Stitching a Privacy Patchwork Together—for Now: The Constitutionality of State Privacy Regulations Under the Dormant Commerce Clause

Michael DeJesus*

TABLE OF CONTENTS

* Michael DeJesus is currently a J.D. Candidate at the George Washington University Law School with an expected graduation date of May 2022. Previously, he has interned at AARP Foundation Litigation, Government Accountability Project, and the CFTC Whistleblower Office. Prior to law school, he was the Public Interest Advocacy Fellow at Taxpayers Against Fraud Education Fund and graduated from American University in 2017.

I. INTRODUCTION

Commentators once hailed the Internet as a force for democratization and freedom, and many had overwhelmingly positive opinions about large technology companies like Google and Facebook—but now, attitudes have shifted drastically, decrying the extent of both state and corporate surveillance.[1] Americans now harbor little trust for large technology companies, and view the Internet as threatening personal privacy: over three out of five Americans say it is "not possible to go through daily life without" either business or the government "collecting data about them."[2] Shifting public attitudes and a newfound concern over privacy have led consumer data privacy advocates to call for consumer protection regulations.

Some advocates look to the European Union's (E.U.) General Data Protection Regulation (GDPR) as a model. But with the U.S. Congress rejecting FCC regulations governing Internet-service provider (ISP) use of consumer data as recently as 2017, consumer data privacy advocates have now focused their efforts on protecting consumers at the state level.[3] Amidst this push, detractors have claimed that a regime of "patchwork privacy" would tear asunder the original liberating impact of the Internet, and would raise nigh-impossible regulatory barriers for the next wave of digital entrepreneurs. They claim state data privacy regulations would simply contribute to the corporate consolidation that many consumer advocates seek to prevent and stymie innovation, without meaningfully protecting consumer

1. *See, e.g.*, Astra Taylor, *How the Internet Is Transforming from a Tool of Liberation to One of Oppression*, HUFFINGTON POST (Aug. 4, 2014), https://www.huffpost.com/entry/internet-oppression-liberation_b_5449838; Nicholas Carr, The World Wide Cage, AEON (Aug. 26, 2020), https://aeon.co/essays/the-internet-as-an-engine-of-liberation-is-an-innocent-fraud [https://perma.cc/VB2Q-92VJ].

2. BROOKE AUXIER ET AL., AMERICANS AND PRIVACY: CONCERNED, CONFUSED AND FEELING LACK OF CONTROL OVER THEIR PERSONAL INFORMATION 2 (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/6F64-SZUW].

3. *See* Glenn G. Lammi, Washington Legal Foundation, *The Nullification of FCC's Broadband Privacy Rules: What It Really Means for Consumers*, FORBES (Apr. 12, 2017), https://www.forbes.com/sites/wlf/2017/04/12/the-nullification-of-fccs-broadband-privacy-rules-what-it-really-means-for-consumers/?sh=7f1f99a779ba (acknowledging that consumer advocates were opposed to the move on the grounds that it allowed Internet service providers to collect and sell consumer personal information) [https://perma.cc/2QKX-2TUS]; *see also* Brian Fung, *What to Expect Now that Internet Providers Can Collect and Sell Your Web Browser History*, WASH. POST (Mar. 29, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/03/29/what-to-expect-now-that-internet-providers-can-collect-and-sell-your-web-browser-history/ (noting that congressional action prevented Internet privacy protections from taking effect that "would have would have banned Internet providers from collecting, storing, sharing and selling certain types of personal information — such as browsing histories, app usage data, location information and more — without [consumer] consent") [https://perma.cc/UY44-P7C4].

privacy.[4] Particularly, they claim state action in this area violates the dormant commerce clause.[5]

But policymakers should not fear patchwork privacy in the face of federal inaction. Instead, they can embrace state-level data privacy legislation as the natural byproduct of federalism. The likely constitutionality of stringent measures like the California Consumer Privacy Act (CCPA), and its successor, the California Privacy Rights Act (CPRA), suggests even the most robust state-level consumer privacy protections do not run afoul of the dormant commerce clause. Accordingly, absent federal action, state legislatures may take the task of consumer data protection upon themselves.

In Section II, I discuss why policymakers might embrace a "patchwork privacy" regime in the face of federal inaction. In Section III, I discuss why the dormant commerce clause does not preclude even the most sweeping state-level consumer data privacy laws, adopting the CCPA as the main statute of focus. Then, in Section IV, I review the different forms of consumer privacy laws at the state level and consider how arguments about the CCPA's constitutionality under the dormant commerce clause might apply. I conclude in Section V by discussing how state consumer data privacy laws might interplay with potential federal regulations in the future, and by recapping the practical necessity of leaning on the states as "laboratories of democracy" at this moment.

II. AMERICANS HAVE LITTLE TO FEAR FROM "PATCHWORK PRIVACY"

Many practitioners and commentators caution against embracing a "patchwork privacy" regulatory framework. Their opposition is rooted in the notion that "the [I]nternet requires a uniform system of regulation," and that state restrictions would tear the "free flow of digital information" asunder.[6] Others have pointed out that patchwork privacy might lead to genuine confusion among consumers and entrepreneurs over which law governs their conduct, and erode Americans' confidence that their personal data will be

4. Jennifer Huddleston, *The Problem of Patchwork Privacy*, TECHNOLOGY LIBERATION FRONT (Aug. 15, 2018), https://techliberation.com/2018/08/15/the-problem-of-patchwork-privacy (arguing "these type of statutes are likely to impact innovation in a misguided attempt to correct issues with data privacy…[and] also unintentionally make it more difficult for small, local companies to compete with Internet giants") [https://perma.cc/Q9TL-7YGC].

5. *See* Jennifer Huddleston & Ian Adams, *Potential Constitutional Conflicts in State and Local Data Privacy Regulations*, REGUL. TRANSPARENCY PROJECT (Dec. 2, 2019), https://regproject.org/paper/potential-constitutional-conflicts-in-state-and-local-data-privacy-regulations/ [https://perma.cc/XD9Q-DKAC].

6. *Id.*

secure.[7] Opponents of state-led action claim also that the regulatory patchwork has little upside for consumers, merely causing a "drag" on the economy, "creat[ing] operational inefficiencies[,] and distort[ing] interstate markets."[8]

However, Americans want their representatives to act. In a 2019 Pew Research Center survey, approximately 75% of Americans expressed support for increased government regulation of how companies handle consumer personal information.[9] So long as Americans' privacy rights and interests remain unprotected at the federal level, state legislators can act to protect their constituents' privacy. Notably, legislators in California passed the CCPA and had it signed into law by the governor in 2018, with the law coming into effect in 2020.[10] Subsequently, California voters passed the CPRA in November 2020, strengthening protections in the CCPA and creating a Privacy Protection Agency to enforce the law.[11]

Not all state consumer data privacy regulations will be perfect or optimal policy. For instance, there are legitimate criticisms of the marginal costs that the CCPA imposes on growing and capitalizing technology companies. However, these legitimate criticisms do not prevent states from taking action to protect their residents now while federal legislation remains elusive.

A. Policymakers Must Deal with the Internet as It Is, Not as They Would Like It to Be—and that Means Embracing Patchwork Privacy in the Interim

Though the Internet was once popularly conceived as a "digital wild west" of innovation, entrepreneurship, and social experimentation, many commentators now claim the Internet is subject to the same institutional

7. Michael Beckerman, *Americans Will Pay a Price for State Privacy Laws*, N.Y. TIMES (Oct. 14, 2019), https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html (claiming "[a] patchwork of state laws means that a California woman who orders an item from a Missouri business that manufactures in Florida could have her data regulated by three separate laws, or by no applicable law… [this] will also undoubtedly lead to inconsistent treatment of data… Americans cannot be confident that their data remains protected as they travel from state to state") [https://perma.cc/KZJ5-8QP2].

