COMMENT

NICE THOUGHT, POOR EXECUTION: WHY THE DORMANT COMMERCE CLAUSE PRECLUDES CALIFORNIA'S CCPA FROM SETTING NATIONAL PRIVACY LAW

KIRAN K. JEEVANJEE[*]

Technology plays a growing role in the lives of Americans. As technology's role in society increases, so does the amount of data companies collect from their consumers. News outlets are publishing an increasing number of stories about how shocking amounts of data are stored and collected with very few checks on the organizations that take part in these practices. Consumers are increasingly aware of the vast amount of data collected by companies, leading to widespread digital privacy anxiety. In the absence of a national law, states have stepped in to tame this largely unregulated space. The California Consumer Privacy Act (CCPA) constitutes California's effort to fill in the void left by the lack of federal privacy legislation. The CCPA attempts to provide comprehensive data privacy protections to California's citizens.

This Comment argues that the CCPA, in its current form, violates the dormant Commerce Clause because it imposes an undue burden on non-California-based businesses by compelling them to comply with stringent requirements before collecting

[*] Senior Symposium Editor, *American University Law Review*, Volume 70; J.D. Candidate, May 2021, *American University Washington College of Law*; B.A. Dance and Political Science, 2018, *The George Washington University*. I am extremely grateful to the many people that helped me take this piece from blank page to publication. I would like to thank my editor, Daniel de Zayas, my faculty advisor, Stephen Wermiel, and the entire *AULR* staff for their constant support, diligent feedback, and valuable assistance in creating this piece. I would also like to thank my family, friends, and Ben for always encouraging me in my endeavors, and for their steadfast support throughout my law school career.

or processing California citizens' personally identifiable information. Furthermore, it urges that Congress should interpret the CCPA as a public desire for a national comprehensive privacy law and work to pass legislation that gives Americans legitimate privacy rights.

TABLE OF CONTENTS

Introduction 77
- I. The California Consumer Privacy Act 81
  - A. Privacy in the United States 81
  - B. The Beginnings of the CCPA 84
  - C. A Closer Look at the CCPA 88
    - 1. Scope, compliance, and predicted impact 92
      - a. The scope of the CCPA 92
      - b. Compliance and its challenges 95
        - i. The right to know & the right to access 96
        - ii. The erasure right 100
        - iii. The right to "opt-out" of data sales 102
        - iv. Anti-discrimination provisions 103
        - v. Minimal private right of action that only exists where there is a data breach 103
- II. The Dormant Commerce Clause 105
  - A. Defining Commerce: *Gibbons v. Ogden* 105
  - B. Discriminatory Impact 106
  - C. The *Pike* Balancing Test 108
  - D. Extraterritoriality 109
  - E. Inconsistent Regulation 114
  - F. A Dormant Commerce Clause for a Modern World? 115
    - 1. Obscenity regulations and the dormant Commerce Clause: *American Library Ass'n v. Pataki* 116
    - 2. Anti-spam regulations and the dormant Commerce Clause: *State v. Heckel* 118
- III. Analysis 120
  - A. The CCPA Does Not Discriminate Against Out-of-State Actors 120
  - B. The CCPA Fails the *Pike* Balancing Test by Imposing Significant and Excessive Burdens on

Interstate Commerce that Are Not Outweighed by the Local Putative Benefits 121
C. The CCPA Regulates Conduct that Occurs Wholly Outside of the State 126
D. The CCPA Will Likely Lead to Multiple Conflicting Comprehensive Data Privacy Laws........ 128
IV. The United States Needs a National Privacy Law......... 130
Conclusion.. 132

INTRODUCTION

Increased integration of technology into the everyday lives of Americans means that more Americans must confront their blatant lack of digital privacy. A father of a teenage daughter was enraged when Target coupons for baby and pregnancy-related products arrived via mail addressed to his daughter. Much to his surprise, the coupons were not the result of a poorly designed ad campaign, but rather Target had predicted his daughter's pregnancy before she had the chance to tell him.[1] Rosie Spinks, a runner, was shocked to discover that her "Enhanced Privacy" settings on the popular running app Strava broadcasted her habitual running routes that strangers could view.[2] In the workplace, companies track employees' texts, chats, emails, and meetings and even review recorded and transcribed phone calls, all under the guise of measuring "productivity, management efficacy[,] and work-life balance."[3] Consumers are beginning to realize

[1] Kashmir Hill, *How Target Figured out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012, 11:02 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did [https://perma.cc/CP7P-JLUE].

[2] Rosie Spinks, *Using a Fitness App Taught Me the Scary Truth About Why Privacy Settings Are a Feminist Issue*, QUARTZ (Aug. 1, 2017), https://qz.com/1042852/using-a-fitness-app-taught-me-the-scary-truth-about-why-privacy-settings-are-a-feminist-issue [https://perma.cc/Y745-VF7M]. *See generally A Look Back at Women Murdered While Jogging*, ABC 7 NEWS (Sept. 19, 2018), https://abc7news.com/mollie-tibbets-women-killed-while-jogging-murdered-famous-murders/4022767 [https://perma.cc/7DPP-X35S] (listing a few cases of women murdered while jogging that captured national attention).

[3] Sarah Krouse, *The New Ways Your Boss Is Spying on You*, WALL ST. J. (July 19, 2020, 5:30 AM), https://www.wsj.com/articles/the-new-ways-your-boss-is-spying-on-you-11563528604.

how little control they have over data that is shared about them.[4] There are an increasing number of stories published about how shocking amounts of data are stored and collected with very few checks on the organizations that take part in these practices.[5]

While most individuals' privacy horror stories result in nothing more than nominal insecurity and inaction, Alastair Mactaggart's digital privacy anxiety led to one of the largest developments in the history of U.S. privacy law. During an evening of pizza and wine at his Oakland, California home, Mactaggart, a wealthy real-estate developer, brought his privacy concerns to a friend who just so happened to be a software engineer at Google.[6] Much to Mactaggart's dismay, his friend informed him that "there was plenty to worry about, [that i]f people really knew what [Google] had on them, . . . they would flip out."[7] This conversation was the genesis of what would soon become the first comprehensive data privacy law in the United States, which would be

[4] *See, e.g.*, Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, PEW RES. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information [https://perma.cc/FV5R-CBYW] (discussing results from various polls confirming that the vast majority of Americans have digital privacy anxiety); *see also* Cindy Compert, *New Poll Shows Consumers' Expectations on Data Privacy Evolve, but so Does Technology*, SECURITY INTELLIGENCE (Sept. 12, 2019), https://securityintelligence.com/posts/new-poll-shows-consumers-expectations-on-data-privacy-evolve-but-so-does-technology [https://perma.cc/73AZ-78M4] (reporting that eighty-four percent of polled consumers feel "flat-out dissatisfied" with the way businesses handle and process consumer data).

[5] *See, e.g.*, Stephen Gandel, *Ring to Tighten Privacy amid Concerns It Shares Customer Data with Facebook and Google*, CBS NEWS (Feb. 14, 2020, 2:55 PM), https://www.cbsnews.com/news/ring-facebook-google-personal-information-privacy-settings-change [https://perma.cc/8ADA-F9TE] (reporting that Ring, an Amazon-owned home security company that provides web-enabled video doorbells and security cameras, shares significant amounts of data with third parties such as Facebook and other companies that have legitimate data security issues); Maya Shwayder, *Houseparty Could Be a Digital Privacy Nightmare, Experts Warn*, DIGITAL TRENDS, (Mar. 30, 2020), https://www.digitaltrends.com/news/houseparty-privacy-tracking-security [https://perma.cc/ENS2-MCB6] (noting that the popular group video chatting app "Houseparty" collects an enormous amount of data about its users, including location information; does not guarantee that it will honor data deletion requests; and has not updated its privacy policy since June 2018).

[6] 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.

[7] *Id.*

would be written, debated, and passed in less than a week: the California Consumer Privacy Act[8] (CCPA).[9]

The CCPA constitutes California's effort to fill in the void left by the lack of federal privacy legislation. While the United States has some federal privacy laws, these laws are either specific to a certain industry or govern how a business can use certain categories of data, but the laws do not cover all situations through which privacy concerns can arise.[10]

Directly responding to consumers' growing digital privacy anxiety, the CCPA grants California residents unprecedented statutory privacy rights, such as the right to know what information businesses collect and the right to request that businesses delete the information altogether.[11] Businesses subject to the CCPA must give consumers the opportunity to exercise those rights[12] and are barred from discriminating[13] against consumers who choose to exercise their rights. Notably, however, the CCPA's business definition includes a broad material scope because the threshold for the amount of data that a business must process before it must comply with the law is relatively low.[14] Businesses subject to the CCPA range from tech giants like Amazon, Google, and Facebook to mom-and-pop shops located wholly outside of California.[15] The

[8] CAL. CIV. CODE §§ 1798.100–99 (West 2020).

[9] Confessore, *supra* note 6.

[10] *See, e.g.*, Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–06 (2018) (children's internet privacy); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2018) (education); Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (sending commercial email); Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (finances); Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (health information).

[11] CAL. CIV. CODE §§ 1798.100(a), 1798.105(a).

[12] *Id.* § 1798.130(a)(1)(A)–(B). The CCPA defines "personal information" much more broadly to include "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." *Id.* § 1798.140(o)(1).

[13] *Id.* § 1798.125(a)(1).

[14] *See id.* § 1798.140(c)(1)(B) (stating that any business that buys, receives, sells, or shares the data of 50,000 or more customers for commercial purposes is subject to the CCPA).

[15] *See* Jeff Kosseff, *Hamiltonian Cybersecurity*, 54 WAKE FOREST L. REV. 155, 179 (2019) (arguing that the CCPA is a cautionary tale against regulating cybersecurity on a state-by-state level); *see also* ERIC GOLDMAN, INTERNET LAW: CASES & MATERIALS 357–64 (2019) (summarizing the CCPA and highlighting its broad and sweeping definitions).

CCPA's intended targets will certainly be forced to overhaul their data practices, but the CCPA's wide reach created unintended consequences.[16]

The boundaries of the CCPA's broad material scope are circumscribed by the dormant Commerce Clause. The dormant Commerce Clause—sometimes called the negative Commerce Clause—is an implied limitation on the states' authority to burden or regulate interstate commerce.[17] Generally, a state's regulation amounts to regulating interstate commerce if (1) it is discriminatory against out-of-state business;[18] (2) it is non-discriminatory, but the burdens the regulation places on interstate commerce outweigh the local benefits (this balancing act is called the *Pike* test);[19] (3) it regulates conduct that takes places wholly extraterritorially;[20] or (4) it is one of many inconsistent regulations across multiple states.[21] The CCPA does not impose different requirements on companies outside of California compared with California-based companies.[22] However, to comply with the CCPA, businesses all over the country must spend significant amounts of time and money overhauling their data privacy practices—all in exchange for the residents of one state to have legitimate privacy rights.[23]

This Comment argues that the CCPA, in its current form, violates the dormant Commerce Clause because it imposes an undue burden on non-California-based businesses by compelling them to comply with

[16] *See infra* Part III (analyzing the consequences of the CCPA).

[17] Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785, 786 (2001) (noting that the dormant Commerce Clause is an entirely judge-made doctrine).

[18] *See, e.g.*, Maryland v. Louisiana, 451 U.S. 725, 756 (1981) (finding that Louisiana's natural gas tax ran afoul of the dormant Commerce Clause because it discriminated against out-of-state actors and favored local interests).

[19] Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970) ("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.").

[20] *See, e.g.*, Healy v. Beer Inst., 491 U.S. 324, 337 (1989) (holding that a Connecticut price-affirmation statute violated the dormant Commerce Clause because the statute regulated commercial activity occurring entirely outside the boundary of Connecticut).

[21] CTS Corp. v. Dynamics Corp. of Am., 481 U.S. 69, 88 (1987) ("This Court's recent Commerce Clause cases also have invalidated statutes that may adversely affect interstate commerce by subjecting activities to inconsistent regulations.").

[22] *See* CAL. CIV. CODE § 1798.140(c)(1)–(2) (West 2020) (defining a business that falls under the CCPA to include both in-state and out-of-state entities that process or collect California residents' data).

[23] *See infra* Section I.C.1 (discussing the specific challenges with CCPA compliance).

stringent requirements before collecting or processing California citizens' personally identifiable information. Furthermore, it urges that Congress should interpret the CCPA as a public desire for a national comprehensive privacy law and work to pass legislation that gives Americans legitimate privacy rights. Part I explains the perceived need for a comprehensive privacy law in the United States and explores the development and specific requirements of the CCPA. Part II discusses the history of the dormant Commerce Clause and examines how courts have interpreted the dormant Commerce Clause to both strike-down and uphold state internet regulation in the form of both pornography[24] and anti-spam statutes.[25] Finally, Part III argues that the CCPA violates the dormant Commerce Clause because it imposes an undue burden on non-California-based businesses, constitutes an extraterritorial regulation of interstate commerce, and raises legitimate concerns about the potential for multiple conflicting laws. This Comment concludes that courts should strike down the CCPA as unconstitutional and that Congress should pass a comprehensive national privacy law because regulation of the use of consumer data is imperative and states cannot enact their own laws without exceeding the scope of their authority.

I. THE CALIFORNIA CONSUMER PRIVACY ACT

Applying a dormant Commerce Clause analysis to the California Consumer Privacy Act first requires a thorough understanding of the CCPA. This Part explores the nation's attitude towards privacy, which led to the CCPA's development. It also discusses the CCPA's scope, compliance costs, and open questions concerning the CCPA's impact.

A. *Privacy in the United States*

Following the Cambridge Analytica scandal—an incident that exposed the data of eighty-seven million Facebook accounts to be used for nefarious purposes[26]—many Americans began to realize how much

[24] Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 178 (S.D.N.Y. 1997).

[25] State v. Heckel, 93 P.3d 189, 190 (Wash. Ct. App. 2004).

[26] Christopher Mims, *Privacy Is Dead. Here's What Comes Next*, WALL ST. J. (May 6, 2018), https://www.wsj.com/articles/privacy-is-dead-heres-what-comes-next-1525608001; *see also Facebook, Social Media Privacy, and the Use and Abuse of Data: Hearing Before the S. Comm. on Commerce, Sci., and Transp. and the S. Comm. on the Judiciary*, 115th Cong. 10 (2018) [hereinafter *Facebook Hearing*] (statement of Mark Zuckerberg, Chairman & CEO, Facebook) (explaining that an app developer, Aleksandr Kogan, created a personality

of their sensitive personal information is gathered, stored, and sold on a regular basis. Consumers consistently sign away their rights to their personal identifiable information without even taking the time to open a company's privacy policy.[27] Even if a consumer did take the time to read that policy, she may not even understand it because these policies are typically written in language that is difficult for the layperson to understand.[28] Additionally, even if the consumer is able to understand the policy, she likely would not be stopped from clicking "I Agree to the Terms and Conditions."[29] Since there is no longer any way to prevent marketers or malicious actors from gathering and using personal information, it is not hard to see why some believe that digital "privacy is dead."[30] Americans' ever-growing dependency on technology

quiz app installed by 300,000 Facebook users who "agreed to share some of their Facebook information as well as some information from their friends whose privacy settings allowed it," which gave Kogan access to tens of millions of Facebook users' data).

[27] *See* Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RES. CTR. (Dec. 4, 2014), https://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is [https://perma.cc/U47V-FRW3] (finding that fifty-two percent of Americans believe that when a company provides a privacy policy, it keeps all of their data confidential).

[28] Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.*, N.Y. TIMES (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html; *see also* Auxier, *supra* note 4 (finding that sixty percent of Americans read some privacy policies, with only nine percent always reading them; twenty-two percent of that sixty percent read policies all the way through; and only thirteen percent of that sixty percent claim to understand the majority of what the policy says); Tatiana Ermakova et al., *Privacy Policies and Users' Trust: Does Readability Matter?*, ASS'N FOR INFO. SYS. 2 (Aug. 2014), https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1141&context=amcis2014 [https://perma.cc/5YFZ-78UV] (finding the mean grade level required to understand a variety of existing privacy policies was a high-school reading level).

[29] *See* Marcus Moretti & Michael Naughton, *Why Privacy Policies Are so Inscrutable*, ATLANTIC (Sept. 5, 2014), https://www.theatlantic.com/technology/archive/2014/09/why-privacy-policies-are-so-inscrutable/379615 (explaining that it is extremely difficult for a consumer to clarify ambiguities in privacy policies and most companies do not provide resources to assist with the process, resulting in most consumers simply accepting the terms without protest).

[30] *See* Mims, *supra* note 26 (reporting pessimistically that Americans have no way to prevent "malicious actors" from obtaining personally identifying information).

at work, at school, and at home and the rise of the Internet of Things[31] only seems to cement the idea that privacy rights no longer exist.[32]

This notion, that privacy rights are dwindling, is not unique to the United States.[33] In April of 2016, the European Parliament approved the General Data Protection Regulation (GDPR),[34] which went into effect in May 2018.[35] This sweeping regulation was the first comprehensive privacy law with a major global impact. The GDPR created meaningful protections for personal information in the European Union (EU), and it created punitive measures for organizations that fail to comply.[36] Perhaps the GDPR's biggest impact was introducing the world to the concept of a "data protection law."[37] Following the implementation of the GDPR, consumers worldwide began to expect more from companies managing their data.[38]

While the United States has some privacy laws, these laws are specific to a certain industry or they govern how certain types of data can be

[31] FEDERAL TRADE COMMISSION, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 5 (2015) ("The IoT includes consumer-facing devices, as well as products and services that are not consumer-facing, such as devices designed for businesses to enable automated communications between machines.").

