information, OR. REV. STAT. ANN. tit. 50, ch. 646A §§ 602, 604, 606, 608, 610, 622 (West 2019); H.B. 1846, 202 Gen. Assemb. (Pa. 2018), H.B. 1181, 203 Gen. Assemb. (Pa. 2019); Insurance Data Security Act, S.C. CODE ANN. §§ 38-99-10 through 38-99-100 (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 22-40-26 (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, 2019 Tex. Sess. Law Serv. Ch. 1326 (West); S.B. 156, 2017-2018 Leg. Sess. (Vt. 2018); 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. § 58.1341.2. (West 2019) (Virginia also introduced a bill in 2018 to amend and reenact § 59.1-200 related to the Virginia Consumer Protection Act. The bill died in committee. H.B. 1588, Reg. Sess. (Va. 2018)); S.B. 5064, H.B. 1071, 66th Leg. Sess., 2019 Reg. Sess. (Wa. 2019).

[150] *See* Derek E. Bambauer, *Privacy versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667, 668-669 (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.").

[151] http://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy/calif.aspx.

[152] Brian Fung, *Trump has signed repeal of the FCC privacy rules. Here's What happens next.*, WASH. PO. (Apr. 4, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/04/04/trump-has-signed-repeal-of-the-fcc-privacy-rules-heres-what-happens-next/. *See* H.B. 230, H.B. 232, 30th Leg. Sess., 1st Sess. (Alaska 2017), H.B. 277, S.B. 160, 30th Leg. Sess., 2nd Sess. (Alaska 2018) (all 4 bills died); H.R. No. 80-18, 29th Leg. Sess., 2018 Reg. Sess. (Haw. 2018) (introduces a task force on ISP privacy); S.B. 243, 2019 Reg. Sess. (Ky. 2019); S.P. 275, 2019 Me. Legis. Serv. Ch. 216 (West); H.B. 1655, 438th Gen. Assemb. (Md. 2018), H.B. 141, 439th Gen Assemb. (Md. 2019); H.B. 382, 191st Gen. Ct. (Mass. 2019); H.B. 1030, 91st Leg. Sess., 1st Reg. Sess. (Minn. 2019), S.B. 433, S.B. 1553, 90th Leg. Sess., 1st Reg. Sess. (Minn. 2018); H.B. 457, 66th Leg. Sess., 2019 Sess. (Mont. 2019) (failed in committee); S.B. 2641, A.B. 3711, A.B. 1927, A.B. 1527, 218th Leg. Sess. (N.J. 2018); S.B. 5245, 242nd Leg. Sess. (N.Y. 2019); H.B. 246, 203rd Gen Assemb. (Pa. 2019).

biometric information or geolocation information to student privacy.[153]

In addition to these individual state proposals, the Uniform Law Commission (ULC) recently voted to begin work on a 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.[154] The ULC 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. One of the authors of this Article, William McGeveran, will serve as the reporter for the committee drafting this legislation. 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 17 states, in addition to California and Puerto Rico, that considered or enacted comprehensive data privacy laws in 2018 and 2019.[155] Five states established task forces with the goal of proposing data privacy legislation.[156] Including task forces, there are at least 19 states (and Puerto Rico) considering or enacting comprehensive data privacy legislation.[157]

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 regulatory contagion around data privacy in the United States 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

---

[153] *See, e.g.*, H.F. 2534, Iowa Online Services and Mobile Apps for Students (2018); Illinois H.B. 2785, Geolocation Privacy Protection Act (2019); New Hampshire H.B. 536 (2019) (biometric information); Oregon H.B. 2866 (2019) (geolocation info); Tennessee H.B. 0352 (2019) (making unauthorized use or distribution of personal health information a violation of consumer protection law); Vermont S.B. 110 (2019) (student privacy law); Virginia H.B. 2535 (requiring sites to let minors request to remove information).

[154] Katie Robinson, Uniform Law Comm'n, Press Release, *New Drafting and Study Committees to Be Appointed* (Jul. 24, 2019), available at https://www.uniformlaws.org/newsandpublications/news.

[155] *See* Hawaii SB 418 (2019); Illinois HB 3358 (2019); Louisiana HB 465 (2019); Maine LD 946 (2019); Maryland HB 901 (2019); Massachusetts S.120 (2019); Minnesota HF 2917 (2019); Missouri HB 1253 (2019); Nevada SB 220 (2019, codified at Chap. 211); New Jersey A4640 (2019); New Jersey A4902 (2019); New Mexico SB 176 (2019); New York A7736 (2019); New York S5642 (2019); Pennsylvania HB 1049 (2019); Rhode Island HB 5930 (2019); Texas HB 4518 (2019); Vermont H. 764 (2018); Washington SB 5376 (2019).

[156] Connecticut SB 1108; Hawaii HCR 225; Louisiana HR 249; North Dakota HB 1485; Texas (council) HB 4390 (establishing the Texas Privacy Protection Advisory Council).

[157] 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.

identical.[158] Like the CCPA, the proposed Connecticut bill granted individuals access rights,[159] a right to deletion,[160] and a right to opt out of the sale of one's data.[161] Like the CCPA, the proposed Connecticut bill prohibited business from discriminating against consumers for exercising their rights.[162] 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.[163] Ultimately, however, legislators replaced the bill with a substitute act establishing a task force concerning consumer privacy, signed into law on July 9, 2019.[164] The Act instructs the task force to "examine what information businesses in this state should be required to disclose to 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."[165]

Massachusetts' proposed data privacy bill, SD 341, also introduced in January 2019, provides another clear example of this mimicry.[166] In multiple places, SD 341 contains language identical to the California law. 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. SD 341's exception for publicly available information, too, almost perfectly adopts CCPA language.[167] While SD 341 does not contain the CCPA's exhaustive list of examples of personal information, its core definition of personal information differs by just one word.[168] The proposed Massachusetts bill would put in place notice, access,

---

158 Compare CCPA 1798.140(c) (defining "business") & 1798.140(o) (defining "personal information" with SB 1108 §1(3) (defining "business") & §1(15) (defining "personal information").