8. Boyd Garriott et al., *The Case for Uniform Standards Grows as States Sew More Laws into Patchwork of Data-Privacy Regulations*, WASH. LEGAL FOUND., Sept. 27, 2019, https://www.wlf.org/wp-content/uploads/2019/09/09272019GarriottBrownWeeks_LB.pdf [https://perma.cc/B8ZL-GABZ].

9. *See* AUXIER ET AL., *supra* note 2, at 43.

10. Tim Peterson, *Why California's New Consumer Privacy Law Won't Be GDPR 2.0*, DIGIDAY (July 9, 2018), https://digiday.com/marketing/californias-consumer-privacy-law-has-digital-ad-industry-searching-for-answers/ [https://perma.cc/2EB3-58XK].

11. Sara Morrison, *California Just Strengthened Its Digital Privacy Protections Even More*, VOX (Nov. 4, 2020, 12:06 PM), https://www.vox.com/2020/11/4/21534746/california-proposition-24-digital-privacy-results [https://perma.cc/D7VL-J5GC].

sclerosis and consumer rights concerns as the wider economy.[12] Technology companies' claim that sectoral self-regulation is necessary for the open Internet is a claim under increasingly rigorous scrutiny. [13] Policymakers are increasingly moving past the notion "that government intervention would be costly and counterproductive" instead, they are embracing it as a tool.[14]

Patchwork privacy may not be the optimal solution for protecting American consumers or regulating an Internet economy. But thus far, attempts to address the issue legislatively have failed on the federal level. Despite legislators' recognition of the issue, Republicans and Democrats remain unable to marry competing bills, with over thirty bills filed since the election in 2018.[15] Perhaps one of the most serious bipartisan pushes for a federal privacy law recently ended in failure. Senior members on the Senate Committee on Commerce, Science, and Transportation who engaged in bipartisan negotiations failed to produce a bipartisan bill and instead released two separate proposals, with the ranking Republican member proposing the United States Consumer Data Privacy Act (USCDPA) and the ranking Democrat proposing the Consumer Online Privacy Rights Act (COPRA).[16] Though the Biden Administration instructed the Federal Trade Commission (FTC) to begin writing rules governing consumer surveillance in a July 2021 executive order, the rulemaking process "is expected to take years to complete" and legislative efforts have still "failed to gain traction."[17] Additionally, though the U.S. House Energy and Commerce Committee voted fund a data privacy bureau within the FTC as part of a proposed $3.5 trillion

12. Shoshana Zuboff, *You Are Now Remotely Controlled*, N.Y. TIMES (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html (describing how technology companies' assurances that "they were capable of regulating themselves and that government intervention would be costly and counterproductive" produced an Internet "operated by private surveillance capital" that takes "behavioral data" and sells it to business customers in the market for "human futures" like targeted online advertising) [https://perma.cc/L657-T6ZB].

13. *See id.* (recounting an "unusually heated" 1997 Federal Trade Commission meeting where technology industry executives vigorously argued against government oversight and disputed civil libertarians' warning that "that the companies' data capabilities posed 'an unprecedented threat to individual freedom'").

14. *Id.*

15. *See* Cameron F. Kerry & Caitlin Chin, *How the 2020 Elections Will Shape the Federal Privacy Debate*, BROOKINGS INST. (Oct. 26, 2020), https://www.brookings.edu/blog/techtank/2020/10/26/how-the-2020-elections-will-shape-the-federal-privacy-debate/ (noting that, in spite of the fact that "the 116th Congress opened with great energy and promise for federal privacy legislation," efforts to pass a bill "fell short" in the wake of the pandemic and "partisan polarization") [https://perma.cc/2BUY-M559].

16. *See id.* (noting "where Chairman Roger Wicker (R-MS) once called for a federal privacy law 'on the books by the end of 2019' and senior members engaged in bipartisan negotiations….[but] [b]y the end of 2019, though, Wicker and Ranking Member Maria Cantwell (D-WA) each released separate proposals").

17. Andrea Vittorio, *Biden's Executive Order Links Data Collection to Competition*, BLOOMBERG L. (July 9, 2021, 4:17 PM), https://news.bloomberglaw.com/privacy-and-data-security/bidens-executive-order-links-data-collection-to-competition [https://perma.cc/C99P-B78X].

domestic policy bill, recent negotiations show a much smaller package is being considered in the Senate and the fate of the proposal is unclear.[18]

Because comprehensive legislation to protect American consumers' privacy rights at the federal level continues to elude proponents, state-level protections are an avenue for protecting consumer data privacy rights in the interim. States have long been recognized as "laboratories of democracy," and have stepped in where the federal government has failed to act. Differing policy approaches towards issues as disparate as marijuana legalization and election regulations have been recognized as an outgrowth of this federalist tradition.[19]

U.S. states' action on privacy is not limited to the patchwork of data breach regulations—rather, states have acted in a number of other pressing areas where federal policy is lacking or nonexistent. Commentators in favor of state action note that "[s]tates have been the source of numerous privacy innovations," favorably citing: "laws on identity theft victim rights, data breach notification, limitations on the use of Social Security numbers, cell phone data privacy, cybersecurity, and cyber-exploitation (sometimes known as 'revenge porn')."[20] These proponents of state action acknowledge that harmonization of competing standards would be ideal, but still recognize these varied policies as "innovative" in the interim.[21]

The patchwork of data breach notification regulations is a counterpoint to those detractors who suggest that state-level regulation only leads to insurmountable regulatory hurdles for business. All fifty U.S. states—as well as the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands—have laws requiring that both public and private entities notify consumers of security breaches that disclose personally identifying information.[22] Though commentators do rue the lack of regulatory consistency and call for the implementation of a national standard, these calls are not accompanied by demands for rolling back all state data breach notification laws in the absence

---

18. *See* Diane Bartz, *U.S. Panel Votes to Approve $1 Billion for FTC Privacy Probes*, REUTERS (Sept. 14, 2021, 7:38 PM), https://www.reuters.com/business/us-panel-votes-approve-1-billion-ftc-privacy-probes-2021-09-14/; Emily Cochrane, *Democrats Are Courting Manchin on Their Agenda. Here's What He Wants*, N.Y. TIMES (Oct. 20, 2021), https://www.nytimes.com/2021/10/18/us/politics/democrats-manchin-domestic-policy-bill.html (noting that Senator Joe Manchin (D-W.V.) "does not want the bill to cost more than $1.5 trillion over the course of a decade…") [https://perma.cc/B6FH-BMK5].

19. *See, e.g.*, Tom Keane, *An Experimental State*, BOS. GLOBE (Jan. 7, 2014), https://www.bostonglobe.com/opinion/2014/01/07/colorado-pot-experiment-testament-founding-fathers/pvUGE1H8lOYktyKzFL1xnL/story.html (calling Colorado's legalization of marijuana a manifestation of states acting as "laboratories of democracy") [https://perma.cc/K4QE-QHGU]; Mark Schmitt et al., *Electoral Systems*, NEW AMERICA, https://www.newamerica.org/in-depth/laboratories-of-democracy/electoral-systems/ (providing information on different states' electoral systems in a wider "Laboratories of Democracy" database) [https://perma.cc/4CD2-637C].