[32] *Id.* at 10.

[33] *See* CENTER FOR INTERNATIONAL GOVERNANCE INNOVATION, 2019 CIGI-IPSOS GLOBAL SURVEY ON INTERNET SECURITY AND TRUST (2019) (finding that sixty-two percent of internet users worldwide distrust companies' ability to keep their data safe).

[34] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

[35] *Id.* art. 99.

[36] *Id.* art. 84 (laying out the GDPR's penalty provisions); *see also* GDPR ENFORCEMENT TRACKER, https://www.enforcementtracker.com [https://perma.cc/6B3S-E6AT] (showing all public GDPR fines); Michael Burne, *Data Protection Regulation "to Show Its Teeth" in 2019*, PRIVSEC REPORT (Dec. 27, 2018), https://gdpr.report/news/2018/12/27/data-protection-regulation-to-show-its-teeth-in-2019 [https://perma.cc/F479-WCYY] (stating that firms in 2019 will start to comply with the mandates set forth in the GDPR and that more regional GDPR-like policies will begin to have an impact).

[37] Kosseff, *supra* note 15, at 170–71 (explaining that data protection law has come into prominence ever since the passing of the GDPR by the EU in 2016).

[38] *See* Kevin Cochrane, *To Regain Consumers' Trust, Marketers Need Transparent Data Practices*, HARV. BUS. REV. (June 13, 2018), https://hbr.org/2018/06/to-regain-consumers-trust-marketers-need-transparent-data-practices (reporting that providing consumers with privacy protections puts businesses at a competitive advantage).

used.[39] There is currently no national law governing the general use of data, and the limited existing U.S. privacy law is extremely narrow and does not cover all of the situations in which privacy concerns can arise.[40] Accordingly, consumers are increasingly aware of how little control they have over their data[41] thanks to the constant stream of privacy horror stories about the amount of data that is stored, collected, and sold with little to no oversight on the data collectors.[42]

B. The Beginnings of the CCPA

The origins of the CCPA rest in millionaire Alistair Mactaggart's discomfort with the United States' delayed approach to regulating digital privacy.[43] While Americans generally share this discomfort,[44] Mactaggart went a step further than most. He researched how much information companies really knew about him by educating himself about data mining and online tracking practices.[45] He scrutinized privacy policies that the average person barely gleaned and discovered that "there was no real limit on the information companies could collect or buy."[46] He learned that the primary purpose of all this data was to help businesses accurately advertise and sell him products that he may want.[47] Alarmingly, the amount of data available for sale allows businesses to predict consumer spending habits with incredible accuracy. In fact, "[w]ith Silicon Valley's help, [advertisers] could

[39] *See, e.g.*, *supra* note 10.

[40] *Cf.* Kirk J. Nahra (work) (@KirkJNahrawork), TWITTER (Apr. 14, 2019, 1:09 PM), https://twitter.com/KirkJNahrawork/status/1117474938259156993 (commenting that a new federal privacy bill would merely supplement existing federal data protections).

[41] Auxier, *supra* note 4.

[42] *See, e.g.*, Geoffrey A. Fowler, *Smartphone Data Reveal Which Americans are Social Distancing (and Not)*, WASH. POST (Mar. 24, 2020), https://www.washingtonpost.com/technology/2020/03/24/social-distancing-maps-cellphone-location (reporting that Unacast created a "coronavirus surveillance system" based on smartphone location tracking information).

[43] *See* Ben Adler, *California Passes Strict Internet Privacy Law with Implications for the Country*, NPR (June 29, 2018, 5:05 AM), https://www.npr.org/2018/06/29/624336039/california-passes-strict-internet-privacy-law-with-implications-for-the-country [https://perma.cc/ZQQ2-BYM2] (interviewing Mactaggart, who stated, "These giant corporations know absolutely everything about you, and you have no rights . . . . I thought, oh, I'd like to find out about what these companies know about me. Then I thought, well, someone should do something about that.").

[44] Auxier, *supra* note 4.

[45] Confessore, *supra* note 6.

[46] *Id.*

[47] *Id.*

make increasingly precise guesses about what [consumers] wanted, what [they] feared, and what [they] might do next: Quit [their] job, . . . have an affair, or get a divorce."[48]

Mactaggart, horrified by what he learned, felt the need to act.[49] He poured $3.5 million of his own money into calling attention to Californians' lack of digital privacy.[50] After consulting with privacy experts, Mactaggart learned that Silicon Valley would fight hard against any meaningful privacy regulation that the legislature tried to pass.[51] Mactaggart focused his efforts on drafting a ballot initiative that would bypass the California legislature and bring the data privacy issue directly to voters.[52] If passed, this initiative would impose significant legal, technical, and administrative burdens on companies, promising almost certain doom for the tech industry:

> Under the proposed law, every California consumer could demand, from most large businesses, an outline of his or her digital dossier, showing what categories of personal information the company had collected. Mactaggart and Soltani included nearly every category of personal information that they could think of: not only whether the companies had collected your name and address but also if they had collected your browsing history, your fingerprints, your face scans or your location data. They would also be required to inform consumers if they were drawing "inferences," the sophisticated guesses companies make about, say, your dating habits or your taste in convertibles. And if consumers didn't like the deal, they could "opt out," demanding that companies no longer sell or share any data in a given category.[53]

[48] *Id.*

[49] *See id.* ("But his research on privacy had stirred something in him. 'It's like that Buddhist thing, where you walk past a mess and a mop and say, "Someone ought to clean up that mess,"' he says. 'And eventually you realize you have to pick up the mop.'").

[50] Adler, *supra* note 43.

[51] *See* Confessore, *supra* note 6 (reporting on the formation of a new California committee that would likely raise over $100 million to fight Mactaggart's data privacy initiative).

[52] *See* CALIFORNIA SECRETARY OF STATE, STATEWIDE INITIATIVE GUIDE 1–12 (2020) (outlining the requirements for a ballot initiative, none of which require input from the California legislature).

[53] *See September 1: The Political Suspense*, CAL. POLITICS PODCAST (Sept. 1, 2017), https://soundcloud.com/politics-california/september-1-the-political-suspense [https://perma.cc/NB6C-AYBV] (commenting on Silicon Valley's efforts to shut down Mactaggart's ballot initiative).

This initiative promised to cripple Silicon Valley. In addition to being difficult to amend, the CCPA includes strict guidelines, hefty compliance costs, and harsh enforcement provisions that would be "toxic to the business community."[54]

Mactaggart's initiative found quick favor with voters and received the necessary number of signatures to ensure his initiative would be on the ballot for the November 2018 election.[55] While the Secretary of State certified Mactaggart's initiative, Mactaggart still faced significant personal costs before the ballot initiative would win over the majority of voters.[56] The technology industry was prepared to spend a lot of money to keep Mactaggart's initiative from becoming law.[57] Therefore, Mactaggart offered the California legislature a deal: draft a meaningful comprehensive privacy law that aligns with the spirit of his initiative, and he would formally withdraw his initiative from the ballot.[58] This was an attractive proposition to both parties; the California legislature had the opportunity to play a role in developing California's privacy legislation, and Mactaggart "would get his desired policy outcome without spending the millions more needed to contest the $100M that opponents threatened to spend."[59]

Moving at unprecedented speeds, the California legislature introduced, amended, and passed the California Consumer Privacy Act.[60] The

[54] Goldman, *supra* note 15, at 357 (noting that amending laws that emerge through the ballot initiative process requires another ballot initiative, which is a cumbersome process).

[55] John Myers & Jazmine Ulloa, *California Lawmakers Agree to New Consumer Privacy Rules that Would Avert Showdown on the November Ballot*, L.A. TIMES (June 21, 2018, 8:40 PM), https://www.latimes.com/politics/la-pol-ca-privacy-initiative-legislature-agreement-20180621-story.html.

For a ballot initiative statute to get on the California ballot, it must be signed by at least five percent of the total votes cast in the last governor race. CAL. CONST., art. II, § 8(b); CAL. ELEC. CODE § 9035. In 2018, the number of signatures needed was 365,880. *Signature Requirements for Ballot Measures in California*, BALLOTPEDIA, https://ballotpedia.org/Signature_requirements_for_ballot_measures_in_California [https://perma.cc/8C4S-DE6K].

[56] Goldman, *supra* note 15, at 357 (noting that Silicon Valley was prepared to spend millions combating Mactaggart's initiative).

[57] Lee Fang, *Google and Facebook Are Quietly Fighting California's Privacy Rights Initiative, Emails Reveal*, INTERCEPT (June 26, 2018, 2:44 PM), https://theintercept.com/2018/06/26/google-and-facebook-are-quietly-fighting-californias-privacy-rights-initiative-emails-reveal [https://perma.cc/S9SE-ANKC].

[58] Confessore, *supra* note 6.

[59] Goldman, *supra* note 15, at 363.

[60] Confessore, *supra* note 6.

governor signed the bill into law on June 28, 2018—just seven days after the bill was introduced.[61] The process did not include ample opportunity for consumer or business input.[62] With the passage of the CCPA, the business community is "now faced with a 'take it, or leave it' scenario which is very problematic given that the business community overall has had little input to these negotiations."[63] This "rushed and non-inclusive process"[64] resulted in a law that is riddled with egregious typos,[65] drafting errors,[66] and flawed policy.[67] The numerous errors make the CCPA extremely confusing and hard to follow.[68] The California legislature passed amendments to the CCPA through September 2019, and the Attorney General did not release the final regulations until June 2020—after the legislature rewrote the bill three times.[69] The CCPA went into effect on January 1, 2020, with many

[61] The original version of the CCPA, AB-375, was introduced to the California Legislature in February 2017 but was ordered to inactive file in September 2017. AB-375 was resurrected from inactive file on June 21, 2018 and eventually became the CCPA on June 28, 2018. *AB-375 History*, CAL. LEG. INFO., https://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml?bill_id=201720180AB375 [https://perma.cc/H22R-FAJY].

[62] Goldman, *supra* note 15, at 363.

[63] S. RULES COMM., 2018 CONG., SENATE FLOOR ANALYSIS OF AB 375, at 9 (Cal. 2018) (arguing against enacting the CCPA due to lack of outside input).

[64] Goldman, *supra* note 15, at 363.

[65] Several sections in the original version of the CCPA are missing necessary commas and incorrectly use "business." *See, e.g.*, CAL. CIV. CODE. 1798.130(a)(7) (West 2020) (amended Sept. 24, 2018) ("Use any personal information collected from the consumer in connection with the business'[sic] verification of the consumer's request solely for the purposes of verification.").

[66] Eric Goldman highlights several provisions of the CCPA that contained drafting errors. Notably, "[Section] 1798.110(c)(5) says that businesses must publish their consumers' 'specific pieces of personal information' in their privacy policies. Oops. Talk about a true lack-of-privacy policy!!! Section 110(c)(5) should be deleted." Eric Goldman, *California Amends the Consumer Privacy Act (CCPA); Fixes About 0.01% of Its Problems*, TECH. & MKTG. L. BLOG (Oct. 4, 2018), https://blog.ericgoldman.org/archives/2018/10/california-amends-the-consumer-privacy-act-ccpa-fixes-about-0-01-of-its-problems.htm [https://perma.cc/652W-QC8D].

[67] *See* Goldman, *supra* note 15, at 365 (arguing that the CCPA will hurt small businesses).

[68] *See* Lothar Determann, *An Open Letter to the California Legislature on Updating the CCPA*, IAPP (Mar. 5, 2019), https://iapp.org/news/a/an-open-letter-to-the-california-legislature-on-updating-the-ccpa [https://perma.cc/QUJ8-A2A7] (urging the California legislature to correct "obvious errors and typos" to ease the burden on businesses attempting to comply with the CCPA).

[69] *See* Deborah A. George, *California Attorney General Releases Modified CCPA Regulations*, NAT'L L. REV. (Feb. 12, 2020), https://www.natlawreview.com/article/california-attorney-general-releases-modified-ccpa-regulations

businesses still wondering how exactly to comply with the cumbersome law.[70] At the time of writing, the final regulations total 11,000 words, which largely ignore comments from the business community and remove business-friendly regulations.[71] Despite the "final" regulations becoming effective in August 2020, the California Attorney General proposed additional modifications in October 2020.[72]

C. A Closer Look at the CCPA

While Mactaggart's original version of the initiative was taken off the ballot, it still managed to lay the foundation for the CCPA.[73] The CCPA's purpose is to provide *comprehensive* data protection to California residents.[74] To achieve this goal, the statute is purposefully wide-ranging and contains definitions that are intentionally vague.[75]

[https://perma.cc/ERQ4-EU3B] (analyzing the set of modified, yet still ill-defined, draft regulations provided by the California Attorney General in February 2020).

[70] As of October 2020, the California Attorney General has released four versions of the CCPA regulations, creating confusion among business owners about their compliance obligations. CAL. CODE REGS. tit. 11, §§ 999.300-.337. (2020) (CCPA proposed text of regulations).

[71] Eric Goldman, *A Review of the "Final" CCPA Regulations from the CA Attorney General*, TECH. & MKTG. L. BLOG (June 29, 2020), https://blog.ericgoldman.org/archives/2020/06/a-review-of-the-final-ccpa-regulations-from-the-ca-attorney-general.html [https://perma.cc/JJ9F-8CK8].

[72] Kirk J. Nahra & Ali A. Jessani, *California AG Proposes Modifications to CCPA Regulations as CPRA Vote Nears*, WILMERHALE BLOG (Oct. 13, 2020) [hereinafter *California AG Proposes Modifications*], https://www.wilmerhale.com/en/insights/blogs/WilmerHale-Privacy-and-Cybersecurity-Law/20201013-california-ag-proposes-modifications-to-ccpa-regulations-as-cpra-vote-nears [https://perma.cc/6RLR-URUL]. Further, on November 3, 2020, California voters approved the California Privacy Rights and Enforcement Act ("CPRA"). Kirk J. Nahra & Ali A. Jessani, *The CPRA Is Voted into Law*, WILMERHALE BLOG (Nov. 4, 2020) [hereinafter *CPRA Is Voted into Law*], https://www.wilmerhale.com/sitecore/content/shared-data/blogs/wilmerhale-privacy-and-cybersecurity-law/2020/11/04/20201104-the-cpra-is-voted-into-law?sc_lang=en [https://perma.cc/4G4R-VWVX]. This new law adds additional obligations to the CCPA and creates the California Privacy Protection Agency, which will be tasked with enforcing the CPRA. *Id.* While the CPRA does not go into effect until January 2023, businesses will, once again, be asked to overhaul their privacy practices. *Id.*

[73] *See supra* Section I.B (explaining the beginnings, drafting, and passage of the CCPA).

[74] *See* Adler, *supra* note 43 (interviewing Mactaggart, who hopes the CCPA will give comprehensive data protections to *all* Americans).

[75] Goldman, *supra* note 15, at 365 (summarizing the various CCPA definitions).

This Section highlights key provisions that raise dormant Commerce Clause concerns.

Since January 1, 2020, California residents[76] have the right to know what personal information businesses subject to the CCPA have collected, sold, and disclosed.[77] California residents must be given the opportunity to opt-out of the sale of their personal information—a broadly defined term[78]—and must be protected from "discrimination" should they choose to exercise these rights.[79] An estimated half a million U.S. companies—primarily small- and medium-sized businesses—fall within the CCPA's grasp.[80] A business is subject to the CCPA if it does any amount of business in California and has more than $25 million in revenue, received or shares personal information for commercial purposes of 50,000 or more consumers, or derives fifty percent or more of its annual revenue from selling consumers' personal information.[81] This broad definition encompasses all kinds of businesses, even ones that exist entirely outside California.[82]

Additionally, the CCPA demonstrates to the forty-nine other states that comprehensive privacy regulation is possible and opens the door

[76] The CCPA protects any consumer, defined as a "natural person who is a California resident." CAL. CIV. CODE § 1798.140(g) (West 2020). The term "resident" is further defined elsewhere as: (1) Any individual in the state for any purpose that is not transitory or temporary; and (2) any individual who is domiciled in the state but is outside the state for a temporary or transitory purpose. CAL. CODE REGS. tit. 18, § 17014 (2020). This further expands the scope of the CCPA because it protects California residents regardless of physical location.

[77] CAL. CIV. CODE § 1798.115(a)(1)–(3).

[78] *Id.* § 1798.140(o)(1). The CCPA defines "personal information" much more broadly to include "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." *Id.*

[79] *Id.* § 1798.125(a)(1). The Act defines discrimination as behavior that includes, but is not limited to: (1) denying goods or services to consumers; (2) charging different prices or rates for goods or services, including through the use of discounts, benefits, or other penalties; (3) providing a different level or quality of goods or services; and (4) suggesting that a consumer will receive a different price or quality of goods or services if the consumer chooses to exercise her rights under the law.

