Hastings Science and Technology Law Journal

Volume 11
Number 1 *Winter 2020*

Article 4

Winter 2020

Who Should Regulate Data?: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws

Nicholas F. Palmieri III

Who Should Regulate Data?: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws

NICHOLAS F. PALMIERI III

Introduction

While companies were still reeling from passage of the European Union's General Data Protection Regulation (GDPR),[1] the California legislature decided to enact its own data protection[2] statute, the California Consumer Privacy Act of 2018 (CCPA).[3] While not nearly as comprehensive as the GDPR, the CCPA provides significant insight into the ongoing trend towards data protection which can be seen throughout the world and into how that trend is affecting laws within the United States.[4]

The CCPA was passed hastily by the California legislature in order to prevent an even more stringent ballot initiative from being passed.[5] As a result, it contained a myriad of uncertainties and faced significant

1. Regulation (EU) 2016/679, 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]. In fact, companies still have not even fully adjusted to the GDPR's stringent requirements and face fines for such failures. *See* Michael Mittel, *What We Can Learn From the GDPR's First Fines*, CMS WIRE (Feb. 14, 2019), https://www.cmswire.com/information-management/what-we-can-learn-from-the-gdprs-first-fines/.

2. Scholarship in this area refers, usually interchangeably, to both data privacy and data protection. This paper will simply use the term data protection to cover both terms, although there are some slight differences between the two concepts. *See* STEPHEN COBB, DATA PRIVACY AND DATA PROTECTION: US LAW & LEGISLATION 1 (2016).

3. CAL. CIV. CODE §§ 1798.100–.192 (West 2018) [hereinafter CCPA].

4. *See* Sarah L. Lode, Note, *"You Have the Data" . . . The Writ of Habeas Data and Other Data Protection Rights: Is the United States Falling Behind?*, 94 IND. L.J. SUPPLEMENT 41, 58–63 (2018).

5. *See* John Stevens, *California Consumer Privacy Act*, ABA (July 2, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/.

criticisms.[6] While some amendments are changing these issues,[7] they do not change the overall picture presented by the CCPA. Although it is a ground-breaking law which will have ramifications throughout the country, if not the world, the CCPA still requires scrutiny before it should be completely accepted and modelled by the rest of the nation.[8]

Six significant amendments have been passed by the California legislature and recently signed into law by the governor.[9] While this paper is not intended to go into great detail on each of them, this brief overview will help to put them into context and inform some analysis of the law. First, A.B. 25 provides exceptions for information related to human resource purposes of a business, including information about an applicant, information related to emergency contacts, and information to help distribute and administer benefits.[10] A.B. 874 broadens the definition of personal information to include any information which may *reasonably* capable of being associated with a particular person or household.[11] However, it also remotes from the definition any de-identified or aggregate consumer information.[12]

A.B. 1564 mandates companies to provide at least two means for customers to submit requests for information, including a toll-free phone

6. *See* Hogan Lovells, *California Consumer Privacy Act: The Challenge Ahead*, LEXOLOGY: CHRONICLE OF DATA PROTECTION (Sept. 12, 2018), https://www.lexology.com/library/detail.aspx?g=ac6d94a0-0b7d-41a4-8d76-7b6cfa5f4d8d.

7. *CCPA Amendment Tracker*, IAPP (Sept. 18, 2019), https://iapp.org/resources/article/ccpa-amendment-tracker/. The most relevant of these amendments will be discussed below, *see infra* Part 0.

8. As it stands, other states are already beginning to copy California. *See* Rachel R. Marmor, Maryam Casbarro, Monder Khoury, Nancy Libin, and Helen Goff Foster, *"Copycat CCPA" Bills Introduced in States Across Country*, DAVIS WRIGHT TREMAIN LLP (Feb. 8, 2019), https://www.dwt.com/blogs/privacy—security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou.