159 SB 1108 §§2, 4, 6.

160 SB 1108 §3

161 SB 1108 §7.

162 SB 1108 §8.

163 SB 1108 §9(1), §10(1).

164 See generally https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&which_year=2019&bill_num=Sb+1108.

165 SB 1108 §1(a).

166 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.

167 *Compare* California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798.198(K)(2) (2018), *with* SD 341, Mass. Acts § 6 (2019).

168 SD 341, Mass. Acts § 6 (2019) (""information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a

and deletion requirements that largely correspond to CCPA requirements.[169] Like the CCPA, the rights are not waivable.[170]

In some places, the proposed Massachusetts bill is stronger than the CCPA. It gives consumers the right to opt out not just of sale of personal information, but of third party disclosure.[171] And unlike the CCPA, it provides for a private right of action, with statutory damages of $750 per consumer per incident, plus attorney fees.[172] Mirroring the CCPA, it directs the state attorney general to write regulations and empowers that office to enforce the new privacy rules.[173]

Also in January 2019, North Dakota introduced data privacy legislation[174] that was similar to the CCPA in a number of ways. Despite its origin story–one of the drafters watched a news report on European privacy law[175]–the North Dakota bill's roots, did not lie in the GDPR either. The North Dakota bill defined a covered business nearly word-for-word identically to the CCPA's definition.[176] The definition of "personal information," too, closely tracked that in the CCPA.[177] It created a right of access similar to the CCPA's. Unlike the CCPA, however, the North Dakota bill would have prohibited disclosure of personal information without express written consent. It also differed from

---

particular consumer or the consumer's device" in MA; "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 household" in CA.").

[169] *Id.* at § 2(10) (Notice At or Before Collection: requiring disclosure of categories of personal info, business purpose, consumer rights, and more); *id.* at § 3(11) (Verifiable Consumer Requests: right to request specific pieces of personal info, names of third parties to whom disclosed, sources, business purpose); *id.* at § 5(14) (Right to Delete: covering right to delete info collected from the consumer); *id.* at § 6(15) (Right to Opt Out of Third-party disclosure instead of sale!).

[170] *Compare* CAL. CIV. CODE § 1798.192, *with* SD 341, Mass. Acts § 14(23) (2019).

[171] SD 341, Mass. Acts § 6(15) (2019).

[172] *Id.* at § 9(19).

[173] *Id.* at § 10, § 11.

[174] H.B. 1485, 66th Leg. Assemb. (N.D. 2019).

[175] Sara Merken, *States Follow EU, California in Push for Consumer Privacy Laws (1)*, BLOOMBERG LAW (last updated 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 ("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.").

[176] *Compare* H.B. 1485, 66th Leg. Assemb. (N.D. 2019), *with* California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798.198 (2018).

[177] *Compare* H.B. 1485, 66th Leg. Assemb. (N.D. 2019) ("'Personal information' means information that identifies, describes, or could reasonably 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 ("CCPA"), CAL. CIV. CODE § 1798.198(o)(1) (2018) ("'Personal information' means 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 household…").

the CCPA because it lacked a notice requirement, or a right to deletion. Also unlike the CCPA, the North Dakota bill would have created a private right of action.[178] In February 2019, the bill was replaced by a proposal for a legislative study of data privacy laws.[179]

The above three states are just a sampling of this dynamic. We find at least eight other states with proposals that could similarly be characterized to various degrees as CCPA mimics.[180] Mississippi, Pennsylvania, and Rhode Island, like Connecticut and Massachusetts, copied portions of the CCPA wholesale in their proposed data privacy bills.[181] One proposed Texas bill, too, largely tracked the CCPA.[182] Texas ultimately enacted another bill into law, the Texas Privacy Protection Act; while initially a broad data protection law, it was ultimately amended to create a council to report back on proposed statutory changes by September 2020.[183] Illinois, too, appears to have imitated the text of the CCPA in its proposed Data Transparency and Privacy Act, which 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 carved out the use of data for advertising and other exemptions.[184] Maryland's bill and Hawaii's original bill (later replaced with a task force) offer a similar set of rights to the CCPA, though they differ in some significant aspects.[185]

Nevada is one of the only states to not just propose but actually enact new data privacy law in this period. Nevada amended its existing privacy law in May 2019, and it will go into effect in October 2019.[186] Existing Nevada law already required websites and online services which collect certain personal information to provide notice to consumers.[187] 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

---

[178] H.B. 1485, 66th Leg. Assemb. § 51-37-05 (N.D. 2019) ("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…").

[179] H.B. 1485, 66th Leg. Assemb. (N.D. 2019).

[180] See also https://www.dwt.com/blogs/privacy--security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou

[181] Mississippi HB 2153; Pennsylvania H.B. 1049 (April 2019); Rhode Island H.B. 5930 (March 2019).

[182] Texas H.B. 4518. By contrast, Texas H.B. 4390 takes more of a blended CCPA-GDPR approach. https://capitol.texas.gov/tlodocs/86R/billtext/html/HB04390I.htm

[183] https://www.jdsupra.com/legalnews/state-and-federal-privacy-legislation-63216/

[184] Illinois HB 3358 http://www.ilga.gov/legislation/fulltext.asp?DocName=&SessionId=108&GA=101&DocTypeId=HB&DocNum=3358&GAID=15&LegID=119864&SpecSess=&Session=

[185] Hawaii S.B. 418, Maryland S.B. 0613. See also https://www.dwt.com/blogs/privacy--security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou

[186] https://www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6365/Overview.