[80] Rita Heimes & Sam Pfeifle, *New California Privacy Law to Affect More than Half a Million US Companies*, IAPP (July 2, 2018), https://iapp.org/news/a/new-california-privacy-law-to-affect-more-than-half-a-million-us-companies [https://perma.cc/JNL6-WM6P].

[81] CAL. CIV. CODE § 1798.140(c)(1).

[82] *See* Heimes & Pfeifle, *supra* note 80 (noting that the CCPA is estimated to apply to more than half a million companies in the U.S. alone that collect data about California consumers).

to fifty competing and conflicting laws.[83] The CCPA is the first of what will likely be many state laws governing the use of data.[84] The California

[83] *See* Mitchell Noordyke, *State Comprehensive-Privacy Law Comparison: Bills Introduced 2018–2020*, IAPP, https://iapp.org/media/pdf/resource_center/State_ Comp_Privacy_Law.pdf [https://perma.cc/U2R3-9HZR] (tracking each state that introduces a comprehensive data privacy bill and the bill's successes).

[84] Several states have already introduced or enacted data privacy legislation. *See* Rachel R. Marmor et al., *"Copycat CCPA" Bills Introduced in States Across Country*, DAVIS WRIGHT TREMAINE LLP (Feb. 8, 2019), https://www.dwt.com/blogs/privacy–security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou [https://perma.cc/L3DA-K4KP] ("Though the California Consumer Privacy Act . . . has been criticized for containing provisions that are inoperable, legislators in other states have embraced both the structure and specific language of that law. Of the nine states, six follow the full model established in the CCPA, and two approach only certain issues addressed by the CCPA. The ninth state is Washington, which is debating a privacy bill modeled after the GDPR . . . . A tenth state, New Jersey has a draft privacy bill that was introduced last July but has not moved out of committee."). *See, e.g.*, S.B. 1108, 2019 Gen. Assemb., Jan. Sess. (Conn. 2019) (enacted) (establishing a task force to review how Connecticut businesses collect and store data and to determine what data practices those businesses should be required to disclose to consumers); S.B. 418, 30th Leg., Reg. Sess. (Haw. 2019) (requiring Hawaii businesses to inform consumers what broad categories of information they collect and what specific information they collect); H.B. 3358, 101st Gen. Assemb., 1st Reg. Sess. (Ill. 2019) (introducing the Data Transparency and Privacy Act, which gives Illinois consumers the right to privacy and a personal property interest in their personal information and creates a consumer right to opt out of the sale of personal information); H.R. 249, 2019 Reg. Sess. (La. 2019) (enacted) (creating a task force to study the effects of the sale of consumer personal information by internet businesses, social media companies, or search engines); S.P. 275, 129th Leg., Reg. Sess. (Me. 2019) (enacted) (prohibiting an internet broadband provider from using, disclosing, selling, or permitting access to customer personal information unless the customer expressly consents to it; providing other exceptions under which a provider may use, disclose, sell, or permit access to customer personal information; and prohibiting a provider from refusing to serve a customer, charging a customer a penalty, or offering a customer a discount for exercising her rights); S.B. 957, 441st Gen. Assemb, (Md. 2020) (creating the Maryland Online Consumer Protection Act, which is very similar to the CCPA but does not have a private right of action); S.B. 1936, 191st Gen. Court of the Commonwealth of Mass. (2019) (providing consumers the opportunity to opt out of third-party data sales); L.B. 746, 106th Leg., 2d Reg. Sess. (Neb. 2020) (creating the Nebraska Consumer Data Privacy Act, which is similar to the CCPA but has no private right of action); S.B. 220, 80th Reg. Sess. (Nev. 2019) (enacted) (departing significantly from the CCPA by only applying to online businesses and requiring a stronger nexus with Nevada in order for a business to fall under the statute); H.B. 1680, 166th Gen. Ct., Reg. Sess. (N.H. 2020) (creating a near copycat CCPA); A. 2188, 219th Leg., 1st Reg. Sess. (N.J. 2020) (requiring "commercial [i]nternet websites and online services to notify customers of collection and disclosure of personally identifiable information and allow[ing] customers to opt out"); S.B. 5642, 242d Legis. Sess. (N.Y. 2019) (creating the New York

legislature's rapid passage of the CCPA also demonstrates that states can enact data privacy legislation quickly.[85] The possibility of a multitude of conflicting laws appearing almost overnight would create problems for the businesses required to comply with them.[86]

Further, the CCPA requires companies to significantly overhaul privacy and data practices shortly after many of these companies were required to change those same practices to comply with the GDPR.[87] For some, compliance with the CCPA means significant costs, some of which are not practical.[88] Even if a business takes steps to avoid doing business in California, the internet has created a world without borders,

Privacy Act, which provides for stronger protection and stricter enforcement than the CCPA); H.B. 1485, 66th Legis. Assemb., Reg. Sess. (N.D. 2019) (enacted) (creating a "legislative management study of consumer personal data disclosures"); H.B. 1049, 2019 Gen. Assemb., Reg. Sess. (Pa. 2019) (creating a similar CCPA-style bill but with substantially less enforcement); H.B. 5930, 2019 Gen. Assemb., Jan. Sess. (R.I. 2019) (creating the Consumer Privacy Protection Act, which is nearly identical to the CCPA); H. 4812, 123d Gen. Assemb., 2d Reg. Sess. (S.C. 2019) (creating the South Carolina Biometric Data Privacy Act); H.B. 4390, 86th Legis. Sess. (Tex. 2019) (enacted) (creating an advisory council to study data privacy laws and mandating that certain businesses disclose security breaches that expose sensitive personal information); H.B. 473, 2020 Reg. Sess. (Va. 2020) (creating the Virginia Privacy Act); S.B. 5376, 66th Leg., Reg. Sess. (Wash. 2019) (creating minimum standards for protecting consumer information); A.B. 870, 104th Leg., Reg. Sess. (Wis. 2020) (creating one of three potential Wisconsin Data Privacy Acts).

[85] *See supra* notes 60–61 and accompanying text (outlining the legislative history of the CCPA).

[86] *See infra* Section II.E (discussing how inconsistent state regulation can amount to a dormant Commerce Clause violation); *see also infra* Section III.D (arguing that the CCPA violates the dormant Commerce Clause because it will lead to multiple conflicting state data privacy laws).

[87] The GDPR and the CCPA are not perfect equivalents, as each requires unique and substantial steps before an organization is considered compliant. ALICE MARINI ET. AL, DATAGUIDANCE AND FUTURE OF PRIVACY FORUM, COMPARING PRIVACY LAWS: GDPR V. CCPA 5 (2019), https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf [https://perma.cc/SP5Z-7KGY]; *see also infra* notes 317–20 and accompanying text (outlining the key differences between the GDPR and the CCPA).

[88] *See* Nicole Lindsey, *New Report Suggests Initial Compliance Costs for CCPA Could Reach $55 Billion*, CPO MAG. (Oct. 15, 2019), https://www.cpomagazine.com/data-protection/new-report-suggests-initial-compliance-costs-for-ccpa-could-reach-55-billion [https://perma.cc/4XZU-LXY4] (projecting compliance costs for businesses with 20–100 employees to be $100,000, for those with 100–500 employees to be $450,000, and for those with 500 employees to be greater than $2 million, aggregating a total of $55 billion "in initial compliance costs").

facilitating unprecedented commercial opportunity.[89] The smallest businesses located entirely outside of California likely processes some data of California residents, and taking steps to avoid the world's fifth largest economy[90] could prove detrimental to certain businesses.[91]

1. *Scope, compliance, and predicted impact*

The CCPA is a unique privacy law that attempts to give Californians legitimate privacy rights in a world where digital anxiety about consumers' lack of control over their personal information runs rampant. However, the CCPA reaches beyond the borders of California and imposes its requirements on businesses that may not have the means to comply. Its rushed passage and vague definitions leave many businesses with open questions about CCPA compliance. This Section explores the CCPA's broad scope, compliance requirements, and remaining ambiguities.

a. *The scope of the CCPA*

Due to its vague and untailored definitions, the CCPA has a broad material scope. Unlike other U.S. privacy laws, the CCPA covers all types of personal data.[92] The CCPA does not give any relevance to the data's origin or intended use.[93] If the information a business collects fits the CCPA's broad definition of "personal information," the law

[89] Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 181 (2018) (commenting on data's ability to circumvent any state's or nation's borders); *see also* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 13–23 (2006) (expounding on the idea that the internet has created a new cyber dimension largely free from government control); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370 (1996) (stating that local governments will fail to regulate the internet because it renders geographical location practically irrelevant).

[90] Kieran Corcoran, *California's Economy Is Now the 5th-Biggest in the World, and Has Overtaken the United Kingdom*, BUS. INSIDER (May 5, 2018, 7:09 AM), https://www.businessinsider.com/california-economy-ranks-5th-in-the-world-beating-the-uk-2018-5 [https://perma.cc/JD9X-AUSL].

[91] *See infra* Section II.F.1 (stating that a statute that has a wide reach may have a "chilling effect" when out-of-state actors take steps to avoid a marketplace).

[92] *See infra* note 96 and accompanying text (noting that the CCPA covers eleven non-exhaustive categories of "personal information").

[93] *See* CAL. CIV. CODE § 1798.140(c)(1)(B) (West 2020) (putting no jurisdictional limits on the data a company must collect to trigger CCPA compliance, instead regulating any business that receives or shares the data of 50,000 consumers annually and does business in California).

protects that information.[94] The CCPA defines "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[95] The CCPA then goes on to define eleven non-exhaustive categories of information that exemplify its definition of "personal information."[96] However, some of these categories mention types of personal information that are unclear or seemingly non-existent.[97] The only categories of data that are explicitly carved out of this definition are (1) information that is publicly available[98] and (2) information that is deidentified or collected as "aggregate consumer information."[99] However, the CCPA provides no guidance as to determining when information is "personal information" as opposed to "deidentified or aggregate consumer information."[100] Further, the CCPA's definition of personal information is substantially different from existing federal and state privacy law, making it more difficult for businesses to identify what information should be protected by the CCPA.[101]

[94] *Id.* § 1798.140(o)(1).

[95] *Id.*

[96] *Id.* § 1798.140(o)(1)(A)–(K).

[97] *See, e.g.*, *id.* § 1798.140(o)(1)(H) (protecting thermal and olfactory information); *see* Kirk J. Nahra (work) (@KirkJNaharawork), TWITTER (Oct. 28, 2019, 1:01 PM), https://twitter.com/KirkJNahrawork/status/1188863438401036290 (highlighting a potential way for olfactory information to manifest through machines learning how to smell).

[98] § 1798.140(o)(2).

[99] *Id.* § 1798.140(o)(3).

[100] Professor Eric Goldman hypothesizes that essentially any data point could be considered personally identifiable information under the CCPA, explaining that "[e]very piece of information about a person is *capable* of being associated with a particular person when combined with enough other data." GOLDMAN, *supra* note 15, at 359. While a person's gender, on its own, does not uniquely identify him or her, combining a person's gender with his or her birthdate and zip code would enable one to uniquely identify eighty-seven percent of the U.S. population. *Id.* The CCPA provides no guidance as to when gender could be classified as deidentified information, and thus the CCPA "likely includes gender information in the 'personal identification' definition because it is 'capable of being associated with a particular consumer when combined with other datasets." *Id.*

[101] *Compare* GDPR art. 4(1) ("'[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person . . . ."), *with* CAL.

The CCPA applies to any for-profit entity that "collects consumers' personal information."[102] Like its definition of "personal information," the CCPA's definition of "business" is broad and encompasses a wide range of businesses with differing abilities to comply.[103] A business that has any activity in California is subject to the CCPA if the business meets one of three statutory thresholds: (1) it has more than $25 million in annual gross revenue, (2) it buys, receives, sells, or shares the personal information of 50,000 or more consumers annually, or (3) it derives fifty percent or more of its annual revenue from selling consumers' personal information.[104] The CCPA only excludes the collection or sale of a "consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California,"[105] meaning that, to be exempt from the law, no part of a data sale can take place in California, and no data collected from California can ever be sold.[106] This only implicates businesses that have minimal connections to California or none at all. A business that swipes an average of 137 credit cards a day or "less than [fourteen] sales per hour over a [ten]-hour business day" would still be subject to the CCPA.[107] This is a low threshold that many local boutiques, coffee shops, and

CIV. CODE § 1798.140(o)(1) (defining "personal information" much more broadly to include "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household"). The key difference between the GDPR and the CCPA is that the GDPR has far fewer categories of personal information and does not mention household information.

[102] § 1798.140(c)(1).

[103] *Id.* (defining a "business" as a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information" and meets specified statutory thresholds); *see What Businesses Outside California Should Know About the California Consumer Privacy Act*, TANNENBAUM HELPERN SYRACUSE & HIRSCHTRITT, LLP (Mar. 20, 2019), https://www.thsh.com/publications/what-businesses-outside-california-should-know-about-the-california-consumer-privacy-act [https://perma.cc/5CJC-K4SM] (providing specific instructions to businesses based outside of California on how to comply with the CCPA).

[104] § 1798.140(c)(1)(A)–(C).

[105] *Id.* § 1798.145(a)(6).

[106] *See* GOLDMAN, *supra* note 15, at 357–58 (noting that a business that accepts any payment from one California resident must comply if it meets the CCPA's threshold).

[107] *Id.* at 358.

mom-and-pop restaurants satisfy.[108] The International Association of Privacy Professionals ("IAPP") estimates that over 500,000 U.S. companies fall within the CCPA's grasp.[109] The extremely broad scope of the CCPA's "business" definition encapsulates the major tech giants with whom the architects of the CCPA were primarily concerned but also captures many smaller businesses that do not have the means to comply.[110]

b. *Compliance and its challenges*

The CCPA establishes significant individual rights for California residents. A majority of these rights create legitimate protections but simultaneously present serious challenges to businesses attempting to provide these complicated rights to their customers.[111] Businesses are facing extraordinary burdens in their attempts to operationalize the CCPA's consumer rights and opt-out requirements.[112] The following are new rights created under the CCPA, each of which poses unique difficulties for businesses.[113]

[108] *Id.* (noting that the CCPA applies to any ad-supported website that receives 50,000 hits from unique IP addresses).

[109] Heimes & Pfeifle, *supra*, note 80.

[110] *See* Eric Goldman, *The California Consumer Privacy Act Should Be Condemned, Not Celebrated (Cross-Post)*, TECH. & MKTG. L. BLOG (Aug. 9, 2018), https://blog.ericgoldman.org/archives/2018/08/the-california-consumer-privacy-act-should-be-condemned-not-celebrated-cross-post.html [https://perma.cc/AB8Q-ASD6] (stating that, due to the CCPA, the blog's author would likely have to turn off any ad software because of his inability to comply with the CCPA).

[111] Kirk J. Nahra, *The Next Major Privacy Challenge for Corporate America—California's New Privacy Law*, PRIVACY L. WATCH (July 5, 2018), https://www.wileyrein.com/media/publication/481_Nahra%20Insight%20-%20PLW.pdf [https://perma.cc/KS8W-AUTR].

[112] Lindsey O'Donnell, *California's Tough New Privacy Law and Its Biggest Challenges*, THREATPOST (Jan. 9, 2020), https://threatpost.com/californias-tough-new-privacy-law-and-its-biggest-challenges/151682 (interviewing Terry Ray, senior vice president of the cyber security company Imperva, about the CCPA compliance costs facing businesses).

[113] The relevant consumer is any "natural person who is a California resident." CAL. CIV. CODE § 1798.140(g) (West 2020). "The term 'resident,' as defined in the law, includes (1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose. All other individuals are nonresidents." CAL. CODE REGS. tit. 18, § 17014 (2020). Consumers domiciled in California but who may be traveling or may have a partial residence in another state are thus protected by the law. There are roughly forty million residents in California, meaning that the CCPA covers a significant portion of the U.S. population. *See* Corcoran, *supra* note 90.

i. *The right to know & the right to access*

A major contributing factor to global digital privacy anxiety is the average consumer's lack of knowledge on how much and what kinds of data businesses collect.[114] Prior to the CCPA, businesses could generally provide information to consumers about what categories of data they collect about consumers. Businesses typically do this in a privacy policy or a terms and conditions agreement.[115] However, these policies are frequently written in complicated language and rarely read by consumers.[116] The CCPA creates several key rights for consumers that center around the right to know about a business's data collection practices and the right to access that information.

The CCPA mandates that businesses disclose their general data policies and practices to consumers and requires that businesses provide ongoing insight to consumers regarding data collected about generic consumers.[117] At or before collection, the law requires a business to notify consumers of the business's "generic collection practices," which inform the potential customer about what categories and specific pieces of information the business collects.[118] A consumer can also request a business's generic collection practices at *any* point following collection.[119]

The CCPA goes beyond generic data practices and extends "the right to know" to the consumer's own personal information.[120] The CCPA enables consumers to request a business which collects that consumer's personal information disclose: (1) the categories of information collected about that consumer, (2) the source from which the consumer's personal information is collected, (3) the businesses or commercial purpose for collecting or selling the consumer's personal information, (4) the categories of third parties with whom the business shares the consumer's

[114] *See* Auxier, *supra* note 4 (finding that "[seventy-eight percent] of U.S. adults say they understand very little or nothing about what the government does with the data it collects," and [fifty-nine percent] say the same about the data companies collect").