9. Hunton Andrews Kurth, *Majority of CCPA Amendment Bills Passed by California Legislature*, PRIVACY & INFO. SECURITY BLOG (Sept. 16, 2019), https://www.huntonprivacyblog.com/2019/09/16/majority-of-ccpa-amendment-bills-passed-by-california-legislature/; *see also* Deborah A. George, *California CCPA Update: Here's What Passed*, NAT'L L. REV. (Sept. 19, 2019), https://www.natlawreview.com/article/california-ccpa-amendment-update-here-s-what-passed.

10. *Id.*

11. *Id.*

12. *See* Angelica A. Zabanal, *California Consumer Privacy Act ("CCPA") Amendments One Step Closer to Passage*, DUANE MORRIS BLOGS (July 23, 2019), https://blogs.duanemorris.com/techlaw/2019/07/23/california-consumer-privacy-act-ccpa-amendments-one-step-closer-topassage/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.*""*

number and a website submission form.[13] At the same time, it grants an exception to businesses that only operate exclusively online can provide just an email address for customers to use in order to submit information requests.[14] A.B. 1146 provides (yet another) exception to a company's deletion requirement, allowing companies to keep data necessary for various possible warranties.[15]

A.B. 1355, perhaps the lengthiest amendment, has a few significant provisions. First, it clarifies that businesses need only inform customers that they may *request* certain specific information, instead of requiring disclosure of the actual information by the business.[16] It also allows for a business to require a verifiable consumer request before disclosing certain information, although it doesn't go into detail on what type of verification is allowed.[17] Finally, this amendment also clarifies the CCPA's anti-discrimination provision, switching the focus from the value provided to the business rather than the to the consumer.[18]

This paper will proceed in three parts. Part I will analyze the CCPA as it currently stands under a previously developed three-part framework: data stewardship, a balance of harms, and redressability[19] While the legislature is free to amend the CCPA further before it comes into effect on January 1, 2020, evaluating the law as is currently stands can provide insight into the minds of the California legislature as well as how companies within the United States as a whole are currently approaching data protection.

Part II will discuss potential constitutional challenges to the CCPA as well as arguments to overcome those challenges. In particular, this paper will look at two primary constitutional doctrines: first, the Dormant Commerce Clause,[20] and in particular how the prevalence of geolocation data affects this issue;[21] second, First Amendment issues.[22] Analysis of

13. Kurth, *supra* note 9.

14. *Id.*

15. *Id.*

16. *Id.*

17. *Id.*

18. *Id.*

19. Nicholas F. Palmieri III, Note, *Data Protection in an Increasingly Globalized World*, 94 IND. L.J. 297, 298–306 (2019). This three-part framework is itself derived from a five-part framework developed by Fred Cate for analysis of Big Data specifically. Fred H. Cate, *Big Data, Consent, and the Future of Data Protection*, *in* BIG DATA IS NOT A MONOLITH 3 (Cassidy R. Sugimoto, Hamid R. Ekbia & Michael Mattioli eds., 2016).

20. *See generally* Amy M. Petragnani, *The Dormant Commerce Clause: On Its Last Leg*, 57 ALB. L. REV. 1215 (1994).

21. *See* Tony Glosson, *Data Privacy in Our Federalist System: Toward an Evaluative Framework for State Privacy Laws*, 67 FED. COMM. L.J. 409, 420–32 (2015).

these doctrines suggests that the CCPA will likely have significant difficulties overcoming the challenges presented here, particularly because it provides little benefit in return for imposing significant burden on out-of-state actors.[23]

Finally, Part III will examine and summarize the previous spread of data breach notification laws throughout the United States,[24] and analogize it to the possible passage of laws similar to the CCPA amongst the other 49 states.

Ultimately, while the CCPA is a step in the right direction with regard to data protection, it ultimately falls short of having the same sweeping, protective scope that the GDPR has achieved. The CCPA does provide some very significant protections for consumers, but suffers from serious drawbacks as well. The law will face significant constitutional challenges, and likely spawn a number of similar, but distinct, laws that may be difficult (if not impossible) to comply with.