[187] NRS 603A.340.

receipt of a "verified request" from the consumer to opt out.[188] The scope of the Nevada law is far narrower 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). It also defines "Sale" less broadly than does the CCPA. But its focus on an opt-out for restricting sale of personal data is distinctly Californian, and not European.

In summary: a considerable number of states are mimicking the precise technical language of the CCPA language, while others are adopting its core framework of individual rights. No state has proposed adopting European-style comprehensive data protection law. The only two proposed state laws we found that focused not just on individual rights but also on more GDPR-like compliance obligations are Washington's recently failed Privacy Act[189] and one of the two bills proposed in Texas.[190] Both ultimately were not enacted, at least not in that form. We discuss the Washington example at further length below. Finally, one of New York's latest proposals reflects a third competing concept of data privacy, which we introduce and discuss in the next section.[191] But our close analysis clearly shows that California, not Europe, is catalyzing comprehensive data privacy legislation in states around the country.

2. Federal Laws

If the state bills are typically modeled on the CCPA, 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.[192] Additionally, a bipartisan group of six Senators has been working on draft legislation that has been widely understood to be the most serious of the proposals, although talks may recently have slowed down.[193] We here compare several of these proposed

---

[188] S.B. 220 (Nev., codified at NRS 603A).

[189] Washington Privacy Act, H.B. 5376, Reg. Sess. (Wash. 2019); s*ee also* H.B. 5919, Reg. Sess. (proposed Wash. 2019).

[190] https://capitol.texas.gov/tlodocs/86R/billtext/html/HB04390I.htm

[191] New York SB 5642, https://www.nysenate.gov/legislation/bills/2019/s5642; Issie Lapowsky, *New York's Privacy Bill Is Even Bolder than California's*, WIRED (June 4, 2019), https://www.wired.com/story/new-york-privacy-act-bolder/.

[192] *See supra* note 4 (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/; 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/.

[193] Gopal Ratnam, *Progress on Federal Data Privacy Bill Slows in Both Chambers*, ROLL CALL (June 25, 2019), https://www.rollcall.com/news/policy/progress-on-federal-data-privacy-bill-slows-in-both-chambers; Harper Neidig, *Senators Ramp Up Privacy Bill Work*, THE HILL (May 1, 2019), https://thehill.com/policy/technology/441667-senators-ramp-up-privacy-bill-

federal laws to show how they differ from both the GDPR and the CCPA—and note how, in fact, a third model has 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, Senator Marco Rubio's American Data Dissemination Act, and Senator Brian Schatz's Data Care Act. We conclude that the substantive provisions of several of the bills draw from older privacy law or from academic proposals, not the GDPR or the CCPA. Only Senator Wyden's bill shows direct signs of influence from both the CCPA and GDPR.

The proposed Consumer Data Privacy Act ("CDPA"), 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 "reasonably linkable" to an individual.[194] Like the CCPA, the CDPA does not cover businesses below a certain size, as long as they meet other restrictions.[195] The CDPA, however, would incorporate a number of aspects of the GDPR: it would require reporting in some circumstances; create access rights,[196] including with respect to companies that lack a direct relationship with consumers;[197] create a right of correction; and require impact assessments for automated decision-making. 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. The CDPA directs the FTC to promulgate regulations, and houses enforcement with the FTC, to

---

work; *Talks of Federal US Privacy Law Slowing Down on Capitol Hill*, IAPP (June 11, 2019), https://iapp.org/news/a/talks-of-federal-u-s-privacy-law-slowing-down-on-capitol-hill/.

[194] Consumer Data Privacy Act ("CDPA"), SIL18b29, 115th Cong. (2019) ("[A]ny information, regardless of how the information is collected, inferred, or obtained that is reasonably linkable to a specific consumer or consumer device" versus CCPA: "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 household.").

[195] *Compare* SIL18b29, 115th Cong. § 5 (2019) (CDPA excludes companies with less than fifty million dollars in average annual gross receipts; it also requires 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) (CCPA excludes companies with less than twenty-five million dollars in annual gross revenues).

[196] CAL. CIV. CODE § 1798.130 (2018) (Businesses required to "identify the consumer, associate the information provided by the consumer in the verifiable request to any personal information previously collected by the business about the consumer" and provides for correction or challenge rights for inaccurate information).

[197] CAL. CIV. CODE § 1798.110 (2018) ("A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer…[t]he categories of third parties with whom the business shares personal information."); Art. 14 GDPR – Information to be provided where personal data have not been obtained from the data subject at 31 (2016), https://gdpr-info.eu/art-33-gdpr/.

which it allocates considerable additional resources. It does not preempt state regulation.

The proposed Data Care Act ("DCA"), introduced in December 2018 by Senator Schatz with fourteen cosponsors, differs fundamentally from both the CCPA and GDPR. The DCA focuses on duties owed by companies with a direct relationship to consumers, not on data brokers or other third parties. The DCA would impose duties of care, loyalty, and confidentiality on online service providers. Thus, the DCA advances a consumer protection rather than data protection model of privacy, and does not impose any of the particular transparency requirements that are central to both the California and EU regimes.

In this way, the DCA embodies an emerging strain of thought about privacy among US scholars who advocate redefining privacy as a matter of "trust" or "fiduciary-like duty" on the part of large-scale data collectors.[198] The "information fiduciary" model of data privacy has not been limited to Senator Schatz's federal proposal; the recent New York Privacy Act, too, was modeled on the concept.[199] 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.

Schatz's bill puts enforcement in the hands of the FTC, already responsible for enforcing aspects of U.S. data privacy under its consumer protection authority. The DCA would not preempt state privacy laws, although state AGs would be prevented from bringing enforcement actions during an FTC enforcement action.[200]

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.[201] Unlike the Privacy Act, which applies only to the federal government, these rules would apply to private sector actors that collect certain types of personal information.