[115] *Id.* ("Core parts of the current system of data collection and privacy protection are built on the idea that consumers are given notice about how firms collect and use data . . . .").

[116] *Id.* (noting that the majority of Americans do not read privacy policies before agreeing to them).

[117] CAL. CIV. CODE §§ 1798.115, 1798.140(d).

[118] *Id.* §§ 1798.100(b), 1798.130(a)(5).

[119] *Id.* § 1798.110(a).

[120] *See Nahra*, *supra* note 111, at 4 (explaining how the CCPA will require many businesses to drastically change their data collection strategies).

personal information, and (5) all specific pieces of the consumer's personal information it has collected.[121] Prior to the CCPA, some companies may have allowed for consumers to request some of their personal information; however, the CCPA requires companies to provide consumers with unprecedented access to their personal information.[122]

A general "right to know" what information a business collects and "right to access" that information pose an extreme challenge to businesses.[123] Many businesses do not currently have the infrastructure to handle these types of data requests because these businesses do not understand how much data they possess.[124] One study estimates that fifty-four percent of businesses do not know where all of their sensitive data is stored, and sixty-five percent of businesses do not have the ability to analyze and process all the data they collect.[125] Within one company, expansive "data sprawl" makes it difficult for a company to know exactly how much data it has on one individual.[126] For example, if a company ran a month-long promotion collecting emails, that information may have been placed in a database that was used for a short period of time and then quickly forgotten.[127]

Further, most businesses do not collect and process data through standardized methods.[128] The data is organized into multiple databases that were developed in silos.[129] Many data-processing systems were designed and developed thirty to forty years ago with dated technology that was not designed with consumer privacy in mind.[130] Among those

[121] § 1798.110(a)(1)–(5).

[122] *See* Kashmir Hill, *I Got Access to My Secret Consumer Score. Now You Can Get Yours, Too.*, N.Y. TIMES (Nov. 4, 2019), https://www.nytimes.com/2019/11/04/business/secret-consumer-score-access.html (reporting difficulties in requesting personal information collected by various businesses).

[123] *See* O'Donnell, *supra* note 112 (discussing provisions of the CCPA that present the most difficult compliance challenges for businesses).

[124] *See* Sead Fadilpašić, *Businesses Are Collecting More Data than They Can Handle—even After GDPR*, ITPROPORTAL (July 10, 2018), https://www.itproportal.com/news/businesses-are-collecting-more-data-than-they-can-handle-even-after-gdpr [https://perma.cc/UB5V-UZHP] (noting that roughly two thirds of businesses struggle to comply with existing data regulations that came before the CCPA).

[125] *Id.*

[126] O'Donnell, *supra* note 112.

[127] *Id.*

[128] *Id.* (noting that data is generally collected within one business by different actors).

[129] *Id.*

[130] *See* Toby Lester, *The Reinvention of Privacy*, ATLANTIC (Mar. 2001), https://www.theatlantic.com/magazine/archive/2001/03/the-reinvention-of-

databases, the metadata that describes the customer's personal information may differ across systems.[131] Without sophisticated supplemental technology, businesses may struggle to determine whether John H. Smith, John Harry Smith, or J. Smith are different customers. While some companies are beginning to implement data-mapping strategies to combat these problems, this solution is expensive and labor intensive.[132] Larger businesses will eventually develop the necessary infrastructure to process and respond to consumer requests, but small- and medium-sized businesses likely will not, forcing them to make tough decisions about avoiding the California marketplace altogether.[133]

Another challenge facing businesses is the CCPA requirement for a covered business to provide a consumer with requested information in response to a "verified consumer request."[134] The CCPA provides that the Attorney General is tasked with developing additional rules consistent with the CCPA.[135] In June of 2020, the Attorney General released his "final" draft of the CCPA regulations.[136] The regulations provide vague guidance.[137] The regulations treat the verification of a consumer requests as a fact-specific scenario. The regulations call for

privacy/302140 (stating that the founders of the internet focused on creating a broadly accessible system and not on privacy and security).

[131] Donal Tobin, *What is Data Mapping?*, XPLENTY (June 22, 2020), https://www.xplenty.com/blog/data-mapping-an-overview-of-data-mapping-and-its-technology [https://perma.cc/Q4BB-8VL6] (demonstrating how three different databases each storing information on popular actors and movies would have different organizational strategies).

[132] *Id.* (noting that businesses can incorporate manual data mapping or purchase various types of automated data-mapping software).

[133] *See infra* Section II.F.1 (explaining that a statute that has a wide reach may have an impermissible "chilling effect," causing out-of-state actors to avoid a marketplace whether or not they actually fall under the statute's reach).

[134] Peter McLaughlin & Annie Bai, *Why the CCPA's 'Verified Consumer Request' Is a Business Risk*, IAPP (Aug. 14, 2019), https://iapp.org/news/a/verified-consumer-request-dont-naively-slip-into-the-crack-or-is-it-a-chasm [https://perma.cc/7FP9-Z8GQ]; *see also* JAMES PAVUR & CASEY KNERR, GDPARRRRR: USING PRIVACY LAWS TO STEAL IDENTITIES 2, 5 (2019), https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf [https://perma.cc/T74L-PUBR] (discussing the inherent risks associated with the GDPR's "right of access" and how businesses often fail to take necessary steps to verify consumer identities).

[135] CAL. CIV. CODE § 1798.185(a) (West 2020).

[136] CAL. CODE REGS., tit. 11, §§ 999.323-.326 (2020).

[137] *Id.* § 999.323(a), (c) (mandating that businesses use "reasonable" security measures but shall avoid asking for any additional personal information (like a driver's license) to verify a consumer's identity).

businesses to consider six factors when verifying consumer requests: (1) the type of information requested; (2) the risk of harm to the consumer; (3) the likelihood a nefarious actor would seek out the data; (4) whether the business can actually verify the consumer's identity based on the information the business has; (5) how the business interacts with the consumer; and (6) the available technology for verifying the consumer's identity.[138] This test transforms verifying consumer requests into a case-by-case-process—minimizing the consumer right while maximizing the onus on businesses.

The majority of businesses struggle to comply with existing privacy laws.[139] If a business responds to a "consumer request" filed by a bad faith actor, that business, in its attempt to comply with the CCPA, provides a neatly-packaged data portfolio for which there may be detrimental consequences.[140] Particularly for smaller businesses, poor guidance on verifying consumer requests could provide nefarious actors with easy access to sensitive personal information.[141] Verifying data requests is difficult and, if done improperly, could compromise the personal information of the very individuals the CCPA seeks to protect.[142]

Operationalizing "the right to know" and "the right to access" is a burdensome task for any business. Businesses must develop new policies, create new database architecture, and implement new data management practices.[143] For small- and medium-sized businesses, these rights will require both a heavy administrative lift and large costs that may severely impact these businesses' bottom line.[144] The CCPA's "right to know" and "right to access" may provide consumers with a

[138] *Id.* § 999.323(b)(3)(a)–(f).

[139] *See* Fadilpašić, *supra* note 124 (finding that sixty-eight percent of businesses struggle to comply with existing privacy law).

[140] *See* McLaughlin & Bai, *supra* note 134 (arguing that companies are likely to implement "low-tech solutions" to verify consumer identities).

[141] *Id.*

[142] *Id.*

[143] Dan Goldstein, *Where to Begin to Operationalize CCPA Compliance*, IAPP (Jan. 29, 2019), https://iapp.org/news/a/where-to-begin-to-operationalize-ccpa-compliance [https://perma.cc/9W8L-YVX2] (providing general guidance to some businesses on developing a CCPA compliance plan).

[144] *See* Lindsey, *supra* note 88 (noting that companies with fewer than twenty employees will pay around $50,000 and that companies with more than 500 employees will pay more than $2 million in initial CCPA compliance costs).

little more control over their data but will harm smaller businesses in the process.

ii. The erasure right

The CCPA provides that "[a] consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer."[145] This right to be deleted is reminiscent of the GDPR's "right to be forgotten."[146] The "right to be deleted" proves to be one of the most difficult challenges facing businesses preparing to comply with the CCPA.[147]

Businesses cannot delete all of a consumer's information because they may not know where that information is located.[148] Many businesses do not have a complete understanding of the location of all of their collected data.[149] For the same reasons that businesses fail to aggregate a single consumer's information, businesses will struggle to track down all the information to fully comply with a "verified consumer's" deletion request.[150] The final draft of the California Attorney General's regulations states that "a business may present the consumer with the choice to delete select portions of their personal information only if a global option to delete all personal information is also offered and more prominently presented than the other choices."[151] Providing customers with a "global option" is an impossible task if a business is not equipped to map and process all of its collected data.

Deleting a consumer's data prematurely can have significant consequences affecting a company's ability to provide its goods and/or services. The CCPA exempts deletion requests for data necessary to complete transactions, uphold legal obligations, maintain security and functionality, protect First Amendment rights, conduct research, and

[145] CAL. CIV. CODE § 1798.105(a) (West 2020).

[146] *See* GDPR art. 17 ("The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay . . . .").

[147] O'Donnell, *supra* note 112.

[148] *Id.*

[149] *See* Fadilpašić, *supra* note 124 (reporting that sixty-five percent of companies are not able to fully analyze the data they collect).

[150] *See supra* Section I.C.1.b.i (noting that businesses struggle to understand how much data they collect).

[151] CAL. CODE REGS. tit. 11, § 999.313(d)(8) (2020).

for internal, normal, and lawful uses.[152] However, businesses are required to examine the nuances of each exemption to the "erasure right" to determine if one is applicable at the time of a consumer request.[153] Businesses will face immense administrative burdens when attempting to process these deletion requests and when determining if a relevant exception applies.[154] In some cases, it may be impossible to anticipate at the time of the request if a relevant exception is applicable—potentially rendering this right useless.[155] For example, in both ongoing and anticipated civil litigation, it is common for businesses to provide their attorneys with huge amounts of information that likely falls within the scope of the CCPA. The CCPA would require businesses to "maintain an inventory of what consumer information is collected and produced in civil litigation" to be deleted when (and if) the litigation ends.[156]

[152] CAL. CIV. CODE § 1798.105(d)(1)–(9) (West 2020).

[153] *See CCPA Deletion Exemptions*, SIXFIFTY, https://www.sixfifty.com/ccpa-exemptions [https://perma.cc/MB7G-5B8E] (providing guidance to potential clients about the breadth of exceptions to the CCPA deletion requirement).

[154] *Compare* CAL. CIV. CODE § 1798.105(a) (stating that "[a] consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer," with several exceptions), *with* GDPR art. 17 ("The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay . . . ."). Many privacy professionals compare the CCPA to the GDPR largely because of the CCPA's broad scope and the so called "erasure right." *See, e.g.*, David Kessler & Anna Rudawski, *CCPA Extends "Right to Deletion" to California Residents*, DATA PROTECTION REP. (Sept. 27, 2018), https://www.dataprotectionreport.com/2018/09/ccpa-extends-right-to-deletion-to-california-residents [https://perma.cc/QY5W-ZY6P]. However, the CCPA's "right to be deleted" is much narrower than the GDPR's erasure right given the GDPR's lack of exceptions. Further, the GDPR's erasure right has raised serious questions about global free speech. *See* Adam Satariano & Emma Bubola, *One Brother Stabbed the Other. The Journalist Who Wrote About It Paid a Price*, N.Y. TIMES (Sept. 23, 2019), https://www.nytimes.com/2019/09/23/technology/right-to-be-forgotten-law-europe.html.

[155] *See, e.g.*, Allison Douglis & David Saunders, *How the CCPA Impacts Civil Litigation*, IAPP (Jan. 28, 2020), https://iapp.org/news/a/how-the-ccpa-impacts-civil-litigation [https://perma.cc/D3SJ-BXN9] (noting the difficulties with implementing the erasure right in the context of civil litigation).

[156] *Id.*

Finally, proving that businesses have deleted customers' requested data is one of the biggest ambiguities concerning CCPA enforcement.[157] The act of deleting data is costly and may be difficult—if not impossible—to prove.[158] Fully deleting data is a complicated, multi-step process.[159] The Attorney General's final regulations require that businesses "inform the consumer whether or not it has complied with the consumer's request."[160] However, this puts businesses in the tough situation of confirming consumer's deletion requests without having the means to prove that the data was actually deleted.

iii. The right to "opt-out" of data sales

The CCPA mandates that "[a] consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information."[161] This provision of the CCPA empowers the consumer to control a business's ability to sell that consumer's data.[162] This opt-out provision applies to a wide variety of transactions because the CCPA defines "sale" very broadly[163] to include any data exchange from one business to another "for monetary or other *valuable consideration*."[164] After a consumer asserts her right to opt out of data sales, a business cannot request the consumer to allow the business to sell her data again for a minimum of twelve months.[165]

The right to opt out of data sales is an easier provision to implement than the "right to know," "the right to access," or the "erasure right."[166]

[157] *See* O'Donnell, *supra* note 112 (hypothesizing that the severity of CCPA enforcement will likely depend on the thoroughness of the auditor).

[158] *Id.*

[159] *See* Mimi Onuoha, *What It Takes to Truly Delete Data*, FIVETHIRTYEIGHT (Jan. 30, 2017, 6:44 AM), https://fivethirtyeight.com/features/what-it-takes-to-truly-delete-data [https://perma.cc/AZY3-WBF2] (stating that data cannot be truly "deleted" and that to destroy data one must either destroy the physical technology where the data is stored or overwrite the data to ensure it cannot be recovered).

[160] CAL. CODE REGS. tit. 11, § 999.313(d)(4) (2020).

[161] CAL. CIV. CODE § 1798.120(a) (West 2020).

[162] *Id.*

[163] A business does not need to personally "sell" data to be subject to this provision. If a business uses certain standard advertising tools that require personal information (e.g., Google Ads and Google Analytics), this falls within the definition of a "sale." *See* § 1798.140(t)(1).

[164] *Id.* (emphasis added).

[165] § 1798.135(a)(5).

[166] O'Donnell, *supra* note 112.

Generally, when businesses are sharing data with third parties, there is a paper trail.[167] Businesses who explicitly sell data will be able to pinpoint exactly what data is actively being shared and enable consumers to "opt-out."[168] While businesses may have an easier time identifying the data they share or sell to third parties, there are still considerable challenges associated with providing this right to consumers. Businesses will need to develop strategies to record and track these requests, which is an enormous administrative burden on small- to medium-sized businesses that rely on consumer data sales to provide free services.[169]

iv. Anti-discrimination provisions

The CCPA bars any businesses from discriminating against a consumer who chooses to exercise her CCPA rights.[170] However, the CCPA does provide for an exception to incentivize consumers to allow businesses to sell their data:

> A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's data.[171]

The classic example is a business providing coupons to consumers who provide their email at check out. The business is able to sell the consumer's data and in return the company rewards the consumer with coupons.

v. Minimal private right of action that only exists where there is a data breach

The CCPA provides that:

> Any consumer whose nonencrypted or nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and

[167] *Id.*

[168] *Id.*

[169] *See* Stephen J. Bronner, *Of Course 'Free' Services Sell Your Data*, ENTREPRENEUR (Apr. 25, 2017), https://www.entrepreneur.com/article/293360 [https://perma.cc/5HUL-5ADE] (reporting that consumer data is a form of currency: consumers allow free services to sell their data in exchange for access to a "free" service).

[170] § 1798.125(a)(1)(A)–(D).

[171] § 1798.125(b)(1).

> practices appropriate to the nature of the information to protect the personal information may institute a civil action . . . .[172]

In the event of a data breach, a consumer may recover anywhere from $100–$750 in statutory damages or actual damages, whichever is greater, "per consumer per incident."[173]

This is a significant shift from other data breach laws that require the Attorney General to bring an enforcement action against businesses that failed to maintain reasonable security procedures.[174] However, the CCPA does require that consumers give businesses a thirty-day opportunity to "cure" that breach before bringing a civil action against that business.[175] In any other circumstance not involving a data breach, the California Attorney General has the exclusive right of action and only after providing the delinquent business with a thirty-day cure period when consumers suffer no actual pecuniary damages.[176] This minimal private right of action lacks the "teeth" that the California legislature promised Mactaggart.[177] Mactaggart and his fellow sponsors of the CCPA were unsatisfied by the final amended product, and the team has launched a new initiative called the California Privacy Rights and Enforcement Act of 2020.[178]

The CCPA went into effect on January 1, 2020; however, the final impact of the law remains unclear.[179] California lawmakers passed the

[172] § 1798.150(a)(1).

[173] § 1798.150(a)(1)(A).

[174] *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 748–50 (2016).

[175] § 1798.150(b). Eric Goldman, in his chapter summarizing the CCPA, notes that the Act does not define how a business can cure data theft, which presents a confusing roadblock to consumers hoping to receive damages. Goldman, *supra* note 15, at 362.