Evaluating the Current CCPA

Before analyzing whether the CCPA will survive constitutional challenges and spur the spread of similar laws throughout the country, one must first determine whether or not a law like the CCPA is even worthwhile. While objectively determining the "worth" of a data protection law is difficult, this paper will apply a three-part framework designed to analyze the function and efficacy of data protection laws during three main stages. First, the data stewardship element looks at the *collection* phase, that is, under what circumstances companies are allowed to collect personal data[25] in the first place, and the security requirements for storing that data once it is collected.[26] Second, the balance of harms element looks at the *use*

22. *See* Jane E. Kirtley, *The EU Data Protection Directive and the First Amendment: Why a "Press Exemption" Won't Work*, 80 IOWA L. REV. 639, 643–46 (1995).

23. *But see* Stephen J. Astringer, *The Endless Bummer: California's Latest Attempt to Protect Children Online is Far Out(side) Effective*, 29 NOTRE DAME J.L. ETHICS & PUB. POL'Y 271 (2015); E. Wesley Campbell, *But It's Written in Pen: The Constitutionality of California's Internet Eraser Law*, 48 COLUM. J.L. & SOC. PROBS. 583 (2015).

24. *See* Jill Joerling, *Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data*, 32 WASH. U. J.L. & POL'Y 467, 471–81 (2010); *see also* Daniel J. Marcu, *The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information*, 68 DUKE L.J. 555 (2018).

25. For the purposes of this paper, the term "personal data" describes any information that can be used to identify a single individual as well as data that refers to such an individual, without explicitly identifying that person. Robert Kirk Walker, Note, *The Right to be Forgotten*, 64 HASTINGS L.J. 257, 260 n.5 (2012).

26. Palmieri, *supra* note 19, at 297–99.

phase, namely how a company decides whether the risks of particular data processing outweigh the benefits of that processing.[27] Third, the redress element looks at the *problem* phase, examining what solutions are available to persons (or even organizations) whose data has been mishandled or misidentified.[28] None of these elements exist alone, and each depends on, informs upon, and influences the other two, making strict application of any single element in the framework a difficult task, though it helps to provide insight into individual aspects of a law which need improvement.

Data Stewardship

The data stewardship element has two main focuses. First, it considers under what circumstances a company may collect personal data. Currently, one of the primary ways that most countries allow for collection of personal data is via privacy policies, which obtain the consent of the consumer before personal data is collected and used. While this has become standard practice across multiple industries,[29] supposedly because it "place[s] the individual at the center of decision-making about personal information use," such consent is rarely actually "informed."[30] In reality, consumers rarely make themselves aware of the circumstances surrounding collection of their data, the nature of the data collected, or the uses to which their data will be put.[31] As a result, users often find themselves agreeing automatically to various clickwrap agreements, without taking any time whatsoever to consider the consequences of that consent.[32]

An additional problem with a consent-based model of data processing is that many websites operate on a "take-it-or-leave-it" basis.[33] Under such

27. *Id.* at 300–02.

28. *Id.* at 302–04.

29. James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 4–18 (2005).

30. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1660 (1999).

31. *Id.* at 1683; *see also* Neil Richards & Woodrow Harding, *The Pathologies of Digital Consent*, 97 WASH. U. L. REV. (forthcoming 2019).

32. *See* Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 466 (2006); *see also* Andrea M. Matwyshyn, *Privacy, the Hacker Way*, 87 S. CAL. L. REV. 1, 62 (2013). Clickwrap agreements, where a user must expressly consent to the agreement before using a website, should be distinguished from browsewrap websites, whereby "consent" is implied from continued use of a website, whose terms are not always enforceable. *See* Kathryn McMahon, *Tell the Smart House to Mind Its Own Business: Maintaining Privacy and Security in the Era of Smart Devices*, 86 FORDHAM L. REV. 2511, 2536 (2018).