---

198 *See* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U. CAL. DAVIS L. REV. 1183 (2016); Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE L. REV. 1057 (2019); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap*, 126 YALE L. J. 1180 (2017); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016); Tim Wu, Opinion, *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.

199 Emily Bruemmer, *State and Federal Privacy Legislation Stalls*, JD SUPRA (June 28, 2019), https://www.jdsupra.com/legalnews/state-and-federal-privacy-legislation-63216/; New York SB 5642, https://www.nysenate.gov/legislation/bills/2019/s5642; Lapowsky, *supra* note 191.

200 Data Care Act of 2018, S. 3744, 115th Cong. §5 (2018).

201 American Data Dissemination Act of 2019, S. 142, 115th Cong. (2019)

The ADD resembles the GDPR and CCPA only to the extent that those two regimes, like the Privacy Act, build on Fair Information Practice Principles (FIPPs). It directs the FTC to adopt regulations that restrict disclosures of records; create an access right; 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 (FCRA). 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.

While the three 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 also hope to limit the 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. To extend the metaphor of regulatory contagion: federal proposals can be characterized as an immunity response mobilizing in Congress, attempting to inoculate national companies against the CCPA and its imitators.

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. California, not Europe, has been catalyzing the rapid proposal of privacy laws both across states and at the federal level. What has been happening is more complex, and more interesting, than the conventional narrative of a long-armed, unilateral Brussels.

In this section, we offer an 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 tightly networked norm entrepreneurs, acting against backdrop forces of 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 far 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 state and non-state actors 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 functionally hijacked 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.[202]

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. state and the federal government, had no comprehensive data privacy law. Real estate developer Alastair Mactaggart wanted to enact such law in California. 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. Mactaggart befriended Mary Stone Ross, who had worked for the CIA and the House Intelligence Committee. They collaborated on drafting the ballot initiative through a group they named the Californians for Consumer Privacy, the political committee that then pushed the bill (although later Ross and Mactaggart had a falling out).[203] 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. Mactaggart then hired Soltani to help revise the proposed ballot initiative, the bones of which became the CCPA.[204] 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."[205]

By using the California ballot initiative process, Mactaggart and his allies forced the state legislature's hand.[206] The California legislature, fearing the practical difficulties of a ballot initiative that would become nearly

---

[202] *See generally* Harold Hongju Koh, *How Is International Human Rights Law Enforced?*, 74 IND. L. J. 1397 (1999); Harold Hongju Koh, *Transnational Legal Process*, 75 NEB. L. REV. 181 (1996).

[203] 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.

[204] 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.

[205] Casey Newton, *How a Wiley Californian Beat Google and Facebook's Influence Operation*, THE VERGE (Aug. 15, 2018), https://www.theverge.com/2018/8/15/17691004/california-data-privacy-law-alastair-mactaggart-regulation.

[206] Confessore, *supra* note 204. The initiative gathered some 629,000 signatures. *Id.*

unchangeable law with immediate effect,[207] scrambled to draft a bill that would persuade the initiative's sponsors to withdraw it.[208] State Assemblymember Ed Chau and State Senator Robert Hertzberg, both from districts neighboring Los Angeles, introduced the bill. The enactment of the CCPA does not represent the action of a legislature that independently recognized a social problem it could help address, but the legislature's reaction to leverage exerted by highly motivated, connected—and, at least in Mactaggart's case, wealthy—individuals.[209]

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 manipulate voters in the 2016 election. Indeed, that scandal was cited by the legislature itself as a motivating factor for the CCPA in its preamble.[210] Second, data 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, which almost all have a 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. This may have made the CCPA more palatable, or at least caused U.S. citizens to wonder why Europeans should get privacy protections that they do not.

What happened next—the spread of the CCPA—was intended and predicted by its originators, who hypothesized that, like California emissions

---

[207] 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 et al., *California's GDPR? Sweeping California Privacy Ballot Initiative Could Bring Sea Change to U.S. Privacy Regulation and Enforcement*, DATA MATTERS SIDLEY (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/; Courtney M. Bowman & Kristen J. Mathews, *The California Consumer Privacy Act of 2018*, PROSKAUER PRIVACY BLOG (July 13, 2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/.

[208] Confessore, *supra* note 204; CCPA Sec. 2(g) ("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.").

[209] To some extent, aspects of the GDPR reflect this dynamic, too. *See Schrems v. Data Protection Commissioner*, Case C–362/14, Curia, Court of Justice (Oct. 6, 2015).

[210] Newton, *supra* note 205 ("Mactaggart benefited from increased skepticism about tech companies broadly, but he also got an unexpected gift this spring: the Cambridge Analytica data privacy scandal").

standards, a baseline data privacy law would spread.[211] 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.[212] It was the first U.S. law to require companies to post a privacy policy.[213] In the intervening years, privacy policies have become ubiquitous across the internet.

Also in 2003, California enacted legal rules requiring companies that have suffered a qualifying data security breach to notify users whose information may have been compromised.[214] 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. At first, some companies limited their compliance with the data breach notification law within the borders of California. One particular security breach demonstrates this in operation. ChoicePoint suffered a data breach in 2004 affecting nearly 145,000 people.[215] Initially, it reported that breach to Californians only, as the law required.[216] However, some soon began inquiring whether the Atlanta-based national operator suffered a breach that targeted only Californians. Faced with this pressure, ChoicePoint voluntarily issued a nationwide notice to all Americans whose information had been breached.[217] ChoicePoint's notification also resulted in a federal enforcement action by the Federal Trade

---

[211] *Id.* (Mactaggart comparing privacy legislation to auto-emission legislation).

[212] CAL. BUS. & PROF. CODE §§ 22575 et seq.