[176] § 1798.155(b).

[177] Angelique Carson, *On Keynote Stage, Mactaggart Addresses His 'New' CCPA*, IAPP (Sept. 26, 2019), https://iapp.org/news/a/on-keynote-stage-mactaggart-addresses-his-new-ccpa [https://perma.cc/EZ4D-PGV2].

[178] Malia K. Rogers, *Insight: CCPA Ink Still Wet While Signatures Being Collected for 'CCPA 2.0' Ballot Initiative*, BLOOMBERG L. (Feb. 13, 2020, 4:01 AM), https://news.bloomberglaw.com/privacy-and-data-security/insight-ccpa-ink-still-wet-while-signatures-being-collected-for-ccpa-2-0-ballot-initiative [https://perma.cc/T6Y6-3299]. On November 3, 2020, the ballot initiative passed. Voters approved the expansion of the CCPA by creating the California Privacy Protection Agency tasked with enforcing the CCPA. *CPRA Is Voted into Law*, *supra* note 72.

[179] The Attorney General will begin to bring enforcement action in July 2020. Only then will the CCPA's full impact become clear. *See* Nahra, *supra* note 111

CCPA in 2018, California lawmakers were passing amendments through late 2019. The California Attorney General, tasked with clarifying ambiguous portions of the law, issued his "final" regulations, which went into effect in August 2020.[180] Nevertheless on October 14, 2020, the AG released yet another draft of regulations currently pending Office of Administrative Law approval. The CCPA is in effect, yet businesses must follow new versions of regulations that come out every few months.

II. THE DORMANT COMMERCE CLAUSE

The dormant Commerce Clause circumscribes the boundaries of the CCPA's broad material scope. The Commerce Clause is a constitutional provision that explicitly grants Congress the power to regulate commerce among the states.[181] Article I, Section 8 affirmatively grants Congress the power to regulate interstate commerce.[182] Although the Constitution does not explicitly prohibit the states from regulating interstate commerce,[183] the Supreme Court has inferred this doctrine from Congress's affirmative power to regulate commerce amongst the states.[184] While the states are not wholly prohibited from regulating interstate commerce, if a regulation furthers protectionist policies, thus unduly burdening the flow of commerce amongst the states, that law will be struck down as unconstitutional.[185] The following Sections explore dormant Commerce Clause jurisprudence and break down the four traditional categories of dormant Commerce Clause violations.

A. *Defining Commerce:* Gibbons v. Ogden

Since 1824, when the Supreme Court decided *Gibbons v. Ogden*,[186] it has consistently read the Commerce Clause to mean that the states

(expressing that businesses need to work quickly to implement the policies in the CCPA).

[180] *See California AG Proposes Modifications*, *supra* note 72.

[181] U.S. CONST. art. I, § 8, cl. 3.

[182] *Id.*

[183] *See id.* (addressing only Congress's ability to regulate interstate commerce).

[184] Donald H. Regan, *The Supreme Court and State Protectionism: Making Sense of the Dormant Commerce Clause*, 84 MICH. L. REV. 1091, 1184 (1986).

[185] *See* Pike v. Bruce Church, Inc., 397 U.S. 137, 145 (1970) (holding that an Arizona law, although furthering a legitimate state interest, was nevertheless unconstitutional because of its excessive burden on interstate commerce).

[186] 22 U.S. (9 Wheat.) 1 (1824).

cannot regulate interstate commerce.[187] In *Gibbons*, New York gave Ogden an exclusive license to operate steamboats within New York-controlled waters.[188] The federal government extended Gibbons a similar license that allowed him to compete with Ogden directly, defeating the purpose of Ogden's monopoly.[189] Ogden filed suit to protect his exclusive right to navigate his steamboats within New York waters.[190] The Court held that while states have the right to regulate commercial activity that occurs wholly within the state, only Congress can regulate commercial activity that occurs amongst the states.[191] The Court defined commerce to include traffic, intercourse, navigation, and commodities associated with interstate commerce.[192] This broad interpretation of commerce gave Congress enormous power, but it also significantly restricted the states' regulatory ability.

B. *Discriminatory Impact*

Since its emergence in 1824, the dormant Commerce Clause has experienced different periods of favoritism.[193] The judge-made doctrine has four traditional categories: (1) discriminatory regulation, (2) unduly burdensome regulation, (3) regulation of conduct that is wholly extraterritorial, and (4) regulation that leads to a patchwork of conflicting laws amongst the states.[194] The dormant Commerce Clause's primary prohibition is against protectionist behavior.[195] Prior to 1969, the only form of dormant Commerce Clause violations were statutes that

[187] *Id.* at 9.

[188] *Id.* at 2.

[189] *Id.*

[190] *Id.*

[191] *Id.* at 4.

[192] *Id.* at 134.

[193] *See* Regan, *supra* note 184, at 1182–84 (discussing the early history of the dormant Commerce Clause as solely involving actions against discriminatory statutes); *see also* Brannon P. Denning, *Extraterritoriality and the Dormant Commerce Clause: A Doctrinal Post-Mortem*, 73 LA. L. REV. 979, 979 (2013) (commenting on the decline of the Court's reliance on the extraterritoriality principle of the dormant Commerce Clause).

[194] *See* Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785, 787–89 (2001) (arguing against the notion that all attempts at regulating the internet violate the dormant Commerce Clause).

[195] *See* U.S. CONST. art. I, § 8, cl. 3 (stating that Congress has the power to regulate commerce among the several states).

enabled a state to discriminate against out-of-state actors.[196] This type of protectionist behavior impedes the flow of commerce and directly infringes on Congress's explicit power to "regulate commerce . . . amongst the States."[197] Further, economists theorize that when states take measures to protect their businesses from competition by restricting imports and exports, "overall economic welfare declines as the losses to in-state consumers and out-of-state producers exceed the gains to the protected in-state producers."[198] Protectionist regulation promotes an unhealthy economy and runs afoul of the dormant Commerce Clause. Therefore, a court will essentially deem per se invalid any state regulation it finds to be clearly protectionist and discriminatory towards out-of-state actors.[199]

The Supreme Court has also found that facially-neutral laws that have a discriminatory impact against out-of-state actors are unconstitutional.[200] Regardless of whether the intent behind the challenged law was to discriminate against out-of-state actors, "[a] court may find that a state law constitutes 'economic protectionism' on proof either of discriminatory effect or of discriminatory purpose."[201] This interpretation prevents states from drafting laws that facially appear to have a legitimate purpose but ultimately result in policies that are harmful to the flow of interstate commerce.

[196] Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970) (creating a balancing test for evaluating whether a state law violates the dormant Commerce Clause).

[197] *Gibbons*, 22 U.S. (9 Wheat.) at 207; Goldsmith & Sykes, *supra* note 194, at 792–93.

[198] Goldsmith & Sykes, *supra* note 194, at 797.

[199] *See, e.g.*, City of Philadelphia v. New Jersey, 437 U.S. 617, 626–27 (1978) (finding a New Jersey statute that prohibited the importation of waste that originated outside New Jersey was facially discriminatory and unconstitutional); H.P. Hood & Sons, Inc. v. Du Mond, 336 U.S. 525, 535 (1949) (condemning any "economic restraints on interstate commerce" that create a local economic advantage).

[200] *See* Hunt v. Wash. State Apple Advert. Comm'n, 432 U.S. 333, 352–54 (1977) (holding a Georgia statute that prohibited the use of a non-"USDA grade" certification on apples was facially neutral but had a discriminatory impact and therefore violated the dormant Commerce Clause). *But see* Exxon Corp. v. Governor of Md., 437 U.S. 117, 125 (1978) (finding that a Maryland statute that prohibited petroleum producers or refiners from operating a retail store within the state did not have a discriminatory impact).

[201] Minnesota v. Clover Leaf Creamery Co., 449 U.S. 456, 471 n.15 (1981) (citation omitted).

C. *The* Pike *Balancing Test*

When a state law is not discriminatory—either in its intent or in its impact—the law can still fail under the dormant Commerce Clause if it imposes an excessive burden on interstate commerce that is not outweighed by the putative benefits.[202] This inquiry is a fact-intensive analysis that turns on how a court measures the burdens imposed on interstate commerce compared with the benefits bestowed on the state's residents.[203] The balancing test emerged in *Pike v. Bruce Church, Inc.*[204] where the Supreme Court evaluated an Arizona statute[205] that required all cantaloupes grown in Arizona for the purpose of sale to "be packed in regular compact arrangement in closed standard containers approved by the supervisor."[206] Bruce Church shipped its unpackaged cantaloupes from its ranch in Parker, Arizona to its processing plant thirty-one miles away in Blythe, California.[207] The Arizona supervisor tasked with enforcing the law commenced an action against Bruce Church, alleging failure to properly package the cantaloupes before shipping them out of state.[208] Bruce Church rebutted by claiming that the Arizona law amounted to "an unlawful burden upon interstate commerce."[209] Despite the Arizona statute being non-discriminatory, the Court held that "[w]here the statute regulates evenhandedly to effectuate a legitimate local public interest,

[202] Pike v. Bruch Church, Inc., 397 U.S. 137, 142 (1970); *see also* Kassel v. Consol. Freightways Corp., 450 U.S. 662, 675–76 (1981) (holding that certain forms of transportation require uniform regulations, and, if left to the states, citizens would be subject to a patchwork of confusing regulations); Bibb v. Navajo Freight Lines, Inc., 359 U.S. 520, 529 (1959) (finding a state regulation that prescribed specific mud flap requirements on trucks that deviated from the norm to be unconstitutional).

[203] *See* Kosseff, *supra* note 15, at 202 (noting that it is difficult to predict whether a state law will fail the *Pike* balancing test due to the significant weight that courts afford to each case's particular facts).

[204] 397 U.S. 137 (1970).

[205] ARIZ. REV. STAT. ANN. § 3-503(C) (repealed 1992).

[206] *Pike*, 397 U.S. at 138.

[207] *Id.* at 139.

[208] *Id.*

[209] *See id.* at 140 (noting that to comply with the Arizona law, Bruce Church would be required to rebuild its packing plant near its ranch in Arizona, which would cost an estimated $200,000—roughly $1.4 million today, accounting for inflation—and take many months before construction would be complete, costing $700,000 in revenue—roughly $5 million today). US INFLATION CALCULATOR, http://usinflationcalculator.com [https://perma.cc/RFT4-KTVD] (enter "1969" in "If in" field, "$200,000" in "I purchased an item for $" field, and "2020" in "then in" field); *id.* (enter "1969" in "If in" field, "$700,000" in "I purchased an item for $" field, and "2020" in "then in" field).

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."[210] This landmark decision gave rise to a new form of dormant Commerce Clause violation: an unduly burdensome regulation.[211]

D. Extraterritoriality

When state legislation regulates conduct that occurs outside the state, a court may strike down the law as a violation of the dormant Commerce Clause.[212] In *Edgar v. MITE Corp.*,[213] the Court struck down the Illinois Business Takeover Act as unconstitutional.[214] The Act required a tender offeror to notify the Illinois Secretary of State and the offeree twenty days before the tender offeror's offer became effective.[215] The Court held that the challenged Act violated the dormant Commerce Clause on two grounds: (1) by regulating extraterritorially and (2) by excessively burdening interstate commerce when compared with the "local interests the Act purport[ed] to further."[216] The Illinois Act directly regulated interstate transactions by requiring out-of-state offerors to apprise the Secretary of State of any tendered offers.[217] The Court hypothesized that a transaction could take place where no Illinois resident would be affected, yet the parties to the transaction would be required to comply with the Illinois Act.[218]

[210] *Pike*, 397 U.S. at 142 (creating the *Pike* test) (emphasis added).

[211] Conservative justices typically find that the *Pike* test is entirely too subjective. Justices Scalia and Thomas go one step further and question whether the "dormant Commerce Clause should apply in the absence of state discrimination against out-of-staters." ERWIN CHEMERINSKY, CONSTITUTIONAL LAW 475 (6th ed. 2020).

[212] *See* Goldsmith & Sykes, *supra* note 194, at 785, 789 (discussing the dormant Commerce Clause's unclear role in state regulation of the internet).

[213] 457 U.S. 624 (1982). '

[214] *Id.* at 643 (White, J., concurring). Although the extraterritoriality provisions of the *Edgar* opinion are a concurrence, the Court later affirmed them. *See* Healy v. Beer Inst., 491 U.S. 324, 336 (1989).

[215] *Edgar* at 626–27 (majority opinion).

[216] *Id.* at 640 (White, J., concurring).

[217] *Id.* at 640–41.

[218] *Id.* at 642 ("[T]he Illinois law on its face would apply even if not a single one of Chicago Rivet's shareholders were a resident of Illinois, since the Act applies to every tender offer for a corporation meeting two of the following conditions: the corporation has its principal executive office in Illinois, is organized under Illinois laws, or has at least 10% of its stated capital and paid-in surplus represented in Illinois.").

The dormant Commerce Clause precludes any "application of a state statute to commerce that takes place wholly outside of the State's borders, whether or not the commerce has effects within the State."[219] Therefore, the Court found that Illinois exceeded the limits of its authority and impermissibly—though indirectly—"assert[ed] extraterritorial jurisdiction over persons or property."[220] In evaluating whether a state exceeds the scope of its jurisdiction, courts must invalidate any law with a "sweeping extraterritorial effect" that may amount to one state projecting its regulatory interests onto another state, despite any local benefits.[221]

Further addressing the extraterritoriality doctrine, in *Healy v. Beer Institute*,[222] a Connecticut statute required beer suppliers to assert that they did not charge Connecticut wholesalers higher prices than wholesalers in other states.[223] The Supreme Court held that this law was unconstitutional, as it violated the extraterritoriality test of the dormant Commerce Clause.[224] Writing for the majority, Justice Blackmun stated that any state law that amounted to "directly control[ling] commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature."[225] By requiring wholesalers to certify that they were charging Connecticut customers no more than non-Connecticut customers, the statute impermissibly regulated the price of beer in neighboring states.[226]

When conducting an extraterritoriality analysis, courts must weigh several different factors.[227] A court should consider the overall impact of the law, the consequences that law has on interstate commerce, and how the law coexists with the other states' regulatory schemes.[228] Further, a court's analysis must also explore the potential effects on

[219] *Id.* at 642–43.
[220] *Id.* at 643.
[221] *Id.* at 642 (finding that the Illinois Business Take-Over Act unconstitutionally regulated transactions that took place "across state lines").
[222] 491 U.S. 324 (1989).
[223] *Id.* at 326.
[224] *Id.* at 343.
[225] *Id.* at 336.
[226] *Id.*
[227] *Id.* at 336–37.
[228] *Id.* at 336.

interstate commerce should one, many, or all the states adopt similar (or conflicting) legislation.[229]

Courts have applied this extraterritoriality analysis in cases primarily related to price-affirmation and price-fixing. For example, in *Brown-Forman Distillers Corp. v. New York State Liquor Authority*,[230] the Supreme Court struck down a New York law that regulated the price that liquor producers charged wholesalers in New York regardless of the location of the liquor producer.[231] The Court acknowledged that, while the New York law regulated "evenhandedly" and New York had a legitimate interest in "assur[ing] the lowest possible prices for its residents,"[232] the regulation amounted to New York "'project[ing] its legislation into [other States] by regulating the price to be paid' for liquor in those States."[233]

However, the dormant Commerce Clause's extraterritoriality doctrine is amorphous and vague.[234] It is considered to be "unsettled[,] poorly understood," and inconsistently applied.[235] Over time, courts have limited the scope of the extraterritoriality prong of the dormant Commerce Clause.[236] In *Pharmaceutical Research & Manufacturers v. Walsh*,[237] the Supreme Court declined to extend its reasoning in *Healy* to strike down a Maine law that required drug manufacturers to participate in a rebate program for low-income patients or else be subject to "prior authorization" procedures.[238] The petitioner claimed the Maine rebate program amounted to extraterritorial regulation of

[229] *Id.*; *see also* Edgar v. MITE Corp., 457 U.S. 624, 642 (1982) (finding that if other states adopted similar legislation, it would restrain the amount of interstate securities transactions induced by tender offers).

[230] 476 U.S. 573 (1986).

[231] *Id.* at 582.

[232] *Id.* at 579.

[233] *Id.* at 582–83 (second alteration in original) (citing Baldwin v. G.A.F. Seelig, Inc., 294 U.S. 511, 521 (1935)).

[234] *See* Denning, *supra* note 193, at 979 (commenting on the steep decline in the courts' reliance on the extraterritoriality principle of the dormant Commerce Clause).

[235] *See* Goldsmith & Sykes, *supra* note 194, at 787, 789 (arguing against the notion that all attempts at regulating the internet violate the dormant Commerce Clause).

[236] *See* Denning, *supra* note 193, at 992–93 (noting that federal court judges are reluctant to strike down a law merely because it may affect out-of-state companies and highlighting that doing so would invalidate many manufacturing and labeling safety regulations).

[237] 538 U.S. 644 (2003).