20. Joanne McNabb, *Can Laboratories of Democracy Innovate the Way to Privacy Protection?*, CENTURY FOUND. (Apr. 5, 2018), https://tcf.org/content/report/can-laboratories-democracy-innovate-way-privacy-protection [https://perma.cc/7EM2-7BUU?type=image].

21. *Id.*

22. *Security Breach Notification Laws*, NAT'L CONF. STATE LEGISLATURES, https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/VD3M-XSQC].

of a federal alternative.[23] The patchwork of data breach notification laws has not led to economic ruin or raised impossible hurdles to compliance. Sometimes a subpar regulatory framework is better than the complete lack of one. In the case of data breach laws, states chose to adopt regulation lest consumers suffer from the potential harm of identity theft.[24]

B. The Federal Government Has Declined to Intercede in this Area for the Benefit of American Consumers

The 2017 nullification of the FCC rule governing ISP handling of consumer data, and the FCC's lack of preemption authority over state and local regulation, show that the federal government has thus far failed to act to protect American consumers. The present lack of clear federal guidelines governing the handling of consumers' personal data should not mean that consumers remain unprotected. Indeed, both prior federal action and federal court rulings suggest that—barring a comprehensive law passed by Congress—states can and should provide protection for their resident consumers.

1. The 2017 Nullification of FCC Rules Governing ISP Handling of Consumer Data Illustrate that the Federal Government Is Currently Unable to Safeguard Americans' Privacy

The federal government's inability, so far, to act decisively to protect consumer data privacy is illustrated by the 2017 nullification of FCC regulations under the Congressional Review Act, which allows Congress to repeal federal regulations and prevent the issuing agency from promulgating similar regulation at later date with the approval of the President.[25] The repeal scrapped previously promulgated 2016 FCC regulations which would have required Internet service providers "to obtain consumer consent before using precise geolocation, financial information, health information, children's information and web browsing history for advertising and marketing."[26]

---

23. *See, e.g.*, Joseph Marks, *Equifax Breach Prompts Renewed Calls for National Breach Notification Standard*, NEXTGOV (Sept. 18, 2017), https://www.nextgov.com/cybersecurity/2017/09/equifax-breach-prompts-renewed-calls-national-breach-notification-standard/141098/ (noting policymakers' support for national standard in data breach notification without their contesting the necessity of state-level regulations in the interim) [https://perma.cc/74MC-L67S].

24. Fabio Bisogni & Hadi Asghari, *More Than a Suspect: An Investigation into the Connection Between Data Breaches, Identity Theft, and Data Breach Notification Laws*, J. INFO. POL'Y, 2020 at 46, https://doi.org/10.5325/jinfopoli.10.2020.0045 [https://perma.cc/3W57-8HJW].

25. Kelly Ding, *Congress Rolls Back FCC Broadband ISP Privacy Rules*, JOLT DIGEST (Apr. 04, 2017), https://jolt.law.harvard.edu/digest/congress-rolls-back-fcc-broadband-isp-privacy-rules [https://perma.cc/9FTL-WWU8].

26. David Shepardson, *Trump Signs Repeal of U.S. Broadband Privacy Rules*, REUTERS (Apr. 3, 2017, 7:50 PM), https://www.reuters.com/article/us-usa-internet-trump-idUSKBN1752PR [https://perma.cc/6PEL-PQVH].

Proponents hailed their repeal, while ruing how the regulations were supposedly, according to then-FCC Chairman Ajit Pai, originally intended to "benefit one group of favored companies, not online consumers."[27]

But with repeal of the regulations, consumers' personal data is even less protected, and both groups of businesses may merely sell it to the highest bidder. Instead, Internet service providers can "monitor their customers' behavior online and, without their permission, use their personal and financial information to sell highly targeted ads."[28] And consumer privacy advocates appropriately have noted that "although consumers can easily abandon sites whose privacy practices they don't agree with, it is far more difficult to choose a different Internet provider" given the paucity of options throughout the U.S.[29]

2. Because the Current Internet Regulatory Framework Is Inadequate for Establishing Consumer Protection Online, the States Should Act Where There Is No Clear Prohibition

The federal government has also ceded overarching national regulatory authority over the Internet in other respects. Notably, the courts have struck down expansive arguments by regulatory agencies that, with or without explicit statutory authority, federal regulations can preempt state or local action in certain circumstances. For instance, courts have stated that the FCC does not have overarching authority to preempt all state regulation of communications.[30]

The decision in *Mozilla Corp. v. Fed. Commc'ns Comm'n*, 940 F.3d 1 (D.C. Cir. 2019), is illustrative. Petitioners in *Mozilla* brought suit challenging a 2018 FCC order that reclassified broadband Internet access as an "information service," as opposed to its prior classification as a "telecommunications service" under the 1996 Telecommunications Act.[31] They also sought to strike down its Preemption Directive, which sought to "bar[] states from imposing any rule or requirement that the FCC repealed or

27. *See id.*

28. Brian Fung, *The House Just Voted to Wipe Away the FCC's Landmark Internet Privacy Protections*, WASH. POST (Mar. 28, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/the-house-just-voted-to-wipe-out-the-fccs-landmark-internet-privacy-protections/ [https://perma.cc/9K5F-R86M].

29. *See id.* (noting "[m]any Americans have a choice of only one or two broadband companies in their area, according to federal statistics").

30. Louisiana Pub. Serv. Comm'n v. FCC, 476 U.S. 355, 373-74 (1986) (stating that "[a]lthough state regulation will generally be displaced to the extent that it stands as an obstacle to the accomplishment of the full purposes and objectives of Congress, a federal agency may pre-empt state law only when and if it is acting within the scope of its congressionally delegated authority").

31. *See Mozilla*, 940 F.3d at 17 (noting "the 1996 Telecommunications Act creates two potential classifications for broadband Internet: 'telecommunications services' under Title II of the Act and 'information services' under Title I").

decided to refrain from imposing in the Order or that is "more stringent" than the Order."[32]

The Court of Appeals for the D.C. Circuit sided with petitioners with respect to the Preemption Directive, finding the FCC lacked the express or ancillary authority necessary to issue the order.[33] The court also rejected the FCC's assertion that a "statement of policy" in 47 U.S.C. § 230(b)(2) stating "the policy of the United States [is] . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation" conferred the necessary authority.[34] The court took care to note that conflict preemption is "fact-intensive" and only applies when "actual preemption of a specific state regulation occurs."[35] The court further declined to find that the principle of conflict preemption justified issuance of the Preemption Directive, because "[w]ithout the facts of any alleged conflict before us, we cannot . . . [make] a categorical determination that any and all forms of state regulation of intrastate broadband would inevitably conflict with the 2018 Order."[36] It noted that the FCC's 2018 Order survived without blanket application of the preemption doctrine to uphold the Preemption Directive, and that the doctrine could still be invoked on a case-by-case basis as originally intended.[37]

The lack of concerted federal legislation in this area shows the federal government has been dilatory in protecting a key interest in the twenty-first century: the Internet privacy rights of American consumers. Proponents of state consumer data privacy initiatives should heed the D.C. Circuit's ruling. *Mozilla* underscores the ability of states to regulate telecommunications where there is no federal statute controlling. In light of *Mozilla*, states—and even local governments—can now identify areas where the federal government has not yet trod, and can take action on their own behalf in response to constituent calls for additional regulation. However, state policymakers should still remain aware that, though the FCC lacks categorical preemption authority in the Order, *Mozilla* does not preclude state-level regulations from being struck down on a case-by-case basis. At this point, courts have not yet opted to do so, and are loathe to find preemption "absent an actual conflict."[38]