[213] *California Online Privacy Protection Act (CalOPPA)*, CONSUMER FEDERATION OF CALIFORNIA EDUCATION FOUNDATION (July 29, 2015), https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/.

[214] CAL. CIV. CODE § 1798.82 (2003) (disclosure requirements for person or business who owns or licenses computerized data including personal information when there is a security breach of the system).

[215] 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.

[216] *See id.*

[217] 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?*, BUSINESS LAW TODAY (Aug. 18, 2011), http://apps.americanbar.org/buslaw/blt/content/2011/08/article-raether.shtml ("ChoicePoint decided initially to notify only California consumers. The backlash was swift and immediate. ChoicePoint quickly modified its decision and notified all affected consumers regardless of their state of residency.").

Commission. ChoicePoint, a provider of credit reporting services, had violated the Fair Credit Reporting Act ("FCRA") by allowing access to some 163,000 consumer reports to persons who were not duly authorized to receive access.[218] By 2005, the California breach notification law had unleashed a "wave" of additional reported security breaches in the state.[219] Notifications in California alerted consumers nationally of breaches that may affect them, and dozens of other states rapidly began adopting their own notification laws in a textbook de jure California Effect. [220] Today, all fifty states have enacted data security breach notification laws.[221] The laws that followed California's not only copied, but also both expanded[222] and contracted[223] California's model. And in 2018, the GDPR introduced security breach notification into European law.[224]

States thus have a history of following California law in this policy space. 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

---

[218] Natalie Kim, *Three's A Crowd: Towards Contextual Integrity in Third-Party Data Sharing*, 28 HARV. J.L. & TECH. 325, 330 (2014). Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 923 (2007). The FTC Choicepoint settlement also authorized the FTC to monitor compliance by "[p]osing as consumers and suppliers" of Choicepoint. *See* United States v. Choicepoint Inc., No. 1:06-cv-00198-JTC, at 19 (Ga. Ct. App. 2008) (FTC.gov).

[219] 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 (2006).

[220] "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." *See* Samuelson Law, Technology & Public Policy Clinic, *Security Breach Notification Laws: Views from Chief Security Officers*, UNIV. of CALIFORNIA-BERKELEY SCH. OF LAW, at 3 (2007) https://www.law.berkeley.edu/files/cso_study.pdf.

[221] *Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[222] Samuelson Law, Technology & Public Policy Clinic, *Security Breach Notification Laws: Views from Chief Security Officers*, UNIV. of CALIFORNIA-BERKELEY SCH. OF LAW, at 43 (2007) https://www.law.berkeley.edu/files/cso_study.pdf ("many states have expanded the definition to include various others forms of personal information").

[223] *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 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.").

[224] Art. 33 GDPR – Notification of a personal data breach to the supervisory authority (2016), https://gdpr-info.eu/art-33-gdpr/.

represents an appealingly pre-packaged compromise, as the state that houses both Silicon Valley industry and a generally liberal electorate.

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. Lawmakers in other states should anticipate that companies are less likely to oppose a bill if it tracks the contours of a California law they must obey already. Even though the CCPA protects only California residents, companies may find it hard to partition that data, or may calculate the cost is low enough to extend their compliance infrastructure to consumers in other states.

Third, compared to the GDPR, the CCPA is a better legal meme for U.S. legislators.[225] 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. The CCPA's relative brevity and simplicity,[226] 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 operating in U.S. jurisdictions. This may lower the resistance of global companies to both state and U.S. data privacy law. Of course, many of the companies most affected by the GDPR were already shouldering regulatory costs under the prior Data Protection Directive. Perhaps the number of companies affected by European law has gone up, because of its more explicit extraterritorial reach. Or perhaps more companies are now taking EU law seriously, given the greatly increased penalties they risk.

A clear example of this dynamic is the proposed Washington Privacy Act that failed in 2019.[227] This bill had more similarities with the GDPR than other state legislation.[228] It used GDPR terminology such as "controller" and "processor."[229] 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.[230]

---

[225] We thank Christina Mulligan for this insightful characterization.

[226] *See supra* note 43 and accompanying text.

[227] S.B. 5376, Reg. Sess. (Wash. 2019).

[228] *See* Washington Privacy Act, H.B. 5376, Reg. Sess. (Wash. 2019); s*ee also* H.B. 5919, Reg. Sess. (proposed Wash. 2019).

[229] Art. 33 GDPR – Notification of a personal data breach to the supervisory authority Sec. 3(4), (12), (2016), https://gdpr-info.eu/art-33-gdpr/.

[230] S.B. 5376, Reg. Sess. (Wash. 2019) (Notice Section 7 "Transparency" categories of personal data, purposes, rights, categories shared with third party, disclose such profiling

Unlike other proposed state laws, the Washington bill included privacy risk assessments, another idea borrowed from the GDPR.[231] It even drew on the GDPR's limitations on automated decision-making.[232]

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.[233] Microsoft declares that it complies with the GDPR worldwide.[234] With over 45,000 employees in the Seattle area, Microsoft is a significant voice in the state.[235] And 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."[236] 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."[237] The Brussels Effect on Microsoft may be driving it to push for state privacy legislation that more closely maps on to the GDPR and thus

---

disclose sale to data brokers).

[231] *Compare* Washington Privacy Act, H.B. 5376, Reg. Sess., Sec. 8 (Wash. 2019), *with* Art. 35 GDPR – Data protection impact assessment, Sec. 7, (2016), https://gdpr-info.eu/art-33-gdpr/ (Risk assessments are confidential and exempt from public inspection and copying; however, must make accessible to AG upon request).

[232] Washington Privacy Act, H.B. 5376, Reg. Sess., Sec. 6(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 suing 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…").