[238] *Id.* at 662–63.

interstate commerce.[239] The Court declined to strike down the Maine law on dormant Commerce Clause grounds, finding that the reasoning in *Healy* was not applicable.[240] While the Maine regulation did prescribe the *terms* of transactions that took place outside of Maine, the Act did not regulate the price of drugs, nor did it tie the price of drugs sold in-state to out-of-state prices.[241] Conversely in *Healy*, the Connecticut statute amounted to Connecticut regulating the price of beer in other states.[242]

The Court's extraterritoriality doctrine reemphasizes the understanding that a state's regulatory power is limited by its borders.[243] However, the Court has not struck down state regulations based solely on extraterritoriality grounds in decades.[244] While some scholars argue that the extraterritoriality doctrine is "dead,"[245] notwithstanding the aforementioned limits, there are three areas where the extraterritoriality doctrine is thought to survive: (1) in cases where a statute links prices between states;[246] (2) in cases when one state seeks to project its own legislation into another state or where it is obvious the state's statute is

[239] *Id.* at 669.

[240] *Id.*

[241] *Id.*

[242] *Id.*

[243] Healy v. Beer Inst., 491 U.S. 324, 336 (1989) (finding a state law "that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature").

[244] *See* Denning, *supra* note 193, at 979–80 (stating that the Court favored the extraterritoriality doctrine in the 1980s, but the current Court has not utilized the doctrine).

[245] *See id.* at 979–80, 996–97 (noting that the extraterritoriality doctrine was a judicial tool used to apply the *Pike* test and that the doctrine has experienced a "loss of fit").

[246] *Id.* at 992.

an attempt to control activities taking place in another state;[247] and (3) "in certain cases dealing with early state regulation of the Internet."[248]

States cannot be allowed to "force those other States to alter their own regulatory schemes" in order for that state's scheme to prevail.[249] If a state passes a statute that regulates conduct that occurs wholly outside the state, then the statute will likely be deemed unconstitutional.[250] When considering whether to strike down a state regulation as unconstitutional, a court must weigh "the nature of the local interest involved, and [ ] whether it could be promoted as well with a lesser impact on interstate activities."[251]

The extraterritoriality doctrine is likely a supplement to a robust *Pike* analysis. In both *Edgar* and *Healy*, the Supreme Court staked its holdings on alternative grounds to justify finding a dormant Commerce Clause violation.[252] Ultimately, when evaluating the dormant Commerce Clause implications of a state's internet regulation, courts base their reasoning on the statute's extraterritorial implications, coupled with a vigorous *Pike* balancing analysis.[253]

[247] *See, e.g.*, Legato Vapors, LLC. v. Cook, 847 F.3d 825, 834 (7th Cir. 2017) (holding an Indiana law regulating e-vapor cigarette liquid unenforceable against out-of-state e-cigarette manufacturers because it amounted to "direct and unconstitutional extraterritorial regulation of out-of-state" manufacturers and purchasers in their home states). *But see* Pharm. Research & Mfrs. of Am. v. Walsh, 538 U.S. 644, 669 (2003) (holding that the *Healy* doctrine did not apply to a Maine law that mandated drug manufacturers to provide rebate for sales to low-income Maine residents because the law did not "regulate the price of any out-of-state transaction, either by its express terms or by its inevitable effect," nor did it require that "manufacturers sell their drugs . . . for a certain price").

[248] *See* Denning, *supra* note 193, at 992–93, 993 n.82 (discussing lower courts' reasoning to this effect); *see also infra* Section II.F (discussing the dormant Commerce Clause's role in the modern world).

[249] Brown-Forman Distillers Corp. v. N.Y. State Liquor Auth., 476 U.S. 573, 583–84 (1986).

[250] *See* Denning, *supra* note 193, at 992–93, 993 n.82; *see Brown-Forman Distillers*, 476 U.S. at 582 (invalidating a New York liquor statute that regulated conduct occurring wholly outside of the state because it violated the Commerce Clause).

[251] Pike v. Bruce Church, Inc. 397 U.S. 137, 142 (1970).

[252] *See* Edgar v. MITE Corp., 457 U.S. 624, 643 (1982) (finding that, in addition to extraterritoriality, the regulation failed the *Pike* test); Healy v. Beer Inst., 491 U.S. 324, 340 (1989) (finding that the statute was extraterritorial and discriminatory); *see also* Denning, *supra* note 193, at 996–97 (implying that the Court has never struck down a statute on dormant Commerce Clause grounds based solely on extraterritoriality).

[253] Denning, *supra* note 193, at 1000–01.

E. Inconsistent Regulation

The final hurdle a state regulation must surpass is the so-called "inconsistent regulation" prong of the dormant Commerce Clause. Courts interpret the dormant Commerce Clause to prohibit state regulations that "adversely affect interstate commerce by subjecting activities to inconsistent regulations."[254] This is the least-developed category of dormant Commerce Clause jurisprudence.[255]

The "inconsistent regulation" component of the dormant Commerce Clause analysis does not automatically invalidate any state regulations that are different from one another. Rather, the inconsistent regulation doctrine prevents "nonuniform state regulations [that] might impose compliance costs that are so severe that they counsel against permitting the states to regulate a particular subject matter."[256] These inconsistent regulations are ones where several states have different requirements, thereby raising the costs of compliance for "multijurisdictional firms."[257]

[254] CTS Corp. v. Dynamics Corp. of Am., 481 U.S. 69, 88 (1987).

[255] Kosseff, *supra* note 15, at 203–05 (stating that the inconsistent regulation portion of the dormant Commerce Clause, while convenient in striking down internet-based regulation, lacks the Court's insight in how the doctrine applies broadly).

[256] Goldsmith & Sykes, *supra* note 194, at 806–07.

[257] *See id.* (noting the Court was particularly aggressive in striking down inconsistent state regulation in transportation cases); *see, e.g.*, Kassel v. Consol. Freightways Corp., 450 U.S. 662, 671, 674–76 (1981) (invalidating an Iowa restriction on truck length because: (1) it provided insufficient safety benefits to Iowa residents that failed to justify the burden on interstate commerce; (2) companies were required to find alternative, expensive means of avoiding Iowa's highways; and (3) there was a "disproportionate burden" imposed on out-of-state actors); Raymond Motor Transp., Inc. v. Rice, 434 U.S. 429, 447–48 (1978) (invalidating a Wisconsin regulation that barred the operation of truck trailers longer than fifty-five feet, reasoning that the local regulation provided only "speculative" safety benefits while unduly burdening interstate commerce, particularly because the regulation was prohibitively expensive for out-of-state trucking companies that would be required to offload their trailers at the state border should they wish to travel through the state); Bibb v. Navajo Freight Lines, Inc., 359 U.S. 520, 529 (1959) (invalidating an Illinois mudguard regulation that conflicted with an Arkansas regulation on the grounds that the local safety benefits did not provide sufficient justification for Illinois to place such a strain on interstate commerce); S. Pac. Co. v. Arizona *ex rel.* Sullivan, 325 U.S. 761, 771, 773 (1945) (invalidating an Arizona regulation that restricted train lengths, finding that the regulation ran contrary to "standard practice," which would "materially impede[] the movement of . . . trains through that state and interposes a substantial obstruction to the national policy" of promoting an "adequate, economical, and efficient" railway in the United States).

While the internet, like navigating interstate commerce, is an area where uniform legislation would be less costly than a patchwork of regulatory laws, this is not necessarily the approach regulators take. One example of regulations that have been found not to violate the dormant Commerce Clause is the co-existing data breach notification laws.[258] Currently, all fifty states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted a data breach notification law.[259] While each state has different requirements, it is possible—though perhaps expensive—for one company to understand the different compliance requirements, as none of the laws directly conflict.[260] Data breach laws have not faced a dormant Commerce Clause challenge; regardless, these laws would likely survive because they provide consumers with valuable information about the safety of sensitive data, and compliance with all the laws is not so costly that it outweighs the benefits.[261] Like the extraterritoriality prong, the inconsistent regulation prong presents an interesting framework that ultimately is a "variant of [the *Pike*] balancing analysis."[262]

F. A Dormant Commerce Clause for a Modern World?

In recent decades, dormant Commerce Clause challenges have not been concerned with protectionist statutes, but rather with obscenity and anti-spam regulations. This Section will explore the two leading cases on state internet regulation: *American Libraries Ass'n v. Pataki*[263] and *State v. Heckel*.[264] These two cases apply a dormant Commerce Clause analysis in the context of an obscenity statute and an anti-spam statute. Although the cases arrive at different outcomes, they provide

[258] Citron, *supra* note 174, at 805. Data breach notification laws require private entities and government organizations to notify individuals whose personally identifiable information has been compromised in a data security breach. *See, e.g.*, MASS. GEN. LAWS ch. 93H, § 3 (2020).

[259] *See Security Breach Notification Chart*, PERKINS COIE, https://www.perkinscoie.com/images/content/2/3/v3/234941/Security-Breach-Notification-Law-Chart-06.22.2020.pdf [https://perma.cc/4SY2-5H5X] (listing all U.S. security breach notification laws by state).

[260] Citron, *supra* note 174, at 805.

[261] *See id.* (noting that the various data breach notifications statutes are relatively easy to understand, and consumers need to know when data breaches take place to take affirmative steps to protect their own data).

[262] Goldsmith & Sykes, *supra* note 194, at 808.

[263] 969 F. Supp. 160 (S.D.N.Y. 1997).

[264] 24 P.3d 404 (Wash. 2001) (en banc).

key insight into the dormant Commerce Clause's role in limiting the states' authority to regulate the internet.

1. *Obscenity regulations and the dormant Commerce Clause:* American Library Ass'n v. Pataki

In *Pataki*, the Southern District of New York applied a dormant Commerce Clause analysis to a New York penal statute aimed at reducing children's access to obscene material online.[265] New York passed New York Penal Law section 235.21(3), which criminalized using a computer to circulate obscene or "indecent material" to minors.[266] Artists, booksellers, and online content distributors were considerably outraged, claiming that this law amounted to impermissibly regulating interstate commerce.[267] The Southern District of New York ultimately struck down the statute as unconstitutional.[268] Judge Preska, writing for the majority, found that the statute violated the dormant Commerce Clause on three separate grounds.[269]

First, the court held that the obscenity law unconstitutionally projected New York law onto conduct occurring "wholly outside" the state.[270] Taking into account both the internet's disregard for geographical boundaries and the New York legislature's intent for the law to govern interstate communications, the court reasoned it was impossible for the law to apply exclusively to intrastate activities.[271]

Second, the court found that the extraterritorial nature of the law ran afoul of the dormant Commerce Clause, as New York "imposed its legislation on the Internet and, by doing so, projected its law into other states whose citizens use the [internet]."[272] Relying on the extraterritoriality prong of dormant Commerce Clause jurisprudence, the court found that the law stretched beyond New York's boundaries to prosecute individuals who may be engaging in otherwise legal activity in their home state without any mechanism to prevent New York residents

[265] 969 F. Supp. at 163, 169.

[266] N.Y. PENAL LAW § 235.21(3) (McKinney 2020).

[267] *See* Kosseff, *supra* note 15, at 197 (discussing how online merchants were frustrated by the statute and believed it raised both Commerce Clause and free speech concerns).

[268] *Pataki*, 969 F. Supp. at 177.

[269] *Id.* at 169.

[270] *Id.* at 169–70.

[271] *Id.* at 170.

[272] *Id.* at 177.

from accessing their websites.[273] Further, the statute had a "chilling effect," where those uncertain of the statute's reach would "steer far wider of the unlawful zone."[274] The court highlighted that the "chilling effect . . . is bound to exceed the actual cases that are likely to be prosecuted."[275] The court claimed that this form of regulation constituted an impermissible overreach of power that undermined the authority of the other forty-nine states.[276]

The court also found that the New York statute was invalid under the *Pike* balancing test.[277] While the New York statute had a "quintessentially legitimate state objective" of protecting children from exposure to pornography, there was little evidence that the statute would result in actual *realized* benefits.[278] On the other end of the *Pike* scale, the court found that the law's "chilling effect," the possibility of New York extending its prosecutorial reach worldwide, and the costs imposed on website owners to comply with the law, outweighed any minimal benefits bestowed on New Yorkers.[279] This "chilling effect" combined with an increase in New York's prosecutorial power amounted to "an extreme burden on interstate commerce."[280]

Finally, the court reasoned that the Act led to an environment where the internet would be filled with inconsistent regulations.[281] The court claimed that certain types of commerce were "susceptible to regulation only on a national level," and it included the internet in this category.[282] The court's decision in *Pataki* received widespread criticism that it had pushed the extraterritoriality doctrine beyond its

[273] *Id.*

[274] *Id.* at 179 (quoting Baggett v. Bullitt, 377 U.S. 360, 372 (1964)).

[275] *Id.*

[276] *Id.* at 178.

[277] *Id.* at 177.

[278] *See* Michelle Armond, *State Internet Regulation and the Dormant Commerce Clause*, 17 BERKLEY TECH. L.J. 379, 388 (2002) (footnote omitted) (quoting *Pataki*, 969 F. Supp. at 177) ("According to the court, other New York laws and the unchallenged parts of the statute left only a small category of cases uncovered, and the court predicted that jurisdictional limitations would constrain the state's ability to prosecute offenders in that category.").

[279] *Pataki*, 969 F. Supp. at 179.

[280] *Id.*

[281] *Id.* at 181.

[282] *Id.*; *see also* Regan, *supra* note 184, at 1184, 1285 (noting the transportation cases involved an application of the *Pike* balancing test weighing the country's significant interest in a national transportation system).

limits and impermissibly halted states from regulating the internet.[283] Despite this criticism, the *Pataki* court's decision led other courts to strike down a variety of internet regulations that stretched beyond a state's borders to regulate wholly out-of-state conduct.[284] Jeff Kosseff, in his Article discussing the need for national cybersecurity legislation, posits that the reasoning in *Pataki* and subsequent cases prevent a state from regulating "the details of a company's cybersecurity program merely because the company stores or processes the data of some customers who live in the state."[285]

2. *Anti-spam regulations and the dormant Commerce Clause:* State v. Heckel

The second leading case in state regulation of the internet is *State v. Heckel*, where the defendants argued that an anti-spam statute in Washington regulated extraterritorially, exposed consumers to inconsistent regulation, and placed an undue burden on interstate commerce.[286] However, unlike in *Pataki*, the Supreme Court of Washington was not convinced and held that any local benefits far outweighed the purported burdens on interstate commerce.[287] In *Heckel*, an Oregon resident sent "between 100,000 and 1,000,000 [spam] messages per week" advertising a booklet entitled "How to Profit from the Internet" for $39.95.[288] The Washington attorney general received several complaints about these

[283] *See* Goldsmith & Sykes, *supra* note 194, at 786 (arguing that the *Pataki* court's reasoning precluded any state from regulating the internet).

[284] Kosseff, *supra* note 15, at 199; *see, e.g.*, PSINet, Inc. v. Chapman, 362 F.3d 227, 239 (4th Cir. 2004) (striking down a Virginia law that closely mimicked *Pataki*); Am. Booksellers Found. v. Dean, 342 F.3d 96, 103–04 (2nd Cir. 2003) (invalidating a Vermont law that prohibited the knowing distribution of harmful material to a minor on the grounds that out-of-state citizens who violated the statute would be subject to prosecution in Vermont); ACLU v. Johnson, 194 F.3d 1149, 1160–62 (10th Cir. 1999) (holding that a *Pataki*-like New Mexico law violated the dormant Commerce Clause because the law interfered with "free private trade in the national marketplace" (quoting Gen. Motors Corp. v. Tracy, 519 U.S. 278, 287 (1997)); Se. Booksellers Ass'n v. McMaster, 371 F. Supp. 2d 773, 787 (D.S.C. 2005) (striking down a statutory provision using *Pataki* analysis as it placed an "undue burden on interstate commerce by regulating commerce occurring wholly outside of South Carolina"); Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d. 606, 662–63 (E.D. Pa. 2004) (invalidating a law that exported state policies to other states and imposed greater burdens than the legislation in *Pataki*).

[285] Kossef, *supra* note 15, at 200.

[286] State v. Heckel, 24 P.3d 404, 405, 411 (Wash. 2001) (en banc).

[287] *Id.* at 411.

[288] *Id.* at 406.

spam emails, alleging that the emails "contained misleading subject lines and false transmission paths" in violation of the Washington statute.[289] Heckel challenged the constitutionality of the Act under the dormant Commerce Clause.[290]

The Washington Supreme Court engaged in a robust analysis relying primarily on the *Pike* test.[291] The court found that the Act evenhandedly regulated against both in-state and out-of-state spammers alike.[292] Further, the Act promoted the "legitimate local purpose" of reducing the cost of deceptive spam for Washington residents.[293] The court weighed that interest against the alleged burdens on interstate commerce:

> To be weighed against the Act's local benefits, the only burden the Act places on spammers is the requirement of truthfulness, a requirement that does not burden commerce at all but actually "facilitates it by eliminating fraud and deception." Spammers must use an accurate, nonmisleading subject line, and they must not manipulate the transmission path to disguise the origin of their commercial messages. While spammers incur no costs in complying with the Act, they do incur costs for noncompliance, because they must take steps to introduce forged information into the header of their message. In finding the Act "unduly burdensome," the trial court apparently focused not on what spammers must do to comply with the Act but on what they must do if they choose to use deceptive subject lines or to falsify elements in the transmission path.[294]

The court emphasized that the statute only impeded spammers who were engaging in purposefully deceptive behavior. Only then would the statute require out-of-state spammers to begin the costly process of sorting out Washington residents. However, the court reasoned that it cost very little to use "nonmisleading" subject lines.[295] For actors nationwide (both in-state and out-of-state) wanting to solicit business via email without a deceptive intent, simply using an accurate subject line describing the contents of their email would not amount to an undue burden requiring the actors to avoid targeting Washington

[289] *Id.* at 406–07; *see* WASH. REV. CODE § 19.190.020(1) (2020) (outlawing emails that contain misleading subject lines or misrepresent the point of origin).