---

32. *Id.* at 18 (internal quotations omitted).
33. *Id.* at 75.
34. *Id.* at 78 (quoting 47 U.S.C. § 230(b)(2)).
35. *Id.* at 81-82.
36. *Id.* at 82.
37. *See id.* at 85 (stating "[i]f the [FCC] can explain how a state practice actually undermines the 2018 Order, then it can invoke conflict preemption. If it cannot make that showing, then presumably the two regulations can co-exist as the Federal Communications Act envisions") (citing 47 U.S.C. § 152(b)).
38. *See* ACA Connects - Am.'s Commc'ns Ass'n v. Frey, 471 F. Supp. 3d 318, 324-26 (D. Me. 2020) (citing Eng. v. Gen. Elec. Co., 496 U.S. 72, 90 (1990)) (rejecting defendant's argument that the State of Maine's consumer data privacy law was preempted by Congress's 2016 abrogation of FCC rules or by the FCC's own RIF order, noting that there is a "strong presumption against implied federal preemption of state law" and that preemption "cannot be a 'mere byproduct of self-made agency policy.'" (quoting *Mozilla*, 940 F.3d at 78)).

C. Proponents of a State "Patchwork" of Data Privacy Regulations Must Grapple with Arguments That These Efforts Violate the Dormant Commerce Clause

Opponents also argue that a regulatory patchwork is not only inefficient, but a violation of the dormant commerce clause. Thus far, the majority of opponents' claims of unconstitutionality have been focused on one piece of consumer data privacy legislation: the CCPA. Many seek to strike down the law due to its "broad, sometimes unclear" language that opponents maintain makes compliance difficult.[39] Other commentators take a broader view of what the CCPA presages for the future of consumer data privacy regulation across the United States. Some fear that similarly comprehensive laws across the country would create an inconsistent patchwork "with different requirements . . . so contradictory that it would be impossible to comply with every state."[40]

Opponents are likely to intensify their efforts with the recent 2020 passage of the CRPA at the ballot box, which clarifies the scope of and expands the protections in the CCPA.[41] The onset of CRPA regulations in 2023—a whole three years after the November 2020 ballot initiative passing it and just after "the ink was barely dry on the CCPA"—underscores how the regulatory environment is in flux.[42] The new regulatory standards in the CRPA are both intended to increase protections for individuals that consumer advocates thought were lacking, and to further harmonize with the higher standards in the E.U. GDPR.

Passage of the CRPA imposes even more stringent checks on businesses in the name of consumer data privacy. The CRPA has been recognized as "the strictest data privacy law in the U.S.," and was intentionally designed to "draw[] on many key aspects of the [E.U.'s]

---

39. *See* Jonathan Ende, *Though CCPA Is Now Live, Questions Concerning Its Constitutionality Linger*, JD SUPRA (Jan. 10, 2020), https://www.jdsupra.com/legalnews/though-ccpa-is-now-live-questions-76600/ [https://perma.cc/7G2F-NWW4].

40. Jennifer Huddleston, *The State of State Data Laws, Part 2: Consumer Data Privacy Legislation*, MERCATUS CTR. (Aug. 6, 2019), https://www.mercatus.org/bridge/commentary/state-state-data-laws-part-2-consumer-data-privacy-legislation (paraphrasing May 2019 Congressional testimony from Commissioner Christine S. Wilson of the Federal Trade Commission) [https://perma.cc/NL98-RVUX].

41. *See CPRA Rivals GDPR's Privacy Protections While Emphasizing Consumer Choice*, AKIN GUMP STRAUSS HAUER & FELD LLP (Nov. 11, 2020), https://www.akingump.com/en/news-insights/cpra-rivals-gdprs-privacy-protections-while-emphasizing-consumer-choice.html (noting that "new CPRA made its way to the November 2020 ballot…" after consumer advocates were "disheartened by the number of statutory amendments proposed by 'special interests' after the CCPA was enacted and the potential that such amendments could eviscerate the statute's key privacy protections") [https://perma.cc/3QEH-U6EZ].

42. *See id.* (stating that "businesses [are] grappl[ing] with the CPRA and prepar[ing] for the majority of the provisions to become operative in 2023…").

GDPR."[43] Though the CRPA raised the threshold application of California privacy law to those businesses serving California residents from 50,000 to 100,000, it also increased other privacy protections for businesses in a manner likely to raise opponents' ire.[44] For instance, the CRPA expands on all consumer rights previously in the CCPA and includes a new right to rectification of incorrect personal data, and a new right to "limit [the] use of disclosure of sensitive personal information."[45] The new Act also increases the fine on businesses that divulge the personal information of minors, and expands consumers' private right of action against noncompliant businesses to include breaches of email addresses, passwords, and security questions.[46]

The measure's originators recognized that detractors might seek to curb some of the regulation's more stringent requirements either in text or in enforcement. Notably, the CRPA also imposes a "one-way ratchet" intended to prevent the measure from being watered down by the California state legislature: though the legislature can impose additional amendments that benefit consumers with a simple majority vote, the CRPA requires that all amendments "enhance privacy and are consistent with and further the purposes and intent of the Act."[47] Yet, perhaps one of the most notable facets of the law is its creation of the California Privacy Protection Agency—the first agency dedicated to consumer privacy in the U.S., and one that consumer advocates have hailed as "a major milestone."[48]

Both the scope of CCPA and CRPA protections and the prospect of similarly broad protections being extended to consumers state-by-state have engendered substantial warnings from commentators. According to opponents of state-level regulation, "[r]egulation of the [I]nternet is inherently cross-jurisdictional."[49] Opponents contend that mandated "changes to the [regulatory] system for out-of-state platforms, content creators, and businesses . . . places an undue burden on commerce conducted or created by these entities."[50] They note that California's actions extend throughout the entire country: that the "practical effect" of state data privacy legislation will "affect entire industries and cost hundreds of millions, if not billions, of

43. Karen Schuler, *Federal Data Privacy Regulation Is on the Way — That's a Good Thing*,, INT'L ASS'N PRIV. PROS. (Jan. 22, 2021), https://iapp.org/news/a/federal-data-privacy-regulation-is-on-the-way-thats-a-good-thing/ [https://perma.cc/8PY2-SHEJ].

44. *CCPA vs. CPRA – What Has Changed?*, ONETRUST (Nov. 10, 2020), https://www.onetrust.com/blog/ccpa-vs-cpra-what-has-changed/ [https://perma.cc/L382-W4V6].

45. *See id.*

46. *See id.*

47. *See* Cybersecurity, Privacy & Data Protection Alert, *supra* note 41 (citing CPRA, 2020 Cal. Legis. Serv. Prop. 24 § 25).

48. Stacey Gray et al., *California's Prop. 24, the "California Privacy Rights Act," Passed. What's Next?*, FUTURE PRIV. F. (Nov. 4, 2020), https://fpf.org/blog/californias-prop-24-the-california-privacy-rights-act-passed-whats-next/ [https://perma.cc/9LV8-MSG8].

49. Huddleston & Adams, *supra* note 5, at 10 (noting that "[t]he The 2015 Open Internet Order, promulgated by the Federal Communications Commission . . . declared that the [I]nternet is inherently an interstate service") (citing In the Matter of Protecting & Promoting the Open Internet, *Report and Order on Remand, Declaratory Ruling, and Order*, 30 FCC Rcd 5601, para. 431 (2015), https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf).