[233] *Microsoft Corporation (MSFT) Stock Price, Quote*, YAHOO FINANCE, (Feb. 18, 2019), https://finance.yahoo.com/quote/MSFT/ (Microsoft's market capitalization as of February 18, 2019 is $830 billion, while Amazon's is $790 billion).

[234] "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." 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/.

[235] Tom Warren, *Microsoft unveils plans for a new modern headquarters*, THE VERGE (Nov. 29, 2017), https://www.theverge.com/2017/11/29/16714290/microsoft-new-headquarters-redmond-seattle.

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

[237] Monica Nickelsberg, *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/.

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. The state's other digital tech giant, Amazon, soon joined in support of the bill.

After sailing through the state senate by a vote of 46-1, the Washington bill foundered amid controversy. After portions of the original legislation were stripped out, the state ACLU opposed the bill as too weak.[238] 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.[239] The bill's sponsor reintroduced it in 2020 with a broader coalition of companies and organizations in support. Microsoft's chief privacy officer, former FTC commissioner Julie Brill, 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."[240]

This story of the Washington Privacy Act displays, the GDPR's Brussels Effect in action. But again, it also underscores the power of norm entrepreneurs. A global company such as Microsoft has good reason to want to impose costs on its competitors while coming off as a good actor. Brill, too, may be playing a role as a former FTC commissioner bringing in compliance norms from a U.S. government agency.

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[241]—to wonder why EU persons get stronger privacy rights than they do, and to question the longstanding narrative that imposing digital privacy regulation will break the internet or otherwise kill innovation.

Some may doubt the sincerity of California as a privacy regulator. Data protection rules, critics will observe, encumber some of its leading corporations. These corporations will hobble any real regulatory enforcement by the state, the critics will argue. But California's economy is far bigger than Silicon Valley alone. Of course, diffuse voices fare poorly against actors with

---

238 *See* 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.

239 *Id.*.

240 Julie Brill, *Our Support For Meaningful Privacy Protection Through the Washington Privacy Act*, OFFICIAL MICROSOFT BLOG (Apr. 29, 2019), https://blogs.microsoft.com/on-the-issues/2019/04/29/our-support-for-meaningful-privacy-protection-through-the-washington-privacy-act/.

241 *See supra* note 175.

concentrated interests, as Mancur Olson observed.[242] 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, the same group now seeks to further strengthen California's law, again using the initiative as a leverage tool.[243] Vogel argues that the California Effect requires that "nonstate actors in rich and powerful political jurisdictions prefer stronger regulatory standards."[244] Content-based industries based in Los Angeles have long complained about how Silicon Valley enterprises are insufficiently attentive to intellectual property piracy. The CCPA's principal authors both represent districts bordering Los Angeles. Many Silicon Valley enterprises themselves support data privacy regulations, though some suggest that the support is a strategic effort to undermine California's privacy law with a weaker, preemptive federal law.[245] There is a reason for responsible Silicon Valley enterprises to embrace privacy law. Silicon Valley enterprises depend on user confidence that revealing more and more of themselves to our electronic assistants will not create privacy risks. Companies that violate that trust undermine trust for other companies as well.[246] Ultimately, whether either Californians or those outside the state trust the state's privacy regulators will depend on their performance.[247]

We close this section with a note on the limits of our knowledge. 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. The Uniform Law Commission's new project to draft model state legislation represents one of the most formal such networks: its commissioners from every state consciously seek to replicate successful innovations across state boundaries in a uniform way. Senator Wyden, for example, has been a privacy advocate for years, and may be taking advantage of current dynamics to push for changes to

---

242 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 interest").

243 Natasha Singer, *Group Behind California Privacy Law Aims to Strengthen It*, N.Y. Times, Sept. 24, 2019.

244 VOGEL, TRADING UP, *supra* note 30 at 268.

245 Russell Brandom, *Tim Cook Wants a Federal Privacy Law — But So Do Facebook and Google*, THE VERGE (Oct. 24, 2018), https://www.theverge.com/2018/10/24/18018686/tim-cook-apple-privacy-law-facebook-google-gdpr.

246 *See* Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559 (2015); *see also* Balkin, *supra* note 198; Richards & Hartzog, *supra* note 198.

247 *Cf.* Ann E. Carlson, *Regulatory Capacity and State Environmental Leadership: California's Climate Policy*, 24 FORDHAM ENVIRONMENTAL L. REV. 63 (2013) (describing success of California's environmental policy agency).

federal law. Civil society groups such as the Center for Democracy and Technology (CDT) have proposed discussion legislation in hopes of influencing the federal debate.[248] 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.[249] 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 [that] work together to harmonize or otherwise adjust different kinds of domestic law."[250] What we are seeing here, however, 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. We turn now, however, to several very real potential constraints 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 potential federal preemption of state law could limit the reach of state law and the catalytic effect of the CCPA.[251] 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. Finally, we note the possibility that new models, notably including "trust" or "fiduciary" concepts, will take root and out-race both the

---

[248] *CDT's Privacy Legislation*, CENTER FOR DEMOCRACY & TECHNOLOGY (last visited Feb. 5, 2020), https://cdt.org/campaign/federal-privacy-legislation/.

[249] Kerry, *supra* note 192.

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

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

GDPR and the CCPA to become the dominant catalyst for new privacy law.

1. The Dormant Commerce Clause

Because internet regulation inevitably extends spills over jurisdictional lines, the dormant commerce clause plays an important role in disciplining any 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."[252] The dormant commerce clause imposes two separate conditions on regulatory spillovers: (1) the regulation at issue must not discriminate against interstate commerce[253] and (2) it must not impose excessive burdens on interstate commerce.[254] 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."[255]

Early cases challenging state internet regulation on commerce clause grounds met with some success. Among the first was a 1997 decision in *American Library Association v. Pataki*, overturning a New York statute that prohibited the transmission of obscene content to minors..[256] Into the early 21st century, a number of courts followed the lead of Pataki when evaluating similar statutes..[257] However, courts in other contexts have departed from

---

[252] Comptroller of Treasury of Maryland v. Wynne, 135 U.S. 1787, 1794 (2015).