[290] *Heckel*, 24 P.3d at 409.

[291] *Id.*

[292] *Id.*

[293] *Id.* at 410 (quoting Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970)).

[294] *Id.* at 411 (footnote omitted) (citations omitted).

[295] *Id.*

recipients.[296] While the Washington Supreme Court ultimately held that the non-discriminatory statute did not violate the dormant Commerce Clause, it provided sound guidance for distinguishing unburdensome extraterritorial state internet regulation.[297]

III. ANALYSIS

Although the newly enacted CCPA has not faced a dormant Commerce Clause challenge yet, it raises several constitutionality issues, such as the substantial burden it places on out-of-state businesses, particularly small businesses, its broad application to businesses with less-than-minimal contacts with California, and the potential for creating a patchwork of fifty conflicting and cumbersome data privacy laws.

This Part applies the *Pike* balancing test with a focus on the extraterritoriality doctrine and the inconsistent-regulation prong of the dormant Commerce Clause.

A. *The CCPA Does Not Discriminate Against Out-of-State Actors*

The dormant Commerce Clause primarily prohibits discriminatory behavior from one state against out-of-state actors.[298] The first step of a dormant Commerce Clause analysis is to ask whether the state law facially discriminates or has a discriminatory impact against out-of-state actors.[299] The CCPA does not have protectionist aims as it applies evenhandedly to both in-state and out-of-state actors. The law is particularly aimed at tech companies, which are plentiful in California—perhaps more so than any other state.[300] A detailed analysis of the CCPA demonstrates that the CCPA has no discriminatory aims or effects.[301] While the CCPA would likely be upheld under the first

[296] *Id.* at 411–12.

[297] *Id.* at 411.

[298] Regan, *supra* note 184, at 1093 & n.3.

[299] *See, e.g.*, City of Philadelphia v. New Jersey, 437 U.S. 617, 626–27 (1978) (finding a New Jersey statute that prohibited the importation of waste that originated outside New Jersey facially discriminatory and unconstitutional).

[300] *See* Kimberly Amadeo, *Silicon Valley, America's Innovative Advantage*, BALANCE (Aug. 25, 2019), https://www.thebalance.com/what-is-silicon-valley-3305808 [https://perma.cc/GZ6T-VZXA] (stating that California's Silicon Valley is the global hub for innovative technology companies).

[301] *See supra* Section I.C (highlighting that the CCPA applies evenhandedly to both in-state and out-of-state actors because the CCPA applies to businesses that satisfy the

prong of a dormant Commerce Clause analysis, a court will likely find that the CCPA impermissibly burdens interstate commerce.

B. *The CCPA Fails the* Pike *Balancing Test by Imposing Significant and Excessive Burdens on Interstate Commerce that Are Not Outweighed by the Local Putative Benefits*

At its core, the *Pike* test balances the challenged regulation's local benefits against the incidental burden imposed on interstate commerce.[302] A clearly excessive burden will be deemed unconstitutional.[303] A court will likely find a clearly excessive burden on interstate commerce when a statute does not support a legitimate local purpose or if the statute does support a legitimate local purpose but unduly burdens interstate commerce to accomplish that purpose.[304] The *Pike* test is a fact-intensive analysis that focuses on the intent behind the contested regulation and the alleged burden imposed on interstate commerce.[305]

The CCPA fails the *Pike* balancing test by imposing significant and excessive burdens on interstate commerce that are not outweighed by the local putative benefits. The CCPA was originally enacted to create meaningful digital privacy protections for California residents and to fill Congress's gap in federal digital privacy legislation.[306] This is a perfectly legitimate local purpose.[307] However, in its attempt to accomplish this goal, the CCPA imposes an immense burden on interstate commerce and "[e]ven with the fullest recognition that [the state interest] is an indisputably valid state goal . . . . [California] cannot avoid the second stage of the inquiry simply by invoking [a] legitimate state interest underlying the Act."[308]

Despite its legitimate local purpose, the CCPA's broad material scope and hefty compliance costs create an undue burden that is "clearly excessive in relation to the putative local benefits."[309] The

statutory thresholds whether or not they are based in California so long as that business collects or processes data from California residents).

[302] Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970).

[303] *Id.*

[304] *Id.*

[305] *See id.* at 146.

[306] *See* Confessore, *supra* note 6 (discussing the CCPA's legislative history).

[307] *See* Hunt v. Wash. State Apple Advert. Comm'n, 432 U.S. 333, 350 (1977) (noting that a state passing regulation in "consumer protection areas" is a "legitimate local concern").

[308] Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 178 (S.D.N.Y. 1997).

[309] *Pike*, 397 U.S. at 142.

CCPA applies to any business that "collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California."[310] To be subject to the CCPA, a business must meet one of three minimum statutory requirements.[311]

One conservative figure estimates that 500,000 U.S. companies will be forced to decide whether to comply with the CCPA or take steps to completely avoid the California marketplace.[312] This latter "chilling effect" is reminiscent of the issue before the court in *Pataki*.[313] Like the New York Statute in *Pataki*, the CCPA "casts its net worldwide."[314] While the CCPA does not impose criminal liability on noncompliant businesses, it does impose huge financial, administrative, and legal burdens on those businesses subject to the law—the vast majority of which have few means to surmount this burden.[315] Businesses subject to the CCPA are projected to spend a collective $55 billion in upfront compliance costs.[316] These huge costs will adversely affect small- and medium-sized businesses that do not have the same resources as larger companies to devote to CCPA compliance.

One might be tempted to argue that the CCPA will not impose significant costs on businesses because the GDPR was such a sweeping regulation that many companies can recycle their GDPR-compliant policies to adhere to the requirements of the CCPA.[317] This assumption

[310] CAL. CIV. CODE § 1798.140(c)(1) (West 2020).

[311] *Id.* § 1798.140(c)(1)(A)–(C). The business is subject to the law if it: (1) has a revenue greater than or equal to $25 million; or (2) "annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices"; or (3) derives greater than fifty percent of its annual revenues from selling consumer data. *Id.*

[312] Heimes & Pfeifle, *supra* note 80.

[313] *See Pataki*, 969 F. Supp. at 177, 179 (deciding that a New York law prohibiting the dissemination of "obscene" material to minors over the internet violated the dormant Commerce Clause).

[314] *See id.* at 179.

[315] *See* Heimes & Pfeifle, *supra* note 80 (reporting that the majority of businesses required to comply with the CCPA are small- to medium-sized businesses).

[316] Lindsey, *supra* note 88.

[317] *See, e.g.*, Alexander B. Reynolds, *Leveraging Your GDPR Compliance Investment for CCPA*, DAVIS WRIGHT TREMAINE LLP (Feb. 26, 2019), https://www.dwt.com/blogs/privacy–security-law-blog/2019/02/leveraging-your-gdpr-compliance-investment-for-ccp [https://perma.cc/VJT9-G7SA] (outlining how companies can leverage GDPR

is flawed in several respects. The GDPR and the CCPA are *not* perfect equivalents.[318] While they both provide for sweeping change with respect to data privacy rights, each has a unique set of requirements.[319] Further, many businesses that were not required to comply with the GDPR will now be required to comply with the CCPA.[320] While many U.S.-based companies are GDPR-compliant, these are primarily large companies that have an EU presence or reasonably target their goods and/or services to EU customers.[321] These large companies will be able

preparation to comply with the CCPA because many, though not all, of the necessary steps for both overlap). *But see* Carol A. F. Umhoefer, *CCPA vs. GDPR: The Same, Only Different*, DLA PIPER (Apr. 11, 2019), https://www.dlapiper.com/en/us/insights/publications/2019/04/ipt-news-q1-2019/ccpa-vs-gdpr [https://perma.cc/DS8X-4KTR] (highlighting key differences between the GDPR and the CCPA, such as the scope of the laws, the definitions for covered entities, and the differences in various exceptions).

[318] *See* Umhoefer, *supra* note 317 (summarizing the differences between the GDPR and the CCPA); *see also supra* notes 101, 154 (comparing the CCPA's and the GDPR's definitions for personal information and the right to be deleted).

[319] *See* Umhoefer, *supra* note 317. The GDPR and the CCPA are similar in how they define certain terminology, how they create additional protections from children sixteen and under, and how they aim to provide greater protections for personal information. *Id.* However, the laws are quite different in scope. The CCPA only protects California residents. CAL. CIV. CODE § 1798.140(g) (West 2020). The GDPR does not have a residency requirement; it applies evenhandedly to any living person whose data is processed by a controller with an EU establishment. GDPR art. 3. Further, the laws differ in what types of data are exempt. The CCPA carves out exceptions for broad categories of data that may already be subject to a US regulation, such as medical information, financial information, and publicly available information. CAL. CIV. CODE §§ 1798.145(c)–(d), 1798.140(o)(2). The GDPR excludes specialized forms of personal information. GDPR art. 4(6). Finally, the biggest difference between the laws is that the GDPR requires "data controllers" to have a legal basis for processing data and the CCPA does not require businesses to establish legal grounds before businesses are allowed to collect and sell personal information. *See* CAL. CIV. CODE § 1798.120; GDPR art. 5–6, 10.

[320] *See, e.g.*, Matt Novak, *Dozens of American News Sites Blocked in Europe as GDPR Goes into Effect Today*, GIZMODO (May 25, 2018, 7:00 AM), https://gizmodo.com/dozens-of-american-news-sites-blocked-in-europe-as-gdpr-1826319542 (discussing U.S. websites, including many newspapers, that chose to block European access to avoid the compliance burdens of the GDPR); *see also* Caitlin Fennessy, *IAPP FAQs: Are GDPR-Compliant Companies Prepared for CCPA?*, IAPP (Apr. 17, 2019), https://iapp.org/news/a/are-gdpr-compliant-companies-prepared-for-ccpa [https://perma.cc/J7NK-J4NN] ("[R]ecent GDPR preparation is helpful, [but] the CCPA has nuanced requirements that go beyond the GDPR.").

[321] The GDPR applies to (1) companies that have an EU-established presence, and (2) organizations that process personal data in connection with "offering of goods or services" or monitoring of the individual's behavior within the EU. GDPR art. 3.

to repurpose their GDPR compliance strategies to fit the CCPA.[322] Further, these large companies are already equipped to "absorb [the CCPA's] up-front compliance costs" due to the availability of in-house counsel, in-house IT personnel, and significantly larger budgets.[323] Small businesses will bear the "undue burden" so that only a few Americans can have online privacy.[324]

This Comment discusses the rights the CCPA created for Californians.[325] While these rights are significant when compared with the lack of privacy rights in the United States, the lack of significant enforcement provisions creates a question as to whether businesses will actually comply if they do not fall into the category of a "tech giant" like Microsoft, Facebook, or Amazon.[326] The CCPA only creates a private right of action for data breaches;[327] the Attorney General is tasked with enforcing the remaining portions of the CCPA.[328] This private right of action enables a consumer to recover anywhere from $100–$750 or actual damages (whichever is greater) "per consumer per incident" for unintentional violations.[329] Further, the Attorney General can level a civil fine up to $7,500 for willful violations for each violation.[330] These penalties will severely impact smaller businesses but

[322] Odia Kagan, *CCPA Draft Regs Regulatory Impact Assessment Provides More Insight into CCPA Compliance*, FOX ROTHSCHILD (Nov. 5, 2019), https://www.foxrothschild.com/publications/ccpa-draft-regs-regulatory-impact-assessment-provides-more-insight-into-ccpa-compliance [https://perma.cc/NA47-K6D8].

[323] *See id.*

[324] *See* Pike v. Bruce Church, Inc., 397 U.S. 137, 145 (1970) (reasoning that the benefits of the Arizona statute did not outweigh the burden placed on companies that would have to pay for "unneeded" and costly services to comply).

[325] *Supra* Section I.C.1.b.i–iii (discussing the CCPA's "right to know," "right to access," "erasure right," and "right to opt-out").

[326] *See* Fadilpašić, *supra* note 124 (noting that sixty-eight percent of businesses struggle to comply with current privacy law). While a strong national pull for more privacy rights may initially lead one to believe that the CCPA's benefits outweigh the costs, it appears that some Californians do not believe that there are strong putative local benefits to the CCPA. Mactaggart and his followers placed a new initiative that adds the "teeth" back into the CCPA on the November ballot, the California Privacy Rights Act of 2020. *See* Rogers, *supra* note 178 (highlighting Mactaggart and his followers' new referendum to build stronger enforcement into the CCPA). This referendum passed with nearly fifty-six percent of the vote on November 3rd and will go into effect January 2023. *CPRA Is Voted into Law*, *supra* note 72.

[327] CAL. CIV. CODE § 1798.150(a)(1) (West 2020).

[328] *Id.* § 1798.155(b).

[329] *Id.* § 1798.150(a)(1)(A).

[330] *Id.* § 1798.155(b).

barely rise to a slap on the wrist for companies like Google and Amazon.[331] While the private right of action and statutory damages for data breach violations are a step in the right direction, the penalties will likely have little effect on the targeted companies.[332]

In addition to the CCPA lacking "teeth," many of the CCPA's new rights and compliance requirements are confusing and present complicated challenges in application.[333] Open questions such as "when is a personal information category truly deidentified?"; "how can a business truly verify a consumer access request?"; and "when is a business actually required to comply with a consumer's deletion request?" require significant resources for businesses to answer.[334] The CCPA is not clear, and the California Attorney General does not provide particularly helpful insight into the regulations, which are as long and confusing as the CCPA itself.[335]

[331] *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*, FED. TRADE COMM'N (Sept. 4, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations [https://perma.cc/EQ8L-8NQE] (noting the settlement amount, which is less than 0.1% of Google and YouTube's yearly revenue).

[332] *See* Peter Kafka, *Facebook Will Pay the US Government a $5 Billion Fine for Privacy Failures—but It Won't Have to Change the Way It Does Business*, VOX (July 24, 2019, 10:00 AM), https://www.vox.com/recode/2019/7/24/20708359/facebook-ftc-settlement-criticism-5-billion-privacy-review-antitrust-mark-zuckerberg (noting that while a $5 billion fine would be devastating to ordinary businesses, it counted for less than thirty-five percent of Facebook's revenue for the previous *quarter*). The government settled for a lesser amount to avoid a long court battle with the technology giant. *Id.*

[333] *See, e.g.*, Douglis & Saunders, *supra* note 155 (noting that in both ongoing and anticipated litigation, it is commonplace for businesses to provide their attorneys with massive amounts of information that likely falls within the scope of the CCPA, meaning that businesses would have to "maintain an inventory of what consumer information is collected and produced in civil litigation"—a likely impossible task).

[334] *See supra* Section I.C.1.b (discussing the various costs to businesses associated with CCPA compliance).

[335] *See, e.g.*, CAL. CODE REGS., tit. 11, §§ 999.301(m), 999.305(a)(2)(a), 999.305(b)–(d) (2020) (proposed CCPA regulations demanding that businesses use short, plain, easy-to-read language in their privacy policies but simultaneously requiring companies to include more information—inevitably making those policies longer); *see also* Angelique Carson, *Critics Say Attorney General's Proposed CCPA Regulations Add Confusion, Not Clarity*, IAPP (Oct. 11, 2019), https://iapp.org/news/a/critics-say-ags-proposed-ccpa-regulations-add-confusion-not-clarity [https://perma.cc/VE87-VJWS] (noting that while the regulations should be written in plain language, they create even more ambiguities than the CCPA itself).

Much like the state regulators in the "transportation cases,"[336] the Arizona regulators in *Pike*, and the New York regulators in *Pataki*, the CCPA's local benefits of consumer privacy are honorable and legitimate.[337] However, the California legislature failed to consider the second part of the dormant Commerce Clause inquiry: the local benefits must also outweigh the burdens imposed on commerce amongst the several states.[338] The CCPA provides digital privacy rights only to Californians. While those rights go beyond any existing U.S. privacy law, the CCPA itself is complicated and confusing; many businesses will struggle to actually provide those rights to Californians. The CCPA's putative benefits, while legitimate, fail to outweigh the immense burdens the CCPA imposes on interstate commerce.