50. *See* Huddleston, *supra* note 40.

dollars, including affecting business practices and industries not limited to conduct occurring within California."[51] Commentators have also claimed that this state-level legislation is merely an attempt to implement national policy by other means: proponents' framing of the consumer benefit in national terms does not lend weight to the argument that state legislation is intended to predominately benefit state residents.[52]

Opponents of approaching consumer data privacy on a state-by-state basis make legitimate points with respect to efficiency and the onerousness of complying with a wide set of conflicting state standards. However, their contention that these measures are likely unconstitutional under the dormant commerce clause is not necessarily true. Below, I consider how state data privacy regulations should survive the dormant commerce clause test established in *Pike v. Bruce Church*, with a focus on the CCPA as amended by the CPRA.

III. COURTS HAVE PREVIOUSLY UPHELD STATE REGULATIONS OF INTERNET ACTIVITY TOUCHING INTERSTATE COMMERCE, FINDING NO VIOLATION OF THE DORMANT COMMERCE CLAUSE

Previously, courts have upheld the constitutionality of various state statutes regulating Internet activities and have found they do not violate the dormant commerce clause. Accordingly, applying the same test used in *Pike*, courts will likely find that consumer data privacy regulations in the mold of the CCPA and CPRA are constitutionally sound. Though *Pike* originally concerned the burden on interstate commerce imposed by Arizona's onerous labeling requirements for produce grown in-state, in that case, the Court laid out its approach to determining the constitutionality of those state laws which touch interstate commerce.[53]

Though states may pass legislation exceeding their ordinary power under the dormant commerce clause in limited circumstances, it is likely that arguments that the U.S. Congress's abrogation of FCC regulations in 2017 constitute a substantive authorization of state laws on the matter will fail, as "it has long been the rule that Congress must "manifest its unambiguous intent before a federal statute will be read to permit or to approve . . . a violation of

51. Alysa Z. Hutnik et al., *Potential Constitutional Challenges to the CCPA*, KELLEY DRYE & WARREN LLP : AD L. ACCESS (Dec. 12, 2019), https://www.adlawaccess.com/2019/12/articles/potential-constitutional-challenges-to-the-ccpa/ [https://perma.cc/EP4H-HDXK].

52. *See, e.g.*, Andrea O'Sullivan, *Are California's New Data Privacy Controls Even Legal?*, REASON (Dec. 17, 2019), https://reason.com/2019/12/17/are-californias-new-data-privacy-controls-even-legal/ (noting "California Attorney General Xavier Becerra… frames his mandate in national terms, stating that 'Americans should not have to give up their digital privacy to live and thrive in this digital age.' That's *Americans*, not Californians") (emphasis in original) [https://perma.cc/Z2VR-P98R].

53. *See generally*, Pike v. Bruce Church, Inc., 397 U.S. 137 (1970).

the Commerce Clause."[54] Nothing in the Congressional Review Act resolution abrogating the standards unambiguously authorizes the states to enact consumer data protection regulation beyond the scope ordinarily provided to the states by the commerce clause.[55]

Under the *Pike* balancing framework, courts consider first whether the law in question facially discriminates against interstate commerce. If the law is not facially discriminatory, then the court considers whether the benefit that inures to state citizens as a result of the regulation is outweighed by the burden the regulation places on interstate commerce.[56] Per the court:

> Where the 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 . . . [if] a legitimate local purpose is found, then the question becomes one of degree. And the extent of the burden that will be tolerated will of course depend on the nature of the local interest involved, and on whether it could be promoted as well with a lesser impact on interstate activities.[57]

Notably, California consumer data privacy laws, as set forth in both the CCPA and CPRA, are not facially discriminatory against out-of-state commerce.[58] Accordingly, the analysis of the constitutionality of state consumer data privacy regulations will mainly consider the balancing test in *Pike*: whether the benefit resulting from the legitimate local purpose outweighs the burden imposed on interstate commerce.

Statutes that "impose such rigidity on an entire industry" that they "preserve or secure employment for the home State" are unconstitutional even if that is not their concealed or express purpose.[59] However, "legislation that may cause businesses to decide to conform nationwide conduct to meet the

---

54. Rousso v. State, 204 P.3d 243, 248 (Wash. Ct. App. 2009) (stating that, despite State's contention, federal statutes in question do not constitute evidence of "unambiguous intent" to permit potential violation of Commerce Clause by State's statute regulating online gambling) (citing *Wyoming v. Oklahoma*, 502 U.S. 437, 458 (1992)) (ruling for the respondent on other grounds).

55. *See* S.J. Res. 34, 115th Congress, 131 Stat. 88 (2017) (expressing "congressional disapproval" and providing that FCC regulations governing ISP use of consumer data have no effect).

56. *Pike*, 397 U.S. at 142.

57. *Id.*

58. *See, e.g.*, CAL. CIV. CODE 1798.140(c), (g) (West 2021) (defining some businesses as those satisfying in-state preconditions and defining consumers as "any natural person who is a California resident"); *Proposition 24: California Privacy Rights Act of 2020*, *in* CAL. SEC'Y OF STATE, OFFICIAL VOTER INFORMATION GUIDE 42, 49, https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf (last visited Nov. 16, 2021) (enacted in CAL. CIV. CODE 1798.199.10–.95) (establishing that the CPRA changes the scope of entities covered, but still only applies to businesses that "[do] business in the state of California" and that consumers are "natural person[s] who [are]… . . . California resident[s]") [https://perma.cc/X78C-54MA].

59. *Id.* at 145-46.

requirements of a given state does not necessarily constitute direct regulation of out-of-state commerce."[60] Additionally, courts have also stated that laws which "[do] not compel any action or conduct of the business with regard to" out-of-state businesses do not violate the dormant commerce clause.[61] Courts have previously considered privacy rights of state residents to constitute a sufficiently weighty interest to pass muster, especially when considering other telecommunications regulations, absent an undue burden on interstate commerce.[62] If so, then the law does not violate the dormant commerce clause.

Nonetheless, courts do not hesitate to strike down laws where the purported public benefit to state citizens is clearly outweighed.[63] They afford "less deference to legislative judgment" with respect to local benefits "where the local regulation bears disproportionately on out-of-state residents and businesses."[64] Courts have previously found that state regulations which "substantially increase the cost of such movement" of goods between states may place a burden on interstate commerce that outweighs the benefit provided to the state's citizens.[65] They have also looked unfavorably upon regulations that have a "speculative contribution" to promoting the intended local interest.[66]

A. State Data Privacy Laws Will Likely Pass the Pike Balancing Test, Because Consumer Data Privacy Protections Are a Legitimate Local Benefit

State data privacy laws of similar scope to the CCPA, as amended by the CPRA, will likely pass the *Pike* balancing test. Contrary to detractors' assertions, protecting the privacy of a state's residents is a legitimate local interest recognized by the courts in previous suits, and can be the basis of a successful defense against charges of dormant commerce clause unconstitutionality.

60. Ades v. Omni Hotels Mgmt. Corp., 46 F. Supp. 3d 999, 1014 (C.D. Cal. 2014).

61. Kearney v. Salomon Smith Barney, Inc., 137 P.3d 914, 922 (Cal. 2006) (holding that California's two-party consent recording law does not violate the dormant commerce clause because it "would affect only a business's undisclosed recording of telephone conversations with clients or consumers in California . . . [not] with non-California clients or consumers").