[253] Dep't of Revenue of Ky. 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.").

[254] Dep't of Revenue of Ky. v. Davis, 553 U.S. 328, 338 (2008) (internal citations and quotation marks omitted) ("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 alternative.").

[255] 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." *See, e.g.*, Maine v. Taylor, 477 U.S. 131, 153 (1986).

[256] Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 169 (S.D.N.Y. 1997) ("…the 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, 811 (2001).

[257] Am. Civil Liberties Union v. Johnson, 194 F.3d 1149, 1161 (10th Cir. 1999); PSINet, Inc. v. Chapman, 362 F.3d 227 (4th Cir. 2004); American Booksellers Found. v. Dean, 342 F.3d 96 (2d Cir. 2003); Southeast Booksellers Ass'n. v. McMaster, 282 F. Supp. 2d 389 (D.S.C. 2003); Cyberspace Communications, Inc. v. Engler, 142 F. Supp. 2d 827 (E.D. Mich. 2001).

Pataki's approach, upholding, for example, state anti-spam statutes against commerce clause challenges.[258] A California appeals court "reject[ed] *Pataki's* holding that any State regulation of Internet use violates the dormant Commerce Clause."[259]

A federal district court case from California seems particularly relevant because it considered a dorman 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 emails in the ordinary course of business."[260] Omni argued that practically speaking, it would have to notify all callers to its customer service about the recording, not just Californians, and that this thus constituted a per se violation of the Commerce Clause.[261] 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. It concluded, "[o]verall, 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."[262] 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 avoids that result.

The CCPA does not appear to facially discriminate against interstate commerce.[263] 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

---

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

[259] Ferguson v. Friendfinders, Inc., 94 Cal. App. 4th 1255, 1264, 115 Cal. Rptr. 2d 258, 265 (2002), *as modified* (Jan. 14, 2002).

[260] *Id.* (internal citation omitted).

[261] Ades v. Omni Hotels Mgmt. Corp., 46 F. Supp. 3d 999, 1012 (C.D. Cal. 2014) ("Omni asserts that because the portability of mobile phone numbers makes it unfeasible to distinguish between Californian and non-Californian calls, compliance with § 632.7 would force Omni to warn all callers, even those from single-consent states, that they could be recorded.").

[262] *Id.*

[263] 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, Inc. v. Oneida-Herkimer Solid Waste Mgmt. Auth., 550 U.S. 330, 338–39 (2007) (internal citations omitted).

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). If nothing else, the resulting uncertainty may deter other states from following the CCPA's lead, at least until any Commerce Clause challenge is resolved.

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. While state laws may be preempted when compliance with both state and federal mandates is impossible,[264] the current lack of comprehensive federal privacy law makes this unlikely in the case of the CCPA. In many domains, however, Congress has adopted federal statutes that explicitly preempt state law in the same area, thus establishing uniform national standards on a topic.[265] A new federal statute with an express preemption clause could 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.[266]

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—

---

[264] *See* Fla. Lime & Avocado Growers, Inc. v. Paul, 373 U.S. 132 (1963).

[265] *See, e.g.*, 17 U.S.C. § 301 (federal preemption provision of Copyright Act); 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).

[266] Writing of this dynamic in other contexts, Rick Hills 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, 50 (2007).

upwards—across the United States.[267] In fact, preemption may be the issue that kills proposed federal data privacy law as powerful Californians and Democrats line up against 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.[268], Meanwhile, industry will be less interested in any federal law if it would not supersede the CCPA.

There are virtues of a single national standard.[269] A national privacy law would establish a standard across the region—rather than promising higher or lower protections depending on where a person is, or where her data is processed or held.[270] It makes cross-border data flows across the United States a process that does not require legal review. It avoids the possibility of inconsistent mandates—inconsistent notice requirements for example. The same service or product could be introduced nationwide, as long as it complies with the national standard. There seems to be little reason to expect that data standards should vary across the country; it would be difficult to explain stricter limits on data collection and use in California than Colorado, or vice versa. Compliance costs 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.[271] States have a long history of regulating privacy, much of it developed through the common law.[272] As Peter Swire has documented, existing federal privacy legislation generally serves as a regulatory floor, not a ceiling, including post-

---

[267] 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).

[268] Darius Tahir, *Pelosi Puts Privacy Marker Down*, POLITICO (Apr. 15, 2019), https://www.politico.com/newsletters/morning-ehealth/2019/04/15/pelosi-puts-privacy-marker-down-424986 ("We 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.").

[269] *See* Paul M. Schwartz, *Preemption and Privacy*, *supra* note 44; Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868 (2009).

[270] Bellia, *supra* note 269.

[271] Citron, *supra* note 50 (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*, https://iapp.org/news/a/us-federal-privacy-preemption-part-2-examining-preemption-proposals/.

[272] William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 391–92 (1960).

1996 sector-specific preemption provisions adopted since the mid-1990s.[273] Buzbee observes that "in most areas focused on regulation of risks, such as discrimination and efforts to enhance public welfare through regulation of environmental and occupational risks, the protective 'one way ratchet' of floor preemption has been the legislative and regulatory norm."[274] Most importantly, a federal preemption ceiling risks losing the regulatory innovation that continued state legislation in the area might supply.[275]

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 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."[276] 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.[277] 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.[278] For

---

[273] Peter Swire, *US Federal Privacy Preemption Part 1: History of Federal Preemption of Stricter State Laws*, IAPP PRIVACY TRACKER (Jan. 9, 2019), https://iapp.org/news/a/us-federal-privacy-preemption-part-1-history-of-federal-preemption-of-stricter-state-laws/. Both HIPAA and GINA serve as floors for state regulation, not ceilings. Health Insurance Portability and Accountability Act, 45 C.F.R. § 160.203 (2002); Genetic Information Nondiscrimination Act, § 2(5). While the FCRA preempts some causes of action, it permits states to regulate identity theft. *See* Fair Credit Reporting Act, 15 U.S.C. § 1681t(a).