C. The CCPA Regulates Conduct that Occurs Wholly Outside of the State

Under the *Pike* balancing test, the CCPA is likely to fail an extraterritoriality analysis. In addition to imposing undue burdens on interstate commerce, the CCPA regulates conduct that occurs entirely outside of California. The CCPA claims that it does not regulate conduct that exists *wholly* outside of California.[339] However, in order to satisfy that threshold, the business cannot conduct sales in California, cannot collect data about a California resident (whether or not that resident is currently in California), and cannot sell information about any California resident.[340] The vast majority of businesses do not categorize their data by resident location, and many businesses cannot guarantee they do not collect data from California residents.[341] Rather than risk an audit, many businesses are complying with the CCPA.[342]

[336] *See, e.g.*, *supra* note 257 (discussing the "transportation cases" in depth).

[337] *See* Hunt v. Wash. State Apple Advert. Comm'n, 432 U.S. 333, 350 (1977) (noting that "consumer protection areas" are matters of "legitimate local concern").

[338] *See* Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 177 (S.D.N.Y. 1997) (reminding state regulators that the *Pike* test is a two-part inquiry).

[339] CAL. CIV. CODE § 1798.145(a)(6) (West 2020).

[340] *Id.*; CAL. CODE REGS. tit. 18, § 17014.

[341] *See O'Donnell*, *supra* note 112 (claiming that many businesses will provide CCPA rights for all customers rather than undergo the costly task of sorting out California-based customers).

[342] *See id.*

By enacting the CCPA, California impermissibly projects its sovereignty onto other states.[343]

The CCPA allows California to control "commerce occurring wholly outside the boundaries of [the] State[,] exceed[ing] the inherent limits of [California's] authority."[344] In *Healy*, the Supreme Court held that state regulation that amounts to "directly control[ling] commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature."[345] The CCPA's broad material scope is precisely the impermissible behavior described by Justice Blackmun in *Healy*.[346] By requiring businesses nationwide to comply with the CCPA if they accept "a single dollar from a California resident,"[347] California impermissibly enacted a national privacy law.

While the CCPA concerns a different subject matter, its broad reach into out-of-state business practices is analogous to the New York Statute's broad reach in *Pataki*. In *Pataki*, the Southern District of New York reasoned that, taking into account both the internet's insensitivities to geographical boundaries and the legislature's intent for the law to govern interstate communications, it was impossible for the New York law to apply exclusively to intrastate activities.[348] Similarly, the CCPA's broad and complicated nature makes it impossible for the law to apply exclusively to intrastate activities. The CCPA is "insensitive

[343] *See* Edgar v. MITE Corp., 457 U.S. 624, 642 (1982) (holding that the Illinois Business Take-Over Act, which regulated transactions that took place "across state lines," was in violation of the Commerce Clause).

[344] Healy v. Beer Inst., 491 U.S. 324, 336 (1989).

[345] *Id.*

[346] *See id.*

[347] Eric Goldman, *41 California Privacy Experts Urge Major Changes to the California Consumer Privacy Act*, TECH & MKTG. L. BLOG (Jan. 17, 2019), https://blog.ericgoldman.org/archives/2019/01/41-california-privacy-experts-urge-major-changes-to-the-california-consumer-privacy-act.htm#:~:text=41%20California%20Privacy%20Experts%20Urge%20Major%20Changes%20to,highlights%20six%20significant%20problems%20with%20the%20CCPA%2C%20including%3A [https://perma.cc/5RG3-2BV9] (discussing a letter written to the California legislature by numerous privacy experts asking for changes to the CCPA).

[348] *See* Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 170 (S.D.N.Y. 1997) (finding that the nature of the internet was to cross state boundaries and the intent of the law was to govern communication).

to geographical distinctions,"[349] as it protects California residents' data in any state or country in which their data is processed.[350] The California legislature intended for the CCPA to protect California residents' data without relevance to the data's origin or the collector's location. Because California residents are often parties to transactions that take place outside of California, the CCPA cannot regulate solely intrastate activities.[351]

Conversely, in *Heckel*, the Washington Supreme Court reasoned that because the only individuals (both in-state and out-of-state) who were going to face immense compliance costs were bad actors, the Washington law did not violate the dormant Commerce Clause.[352] Unlike in *Heckel*, those wishing to do business in California cannot simply rephrase a subject line to no longer risk violating the CCPA.[353] The CCPA has intricate and nuanced requirements that require significantly more work than revising an email.[354] The CCPA requires businesses to implement new data management strategies, provide new training to all employees, and overhaul existing technological systems.[355] Both good and bad faith actors alike will be forced to undergo expensive financial and administrative changes to continue to do business that is tangentially connected to California.

D. *The CCPA Will Likely Lead to Multiple Conflicting Comprehensive Data Privacy Laws*

A multitude of complicated and conflicting data privacy laws is a matter of when, not if. Many states are actively considering a comprehensive privacy law.[356] Some of these recently introduced bills are modeled after

[349] *Id.*

[350] CAL. CIV. CODE § 1798.140(c),(g) (West 2020); CAL. CODE REGS. tit. 18, § 17014 (2020) (defining a California resident as one who is domiciled in California, but not necessarily physically in California).

[351] *See Confessore*, *supra* note 6 (noting Mactaggart's hope that the CCPA would result in national privacy protections).

[352] State v. Heckel, 24 P.3d 404, 411 (Wash. 2001).

[353] *See id.*; *see also* CAL. CIV. CODE § 1798.140(c) (defining businesses broadly and not limiting covered entities to those acting in bad faith).

[354] *See, e.g.*, § 1798.100 (providing consumers with the right to know about a business's general data practices, which requires that business to create a new privacy policy and provide ongoing insight to consumers who wish to know more about the business's collection strategies).

[355] *See supra* Section I.C.1 (summarizing the CCPA's extensive compliance requirements).

[356] *See supra* note 84 (demonstrating the numerous pending state privacy bills).

the CCPA, but many are not.[357] In considering whether or not the CCPA will lead to many conflicting laws, a court must consider the full effect of the challenged law.[358] Here, the CCPA has global consequences.[359] The CCPA has already prompted a patchwork of conflicting comprehensive data privacy laws that will prove unworkable.[360] These pending state bills provide a range of protections. Some provide for a "right to know" and a "right to access" but do not provide for a private right of action in the event of a data breach.[361] Others go beyond the CCPA and provide a general private right of action for any violation of the law.[362] Additionally, California passed ground-breaking legislation in seven days.[363] While the current bills are not being pushed through the legislative process at the same speed, it is more than possible for another state to follow in California's footsteps.

The lack of a comprehensive national privacy law, combined with the loud public cry for increased data protections, will lead the states to develop a patchwork of privacy laws that will prove to be unworkable and costly. This patchwork of pending "nonuniform state regulations [will] impose compliance costs that are so severe that they counsel against permitting the states to regulate [data privacy]."[364] The *Pataki* court's instincts about internet regulation were correct; the internet is among the categories of commerce that is "susceptible to regulation only on a national level."[365]

[357] Marmor, *supra* note 84 ("Though the California Consumer Privacy Act . . . has been criticized for containing provisions that are inoperable, legislators in other states have embraced both the structure and specific language of that law. Of the nine states, six follow the full model established in the CCPA, and two approach only certain issues addressed by the CCPA. The ninth state is Washington, which is debating a privacy bill modeled after the GDPR . . . . A tenth state, New Jersey has a draft privacy bill that was introduced last July but has not moved out of committee.").

[358] *See* Edgar v. MITE Corp., 457 U.S. 624, 642 (1982) (analyzing the full effect of the challenged Illinois statute).

[359] *See* Andrew R. Lee, *How the California Consumer Privacy Act Could Impact Your Business*, NAT'L L. REV. (Nov. 20, 2019), https://www.natlawreview.com/article/how-california-consumer-privacy-act-could-impact-your-business [https://perma.cc/2EW5-DTG8] (noting the CCPA's likely impact on "businesses worldwide").

[360] *See supra*, note 84 (summarizing the various pending state privacy legislation).

[361] *See* Marmor, *supra* note 84 (explaining that Hawaii and Maryland have such bills).

[362] *See* Marmor, *supra* note 84 (noting the Massachusetts and New York bills as examples).

[363] *See supra* note 61 and accompanying text (chronicling the hurried passage of the CCPA).

[364] Goldsmith & Sykes, *supra* note 194, at 806–07.

[365] Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 181 (S.D.N.Y. 1997).

IV. THE UNITED STATES NEEDS A NATIONAL PRIVACY LAW

The dormant Commerce Clause precludes the CCPA from setting national privacy law. However, it is time for the United States to establish national data privacy legislation. Congress must pass a comprehensive privacy law that gives all Americans legitimate data protections. The current U.S. privacy regulatory landscape "does not reflect the reality that the internet and connected services and devices have been integrated into every facet of our society."[366] Countries worldwide are beginning to pass legislation to protect the data rights of their citizens, yet the United States has fallen behind in this global movement.[367] Historically, U.S. privacy law has failed to keep pace with rapidly advancing technology.[368] Thus far, Congress has passed privacy laws that are industry-specific.[369] General data practices are currently governed by the FTC, which prohibits businesses from engaging in deceptive practices.[370] Therefore, the FTC can only bring an enforcement action if a business manages consumer data in a way that runs contrary to its own privacy policy, violates existing federal privacy laws, or seriously injures consumers.[371] Limited accountability of large companies that manage huge amounts of data can have serious

[366] *Examining Legislative Proposals to Protect Consumer Data Privacy: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 116th Cong. 1–2 (2019) (statement of Michelle Richardson, Director, Privacy and Data Center for Democracy and Technology).

[367] Governments in over 140 countries have enacted some sort of data privacy legislation. *See* Graham Greenleaf & Bertil Cottier, *2020 Ends a Decade of 62 New Data Privacy Laws*, 163 PRIV. L. & BUS. INT'L REP. 24 (2020); *see, e.g.*, Lei No. 13,709, de 14 de Agosto de 2018 (Braz.); GB/T 35273-2017 信息安全技术 个人信息安全规范 [GB/T 35273-2017 Information Technology—Personal Information Security Specification] (Jan. 2, 2018, effective May 1, 2018) (China); Personal Data Protection Bill (draft bill 2018) (India); Act on the Protection of Personal Information (amended June 5, 2020) (Japan); The Data Protection Act, No. 24 (2019) KENYA GAZETTE SUPPLEMENT NO. 181; Personal Data Protection Act, B.E. 2562 (2019) (Thai.).

[368] *See* SENATE DEMOCRATS, PRIVACY AND DATA PROTECTION FRAMEWORK 1 (2019) (noting that technology and data collection play a significant part in our lives, but privacy legislation has not "evolved" in a similar manner).

[369] *See supra* note 10.

[370] *See* Federal Trade Commission Act, 15 U.S.C. § 45 (2018) (broadly conferring the power to hold businesses accountable for all deceptive practices, not just in the realm of data privacy).

[371] *Privacy and Security Enforcement*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement [https://perma.cc/F8A5-K62B].

consequences ranging from exposing sensitive data[372] to compromising U.S. democracy.[373]

This segmented approach to privacy is no longer sufficient to protect Americans' privacy interests. Massive data breaches grace headlines on a fairly regular basis.[374] Consumers need legitimate privacy protection in order to live in a digital world.[375] The majority of Americans do not feel their data is safe and strongly favor more government regulation surrounding data use.[376] To bolster consumer confidence, Congress must pass a national data privacy law.

Lawmakers are not oblivious to the fact that the United States is behind in developing a comprehensive data privacy law.[377] Members of Congress have introduced several different bills that each take a different approach to providing Americans with the comprehensive data protections they crave.[378] These bills have been introduced by both Democrats and Republicans, signaling to Americans that Congress—on both sides—is aware of the need for more data oversight. However, the various bills disagree on key factors, including a private right of action, carve-outs for small businesses, and federal and state

[372] *See, e.g.*, Tara Siegel Bernard et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html; Emily Flitter & Karen Weise, *Capital One Data Breach Compromises Data of over 100 Million*, N.Y. TIMES (July 29, 2019), https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html; Paul Ziobro & Danny Yadron, *Target Now Says 70 Million People Hit in Data Breach*, WALL ST. J. (Jan. 10, 2014, 8:36 PM), https://www.wsj.com/articles/no-headline-available-1389359240.

[373] *See Facebook Hearing*, *supra* note 26, at 11–13 (statement of Mark Zuckerberg, Chairman & CEO, Facebook) (discussing Russian interference in the 2016 presidential election).

[374] *See supra* note 372 (noting three major data breaches in the past decade that affected millions of Americans).

[375] *See* SENATE DEMOCRATS, *supra* note 368, at 1 (highlighting how the lack of data regulation has significantly harmed consumers).

[376] *See* Auxier, *supra* note 4 (finding that eighty-one percent of adults feel like they do not have control over their data, and seventy-nine percent of adults are concerned with how that data is used).

[377] *See* Cameron F. Kerry, *Will This New Congress Be the One to Pass Data Privacy Legislation?*, BROOKINGS INST. (Jan. 7, 2019), https://www.brookings.edu/blog/techtank/2019/01/07/will-this-new-congress-be-the-one-to-pass-data-privacy-legislation [https://perma.cc/3MVN-Y8NH].

[378] *See, e.g.*, Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. (2020) (introduced by Sen. Moran (R-KS)); Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019) (introduced by Sen. Cantwell (D-WA)); DATA Privacy Act, S. 583, 116th Cong. (2019) (introduced by Sen. Cortez-Masto (D-NV)).

preemption.[379] Both political parties must work together to develop a bill that will assuage Americans' digital privacy worries.

The United States is behind many countries in developing comprehensive data privacy legislation.[380] This gap in regulation has fostered consumer digital privacy anxiety, allowed dangerous data breaches, and left the door open for confusing and conflicting state comprehensive data privacy laws that impose unnecessary costs onto businesses while providing a patchwork of data privacy rights to only a select few.[381] If Congress fails to develop a national privacy law, the patchwork quilt of state privacy regulations will only grow, and, ultimately, consumers will pay the price.[382]

CONCLUSION

The CCPA, while non-discriminatory both facially and as applied, goes beyond the scope of California's regulatory authority and amounts to unlawful regulation of interstate commerce. The CCPA runs afoul of the dormant Commerce Clause by reaching too far beyond its territorial boundaries and regulating activity that occurs wholly outside California's borders.[383] It further violates the dormant Commerce Clause by burdening interstate commerce in exchange for putative benefits that fail to justify the onerous costs.[384]

The Supreme Court deems that a state action regulates interstate commerce when it: (1) facially or effectively discriminates against out-of-state actors;[385] (2) fails the *Pike* balancing test;[386] (3) regulates conduct

[379] *Compare* S. 3456 (providing for explicit state preemption), *with* S. 2968 (enabling state laws to remain intact).

[380] *See supra* note 367 (listing just a few countries with comprehensive privacy laws).

[381] *See* 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 (noting that big data has become too large to regulate on a state-by-state level and that state-by-state privacy legislation leads to "inconsistent treatment of data" and "consumer confusion" about when their data is protected).

[382] *Id.*

[383] *Supra* Section III.C.

[384] *Supra* Section III.B.

[385] *See, e.g.*, Maryland v. Louisiana, 451 U.S. 725, 756 (1981) (finding that Louisiana's natural gas tax was invalid under the dormant Commerce Clause because it favored local interests).

[386] Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970) ("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.").

that takes place extraterritorially;[387] or (4) prompts inconsistent regulation across the nation.[388] By projecting California's sovereignty across state lines and unduly burdening interstate commerce, the CCPA meets the Court's definition of an impermissible state action and therefore violates the dormant Commerce Clause's implicit prohibition on state regulated interstate commerce.

The United States cannot allow one wealthy real-estate developer to singlehandedly shape the nation's approach to regulating digital privacy—no matter how well-meaning his intentions.[389] Alastair Mactaggart's CCPA is a complicated and cumbersome law that impermissibly amounts to regulating data privacy on a national scale.[390] The courts must strike down the CCPA as unconstitutional. However, lawmakers must heed the CCPA's call for stronger privacy protections. Congressional gridlock and partisan polarization seem to spell doom for any hope of a national privacy law.[391] If Congress refuses to act, the states will continue to pass confusing, complicated, and conflicting privacy legislation that will ultimately do more harm than good to businesses and consumers alike.

[387] *See, e.g.*, Healy v. Beer Inst., 491 U.S. 324, 336–37 (1989) (striking down a Connecticut price affirmation statute on the grounds that it set the price of beer in states other than Connecticut).

[388] CTS Corp. v. Dynamics Corp. of Am., 481 U.S. 69, 88 (1987) (noting that inconsistent regulations "adversely affect" interstate commerce).

[389] *See supra* Section I.B (discussing millionaire Alastair Mactaggart's significant role in developing the CCPA).

[390] *See supra* Section III (explaining that the CCPA violates the dormant Commerce Clause by imposing an undue burden on interstate commerce, by regulating extraterritorial conduct, and by prompting a patchwork of inconsistent privacy regulations).

[391] *See* Cameron F. Kerry & John B. Morris, *Preemption: A Balanced National Approach to Protecting All Americans' Privacy*, BROOKINGS INST. (June 29, 2020), https://www.brookings.edu/blog/techtank/2020/06/29/preemption-a-balanced-national-approach-to-protecting-all-americans-privacy [https://perma.cc/U82V-WNRP].