62. *See, e.g.*, *Ades*, 46 F. Supp. 3d at 1014 (holding that a California statute prohibiting nonconsensual recordings "has the purpose of preventing privacy harms to Californians" and that effects to interstate commerce were "incidental" even though "it might create incentives for [defendant] to alter its behavior nationwide"); Rezvanpour v. SGS Auto. Servs., Inc., No. 8:14-CV-00113-ODW, 2014 WL 3436811, at *5 (C.D. Cal. July 11, 2014) (declining to grant a defendant's motion to dismiss a claim under a California statute prohibiting nonconsensual recording of communications involving at least one cell phone on the basis it violated dormant commerce clause, in part because defendant lacked extrinsic evidence to prove their claim of being unable to ascertain geographic location of cell phone calls based on area code).

63. Kassel v. Consol. Freightways Corp. of Del., 450 U.S. 662, 671 (1981).

64. *Id.* at 676.

65. Raymond Motor Transp., Inc. v. Rice, 434 U.S. 429, 4457-48 (1978).

66. *Id.* at 447.

Securing residents' personal privacy is not a frivolous concern—rather, courts have recognized it as a legitimate purpose for state legislation.[67] In *Ades*, the court explicitly rejected a defendant's contention that applying a law intended to protect residents' personal privacy rights "provide[d] 'no real benefit whatsoever,'" and underscored that a properly functioning regulatory regime designed to protect privacy implicates "real local interests."[68] A successful challenger would need to provide clear evidence that protecting residents' privacy rights placed an undue burden on interstate commerce, not merely make a factual supposition that this is the case.[69]

Here, the local interests at stake are identical to those in *Zephyr* and *Rezvanpour*: California residents' privacy interests, and state residents' privacy interests more broadly. The CCPA, both alone and as amended by the CPRA, only seeks to regulate the handling of consumer data of those natural persons living in California.[70] If privacy interests are sufficient to justify a California law regulating the recording of telephone conversations including California residents, it makes little sense to exclude the regulation of consumers' personal data on the grounds that personal privacy is insufficiently weighty as to justify *any* burden placed on interstate commerce. The contemporary extent of surveillance is much more comprehensive than contemplated in the California statue. Surreptitious recordings of telephone conversations are merely one way to infringe on residents' privacy. Smartphones, Internet browsers, particular websites, and smartwatches are all collecting vast amounts of personal data that, even if anonymized, can still identify a consumer and make predictions about a consumer if aggregated—providing the unique snapshot of an individual that consumers commonly associate with "social security numbers [and] account numbers."[71] Even

67. Zephyr v. Saxon Mortg. Servs., Inc., 873 F. Supp. 2d 1223, 1229 (E.D. Cal. 2012) (observing that the California Supreme Court previously "held that the federal law does not preempt the application of California's more protective privacy provisions… [and] that states could enact more restrictive privacy laws than those imposed by federal law").

68. *See Ades*, 46 F. Supp. 3d at 1015 (C.D. Cal. 2014) (holding that a refusal to apply the law in this instance would "impair the privacy policy guaranteed by California law," that protection of residents' privacy fell under "real local interests," and that the defendant needed evidence to "[show] clearly excessive burdens on interstate commerce") (internal citations omitted).

69. *See, e.g.*, *Zephyr*, 873 F. Supp. 2d at 1231-32 (ruling against defendant because "Saxon has presented no evidence of any particular burden that would compel this Court to conclude that the burden on interstate commerce so outweighed the benefit to California residents"); *see also* Rezvanpour v. SGS Auto. Servs., Inc., No. 8:14-CV-00113-ODW, 2014 WL 3436811, at *5 (C.D. Cal. July 11, 2014) (finding that extrinsic evidence was necessary to prove contention that interest in protecting privacy was outweighed by burden on interstate commerce).

70. *See CPRA Rivals GDPR's Privacy Protections While Emphasizing Consumer Choice*, *supra* note 41.

71. Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today - and How to Change the Game*, BROOKINGS INST. (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ (noting that "aggregation and correlation of data from various sources make it increasingly possible to link supposedly anonymous information to specific individuals and to infer characteristics and information about them ") [https://perma.cc/ERS2-3HXK].

devices connected via the Internet of things (IoT) are now sources of sensitive personal information "just waiting to be mined" or sold.[72] Experts have gone so far as to call our current age the "Golden Age of Surveillance," with the IoT "providing more access than ever in history."[73]

Detractors and defendants may argue that consumers care little about privacy regulations, and that whatever weight the public places on them is outweighed by any burden that protective regulations place on interstate commerce. But in the case of California, residents have made their desires clear. In a November 2020 referendum, over 55.86% of participating eligible voters—over 9.3 million people—voted in favor of passing the CPRA.[74]

In short, standing caselaw suggests that the protection of state residents' privacy is a justifiable, legitimate local benefit in an age of widespread consumer surveillance. Accordingly, state consumer data privacy laws in the mold of the CCPA should pass the portion of the *Pike* inquiry which implicitly requires a legitimate local interest.

B. The Benefit of State Data Privacy Laws Likely Outweighs the Burden on Interstate Commerce

State consumer data privacy legislation in the mold of the CCPA is also likely constitutional under the dormant commerce clause because it does not place an undue burden on interstate commerce. Despite opponents' arguments, various courts' rulings upheld the constitutionality of other state-level regulations of online conduct as varied as sending "spam" emails to those engaging in online gambling. Therefore, courts may not find that consumer data privacy legislation in the mold of the CCPA is so uniquely onerous as to violate the dormant commerce clause.

Courts across the country have recognized the constitutionality of various state laws that regulate business conduct on the Internet. In *State v. Heckel*, the Washington State Supreme Court concluded that a state law prohibiting spam emails was constitutional under the dormant commerce clause.[75] The court looked at how the law benefited multiple groups—spanning both consumers and industry—as well as how the harms of spam were well-known: "The Act protects the interests of three groups—ISPs, actual owners of forged domain names, and e-mail users. The problems that spam causes have been discussed in prior cases and legislative hearings."[76] Other courts cited *Heckel* in upholding their own laws directed against spamming and reducing fraud, finding that the burden on online senders of

72. Elanie McArdle, *The New Age of Surveillanc*e, HARVARD L. TODAY (May 10, 2016), https://today.law.harvard.edu/feature/new-age-surveillance/ [https://perma.cc/RV4H-U8GT].

73. *Id.*

74. Sara Morrison, *Live Results for California's Data Privacy Ballot Initiative*, VOX (Nov. 4, 2020), https://www.vox.com/policy-and-politics/2020/11/3/21546835/california-proposition-24-live-results-data-privacy

75. State v. Heckel, 24 P.3d 404, 409 (Wash. 2001).

76. *Id.*

unsolicited commercial emails "clearly does not outweigh" the local benefits provided by the legislation.[77]

In another suit, the Maryland Court of Special Appeals found the Maryland Commercial Electronic Mail Act did not run afoul of the dormant commerce clause on similar grounds. The Court ultimately held that:

> MCEMA... does not prevent senders of email advertisements from soliciting the residents of other states; *it merely regulates those that are sent to Maryland* residents or from equipment located in Maryland. *The Act does not project Maryland's regulatory scheme into other states because email advertisers remain free to send emails to other states*.[78]

The court also cited *Heckel* favorably throughout the opinion and noted the similarity between the Maryland and Washington laws.[79] Ultimately, *MaryCLE* stands for the proposition that merely regulating Internet conduct involving Internet users in a certain state does not constitute "projecting" that state's regulatory scheme into other states.

Accordingly, courts' application of the dormant commerce clause was not limited to laws regulating spam emails. Instead, courts proved themselves willing to allow states to regulate other activities on the Internet and were not reflexively supportive of plaintiffs' claims that laws regulating Internet-based businesses proved too costly to justify the purported public benefit.