[274] William Buzbee, *Asymmetrical Regulation: Risk, Preemption, and the Floor/Ceiling Distinction,* 82 N.Y.U. L. REV. 1547 (2007).

[275] Paul M. Schwartz, *Preemption and Privacy*, *supra* note 44 (describing states as "laboratories for innovations in information privacy law").

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

[277] Schwartz, *supra* note 275, at 935.

[278] *See* H.B. 5919, Reg. Sess. (proposed Wash. 2019). *See also* 9 V.S.A. § 2453, Gen. Assemb., Reg. Sess. (Vt. 2018); 201 CMR 17, 2009 Leg., Reg. Sess. (Mass. 2009); ORS 646A.600-628, 2007 Leg., Reg. Sess. (Or. 2007).

example, this approach would destroy the prospect of a new "trust" model emerging from legislation such as the bill proposed in New York.

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 be fully discovered. The last handful of years have brought us tracking pixels, facial recognition, deep fakes, robot dogs, and even omnipresent satellites.[279] 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.[280]

If a federal law preempts state information privacy law, the CCPA might be lost to history. Yet it would 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."[281] This would be a significant and long-lasting California Effect, indeed.

3. The First Amendment

Another potentially significant 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 EU 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.

---

[279] Clare Garvie, Alvaro Bedoya, & Jonathan Frankle, *Perpetual Line-Up: Unregulated Police Face Recognition in America,* https://www.perpetuallineup.org/; Ry Crist, *Yes, the Robot Dog Ate Your Privacy*, CNET, June 28, 2019 8:21 am PDT, https://www.cnet.com/news/yes-the-robot-dog-ate-your-privacy/; Christopher Beam, *Soon, Satellites Will Be Able to Watch You Everywhere All the Time*, TECH. REV. (June 26, 2019), https://www.technologyreview.com/s/613748/satellites-threaten-privacy/.

[280] 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." SABEL ET AL., BEYOND BACKYARD ENVIRONMENTALISM 7 (2000). *See also* 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 (2013); McGeveran, *supra* note 14; Lauren E. Willis, *Performance-Based Consumer Law*, 83 U. CHI. L. REV. 1309 (2015).

[281] Heather K. Gerken & James T. Dawson, *Living Under Someone Else's Law*, 36 DEMOCRACY J. 42, 46 (2015).

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).[282] A series of First Amendment cases on public records established significant limitations on laws restricting the distribution of lawfully obtained information.[283] More recently, the Supreme Court has applied the First Amendment to find unconstitutional a Vermont law regulating the sale of prescription drug user data.[284] And in 2018, the Supreme Court found unconstitutional a series of disclosure requirements aimed at protecting women patients from pro-life organizations posing as abortion providers.[285]

Recently, the expansive coverage and protection of First Amendment doctrine has led some to decry its potential deregulatory effects.[286] On the other hand, privacy scholars have noted that the First Amendment provides arguments for effective privacy law, as a lack of privacy can chill free expression.[287] Commentators broadly disagree on how much of data privacy law might survive First Amendment challenges.[288] Through court challenges or

---

[282] *See* Margot E. Kaminski, *Privacy and the Right to Record*, 97 B.U. L. REV. 167 (2017).

[283] Cox v Cohn, *see* Volokh, *supra* note 90.

[284] Sorrell v. IMS, 564 U.S. 552 (2011). *See* Anupam Chander, *Free Speech*, 100 IOWA L. REV. 501, 522 (arguing that *Sorrell* demonstrates "the seriousness of First Amendment constraints on privacy regulations on information intermediaries"). *Cases such as* Florida Star v. BJF, 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) 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. (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). Sorrell https://www.oyez.org/cases/2010/10-779.

[285] *National Institute of Family Life v. Becerra*, SCOTUSBLOG (last visited Feb. 5, 2020), https://www.scotusblog.com/case-files/cases/national-institute-family-life-advocates-v-becerra/.

[286] *See* Amanda Shanor, *The New Lochner*, 2016 WISC. L. REV. 133 (2016); MARY ANNE FRANKS, THE CULT OF THE CONSTITUTION (2019).

[287] *See, e.g.*, Marc Jonathan Blitz, C*onstitutional 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 (2006); Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387(2008); Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. Rich. L. Rev. 465 (2015); Scott Skinner-Thompson, *Recording as Heckling*, 108 Geo. L. Rev. 125 (2019); Anupam Chander, *Youthful Indiscretion in an Internet Age*, in THE OFFENSIVE INTERNET 124, 134 (2010).

[288] For a sampling of this extensive debate, see Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57 (2014); Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501; Volokh, *supra* note 90.

through its expanding cultural penumbra, the First Amendment thus 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 effective privacy law governing global corporations will be the strictest aspects of both California and European law—a figurative, but not literal, highest common denominator.[289] Corporations operating across the Atlantic 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. "Under [the CCPA], the attorney general of California will become the chief privacy officer of the United States of America," Alastair Mactaggart declared.[290]

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 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.[291] 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 has emerged as the superregulator of U.S. privacy law.

---

[289] 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.

[290] Confessore, *supra* note 204.

[291] Clearview, Privacy Request Forms, https://clearview.ai/privacy/requests (last visited Feb. 6, 2020 at 7:43 pm) (including a separate reference to the UK, as necessitated by Brexit).