Courts have permitted regulation of Internet payday lending even when "plaintiff contend[ed] that the burden on interstate commerce created by Kansas's regulation of out-of-state Internet payday lenders clearly exceed[ed] the benefits afforded by such regulation . . . "[80] But it held the plaintiff must show evidence "of what those costs might be[;]" simply arguing it is burdensome is insufficient.[81] Courts also have upheld online gambling regulations in the absence of being able to identify nondiscriminatory alternatives, and have found that the future existence of "more sophisticated means of policing the [I]nternet" did not preclude state legislation that treats "online betting differently than gambling that takes place at brick-and-mortar establishments."[82] "The introduction of a new technology" like the Internet

77. Ferguson v. Friendfinders, Inc., 115 Cal. Rptr. 2d 258, 269 (2002) (modified Jan. 14, 2002) (upholding the constitutionality of CAL. BUS. & PROF. CODE § 17538.4 (West 2021) (repealed 2003), which regulated the sending of unsolicited commercial emails by entities engaging in business in California).

78. MaryCLE, LLC v. First Choice Internet, Inc., 890 A.2d 818, 843 (Md. Ct. Spec. App. 2006) (emphasis added).

79. *See generally id.*

80. Quik Payday, Inc. v. Stork, 509 F. Supp. 2d 974, 978 (D. Kan. 2007), *aff'd*, 549 F.3d 1302 (10th Cir. 2008).

81. *Id.* at 980.

82. Churchill Downs Inc. v. Trout, 979 F. Supp. 2d 746, 755 (W.D. Tex. 2013), *aff'd*, 767 F.3d 521 (5th Cir. 2014).

makes regulation "more daunting," and further tips the balance away from the finding an undue burden exists on interstate commerce.[83]

The breadth of areas where courts have permitted regulation of online conduct likely bodes well for proponents of state data privacy legislation. Though the CCPA and CPRA are much wider in scope than most state regulatory frameworks that courts considered here, courts' declination to strike down state regulations of online commerce affecting state residents cuts against opponents' arguments that the Internet is such an interstate medium that state-level data privacy regulations are likely to place an undue burden on interstate commerce. Like the statute prohibiting unsolicited email advertisements in *MaryCLE* was not said to "project" Maryland's statutory prohibition into other states because "it merely regulates those that are sent to Maryland residents," the CCPA as amended by the CPRA cannot be said to project California's statutory scheme into other states, because it solely covers California consumers.[84] Just as the court in *Churchill Downs* noted that the introduction of new technologies made the court less likely to find an undue burden existed with the approval of online gambling regulations, so too should future courts find that the rapid expansion of consumer data collection technologies justify the CPRA regulations.[85]

C. State Consumer Data Privacy Laws Are Likely to Pass the Pike Test Where State Regulations Are Similar and Multistate Compliance Is Simple

Opponents of California's consumer data privacy laws often argue that the costs of complying with a "patchwork" of laws in a similar vein create the "undue burden" that defeats these measures under the dormant commerce clause.[86] Indeed, courts have previously considered whether the state regulations at issue are contemporaneously inconsistent with other states' regulations in determining whether they violate the dormant commerce clause.[87]

But commentators have also identified instances when regulatory statutes challenged under the dormant commerce clause prevailed in part because they mirrored regulatory schemes widely adopted throughout the

83. *See Churchill Downs Inc.*, 979 F. Supp. 2d at 754 (holding that "When the issue is, as here, the introduction of a new technology into an already difficult to control area like gambling, the state's interest in regulating the conduct becomes even more compelling").

84. MaryCLE, LLC v. First Choice Internet, Inc., 890 A.2d 818, 843 (Md. Ct. Spec. App. 2006).

85. *See Churchill Downs Inc.*, 979 F. Supp. 2d at 755.

86. *See* Huddleston, *supra* note 5 (stating that "even slight differences in state level privacy laws will create [d]ormant [c]ommerce [c]lause-triggering undue burdens as out-of-state companies confront the choice to either comply with the most stringent state laws or create individual and less efficient products for each state or local regulation.").

87. *See, e.g.*, IMS Health Inc. v. Mills, 616 F.3d 7, 28 (1st Cir. 2010), *vacated and remanded by sub nom.* IMS Health, Inc. v. Schneider, 564 U.S. 1051 (2011), (noting that "Maine's law does not risk imposing regulatory obligations inconsistent with those of other states. No other states have erected competing regulations, much less opposing regulations requiring the transfer of Maine prescribers' data").

United States. Arguing for the constitutionality of the CCPA under the dormant commerce clause, Spivak identifies *State v. Maybee* as of particular interest.[88] In *Maybee*, the Oregon Court of Appeals' decision upheld an Oregon statute requiring tobacco producers not party to a prior settlement agreement with the state to provide information to the state attorney general.[89] Spivak stated that, "[i]n performing its balancing test, the court was careful to note that 'the burden on interstate commerce is minimal, in light of the fact that forty-six other states have similar statutes.'"[90]

Some commentators have noted that the CPRA mirrors the E.U. GDPR so closely that "several of the new CPRA provisions are based on the [GDPR] with an eye towards obtaining an adequacy decision from the European Commission."[91] Because many websites have already configured their businesses to comply with the GDPR, compliance with the CPRA is less likely to be found an undue burden than in the regulation's absence.[92]

However, a disharmonious patchwork of consumer data privacy regulations could lead to a court striking down a state's data privacy law under the *Pike* test. In this scenario, contradictory state laws that make interstate compliance effectively impossible would place enough of a burden on interstate commerce to justify striking one of them down. *IMS Health* suggests that inconsistent regulatory standards across state lines might constitute a dormant commerce clause violation.[93] Previously, in *Healy v. Beer Inst.*, the Supreme Court pointedly stated that the dormant commerce clause "protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another [s]tate."[94] Subsequent circuit courts have cited this criterion as one of part of the "principle against extraterritoriality."[95]

However, this element of the principle against extraterritoriality does not necessitate categorically prohibiting state data privacy laws. Harmonious regulations across the several states would not lead to the same burden as in *Healy*, because they would not make interstate compliance impossible. As

88. Russell Spivak, *Too Big a Fish in the Digital Pond? The California Consumer Privacy Act and the Dormant Commerce Clause*, 88 U. CINCINNATI L. REV. 512, 512 https://scholarship.law.uc.edu/cgi/viewcontent.cgi?article=1342&context=uclr (citing *State v. Maybee*, 232 P.3d 970, 977 (Or. Ct. App. 2010).

89. *Maybee*, 232 P.3d at 971.

90. Russell Spivak, *supra* note 88 (citing *Maybee*, 232 P.3d at 971).

91. *See CPRA Rivals GDPR's Privacy Protections While Emphasizing Consumer Choice*, *supra* note 41.

92. Caitlin Fennessy, *CPRA's Top 10 Impactful Provisions, International Association of Privacy Professionals* (May 12, 2020), https://iapp.org/news/a/cpra-top-10-impactful-provisions/ (noting that, for a portion of the CPRA, "[t]hese new provisions will be familiar to many businesses already complying with the GDPR, which the CPRA mirrors in this regard") [https://perma.cc/4XBJ-XXDX].

93. *See* IMS Health Inc. v. Mills, 616 F.3d 7, 28 (1st Cir. 2010), *vacated and remanded by sub nom.* IMS Health, Inc. v. Schneider, 564 U.S. 1051 (2011).

94. *Healey v. Beer Inst., Inc.*, 491 U.S. 324, 337 (1989).

95. *See Ass'n for Accessible Medicines v. Frosh*, 887 F.3d 664, 669 (4th Cir. 2018) (striking down a Maryland statute prohibiting price gouging in prescription drug sales on the grounds it violated the dormant commerce clause).

discussed above, consumer data privacy laws would likely pass muster so long as compliance is not impossible for covered entities.

IV. THE LIKELY CONSTITUTIONALITY OF A BROAD STATUTE LIKE THE CCPA SUGGESTS DORMANT COMMERCE CLAUSE CHALLENGES TO OTHER STATES' CONSUMER PRIVACY PROTECTIONS MAY FAIL

Because the CCPA or CRPA may pass constitutional muster under the dormant commerce clause, other consumer data privacy statutes in other states will likely survive—especially given that many other states' regulations are of a much more limited scope. According to the National Conference of State Legislatures, over thirty U.S. states and Puerto Rico considered implementing data privacy legislation in 2020.[96]

Nevada and Maine adopted their own versions of consumer data privacy legislation in 2019.[97] However, neither statute is as expansive as the CPRA. The Maine statute, the Act to Protect the Privacy of Online Consumer Information, only applies to Internet service providers in the state, and requires them to get permission from consumers "before selling or sharing their data with a third party."[98] It also prohibits internet service providers "from offering consumers discounts in exchange for selling their data."[99] Nevada passed a similar consumer data protection law more expansive than the Maine statute—the Nevada law does not only apply to Internet service providers, but "operators of Internet websites and online services" as well.[100] However, the statute is narrower than either the CCPA or CPRA—particularly when defining who is a "consumer" under the terms of the Act.[101]

Meanwhile, the recent passage of the Consumer Data Protection Act (CDPA) in the Virginia state legislature is perhaps the most significant development in the state data privacy legislation landscape. Hailed as "the East Coast version of the [CCPA]," the CDPA is of similar scope to both the

96. *2020 Consumer Data Privacy Legislation*, NAT'L CONFERENCE OF STATE LEGISLATURES, (Jan. 17, 2021) https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx.

97. Gary Guthrie, *Consumer Privacy Regulation Progresses at the State Level*, CONSUMERAFFAIRS (June 19, 2019), https://www.consumeraffairs.com/news/consumer-privacy-regulation-progresses-at-the-state-level-061919.html.

98. Steven Musil, *Maine Governor Signs Strict Internet Privacy Protection Bill*, CNET (June 6, 2019), https://www.cnet.com/news/maine-governor-signs-internet-privacy-protection-bill/ [https://perma.cc/S6NZ-RFN3].

99. *Id.*

100. Alexandra Scott & Lindsey Tonsager, *Nevada's New Consumer Privacy Law Departs Significantly from The California CCPA*, COVINGTON: INSIDE PRIVACY (June 10, 2019), https://www.insideprivacy.com/united-states/state-legislatures/nevadas-new-consumer-privacy-law-departs-significantly-from-the-california-ccpa/ [https://perma.cc/NUE4-T76X].

101. *See id.* (contrasting the Nevada Act's definition of "consumer" with the expansive definition adopted by the California Legislature in the CCPA, which "includes any California resident").

CCPA and GDPR and is expected to be signed into law by the governor.[102] The act "expands Virginia's definition of personal data" to include "sensitive data" covering sexual orientation, race, religion, medical diagnoses, and biometric data, among other categories.[103] It also, like the CCPA and GDPR, allows consumers to delete or obtain copies of personal data collected by companies, and opt out of company processing and profiling of personal data. The CDPA does, however, contain exemptions "far broader" than other state data privacy laws.[104] It does not apply to individual data obtained from individuals in business-to-business transactions, or to the personal data of employees.[105] The CDPA also "applies to persons who conduct business in Virginia."[106] Additionally, unlike the CCPA, it lacks a private right of action for consumers, and is enforced solely by the state's Attorney General.[107] Under the CDPA, violators would be subject to fines up to $7,500.[108]

Consumer advocates and supporters of the CPRA should be heartened by the adoption of consumer data privacy protections in an increasing number of states. However, these statutes are likely to run into the same criticism and legal opposition as the CPRA, despite many new statutes' more limited scope. Proponents and supporters can reduce the likelihood that courts will find that these new measures impose an undue burden by harmonizing with CPRA guidelines, as well as those in the GDPR. The easier compliance is for businesses, the less likely that state regulations will be struck down as undue and onerous. Accordingly, state policymakers should heed some commentators' distain for a patchwork regulatory framework and avoid unnecessary variation across state statutes.

V. CONCLUSION

A federal framework establishing clear, harmonized national guidelines for consumer data privacy protection would provide American consumers with peace of mind and ease business' efforts to comply with a patchwork of varied regulations. But the current lack of federal regulation is far from ideal. Patchwork privacy, while not necessarily an optimal solution, is necessary in

102. Allison Schiff, *CCPA On The East Coast? Meet CDPA, Virginia's Consumer Data Protection Act*, AD EXCHANGER (Feb 2, 2021), https://www.adexchanger.com/privacy/ccpa-on-the-east-coast-meet-cdpa-virginias-consumer-data-protection-act/.

103. Elizabeth Harding & Caitlin A. Smith, *New Virginia Privacy Bill*, 11 NAT. L. REV. 47 (Feb. 16, 2021), https://www.natlawreview.com/article/new-virginia-privacy-bill [https://perma.cc/9ALQ-NAHT].

104. Alexander Koskey III & Matthew White, *Privacy Legislation Floodgates Have Opened: Virginia Passes the Consumer Data Protection Act*, JDSUPRA (Feb. 24, 2021), https://www.jdsupra.com/legalnews/privacy-legislation-floodgates-have-7999102/ [https://perma.cc/4JB9-Q2HL].

105. *See id*.

106. *Id.*

107. *Id.*

108. Matt Dumiak, *CDPA: Virginia's Consumer Data Protection Act*, COMPLIANCE POINT (Feb. 18, 2021), https://www.compliancepoint.com/privacy/cdpa-virginias-consumer-data-protection-act/ [https://perma.cc/MMG5-6A9T].

light of the federal government's inability to safeguard the privacy rights of American consumers.

Here, analysis of dormant commerce clause constitutionality has mainly been confined to the CCPA, as amended by the CPRA, due to sweeping scope of consumer data protection regulations in California. The great weight of commentary on these pieces of legislation has been critical. Many claim that beyond heralding in a completely unworkable patchwork regulatory framework, these provisions burden interstate commerce to such an extent as to be unconstitutional. But as shown above, this is not necessarily true. There is a body of caselaw that has held both that privacy constitutes a legitimate local interest and that state laws regulating online commercial conduct affecting their residents do not necessary constitute an undue burden on interstate commerce. Accordingly, proponents for taking CPRA-style consumer data privacy protections nationwide can point towards this precedent. Harmonizing regulations between states and between widely adopted international standards like the GDPR would further minimize any burden on interstate commerce. And already existing state laws outside of California are likely to continue to stand, if only because their narrower scope likely means that they place a smaller burden on interstate commerce.

Additionally, adopting a patchwork privacy regime now does not preclude a comprehensive federal fix in the future. Whether or not an overarching federal law should preempt then-existing state consumer data privacy regulations depends in large part how unharmonized the future patchwork becomes; commentators are correct to point out that wildly inconsistent regulatory regimes will make business compliance efforts difficult. And contradictory state data privacy regimes that effectively make compliance impossible across states may raise their own discrete questions under the dormant commerce clause. Ultimately, these questions are fertile ground for future research.