33. *See* Richards & Harding, *supra* note 31, at 28–34 (discussing the concept, and illegitimacy, or coerced consent).

a model, users are confronted with the choice either to accept a website or company's collection of their personal data, or to go without using that service. In today's modern world, many Internet-based services are simply necessary to life, leaving consumers no choice but to "consent" to collection of their data or go without a necessary service in their lives.[34]

Second, this element considers how that data is stored and a company's duty to properly manage and protect any personal data in its possession (separate from how it may or may not use that data for any data processing). This is, in reality, the far more important focus when it comes to collection of personal data. As previously discussed, data collection based on consent has significant weaknesses. As such, consumers—who in their everyday lives have little time (and thus inclination) to worry about the potential risks of data processing, the categories of data collected, or sometimes even who is collecting their data[35]—would be far better protected by setting up a minimum standard of applies to all companies and upon which consumers may rely.[36] In this way, companies can be incentivized—in various ways—to set up proper infrastructure to protect personal data, rather than merely relying on user consent agreements to avoid liability for misuse or misallocation of personal data.[37]

Under the first consideration, the CCPA falls extremely short, especially when compared to laws like the GDPR. The CCPA contains no provisions which define the actual circumstances under which a company can collect personal data, nor does it define specific criteria which must be met in order for data collection to occur.[38] While the GDPR is far from perfect,[39] it at least allows for multiple circumstances by which a company can become legally authorized to collect personal data, beyond mere consent of users.[40] While the data stewardship element seeks definition of *more* than mere conditions for legal collection of data, having at least some predefined conditions gives minimal notice to (interested) users that their

34. Tanith Balaban, *Comprehensive Data Privacy Legislation: Why Now is the Time*, 1 CASE W. RES. J.L. TECH. & INTERNET 1, 24 (2009).

35. *See* Schwartz, *supra* note 30.

36. Palmieri, *supra* note 19, at 309.

37. *See, e.g.*, Jeff Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive Based System*, 19 CHAP. L. REV. 401 (2016) (suggesting a tax incentive which encourages proactive data security); *see also* Matwyshyn, *supra* note 32, at 48 (suggesting a new standard of "digital usability and quiet enjoyment" with respect to collection and storage of personal data).

38. CYNTHIA J. COLE & NEIL COULSON, BAKER BOTTS LLP, CALIFORNIA V. GDPR: COMPARE AND CONTRAST (2018).

39. Palmieri, *supra* note 19, at 307–8

40. GDPR, *supra* note 1, art. 6.

personal data could be collected and provides a moderately easily accessible means of determining exactly how and why their data was collected in the first place.

The CCPA's merits do not improve greatly when looking at the second focus of the data stewardship element. While it does mandate that a company which collects personal data keep track of various information—categories of data collected and sold, categories of sources of personal data, purpose of collection, and specific pieces of personal data collected[41]—there are no real baseline security measures that are mandated for companies which collect personal data. While some may argue that the market would adequately punish companies who do not properly protect personal data,[42] such *ex post facto* reliance fails to take into account one of the most basic considerations of data protection laws: to prevent the free dissemination (and thus misuse) of personal data in the first place. Because of the ease with which personal data can be spread across the globe as well as the ample harms that can arise from misuse of that data,[43] it is imperative that companies be incentivized, on the front-end, to prevent any possible data breaches, rather than merely being punished after the fact of a data breach, since gauging adequate compensation in the event of a data breach is very difficult.

The CCPA amendments, signed October 11th, 2019, [44] influence this element, but do not change the CCPA's overall outlook. While A.B. 874 might broaden the range of information that is covered by the CCPA, it does not address any of the underlying concerns which consumers should be concerned with. In addition, A.B. 25 weakens the data protection of the CCPA, since it gives employers significantly more freedom to collect and use the personal information of their employees. While true that the CCPA is focused at the protection of consumers, the fact that legislators have chosen to specifically exclude employees from the scope of some CCPA protections goes a long way towards showing that the CCPA is, at its heart, a data transparency bill rather than a data protection bill.

As such, the CCPA definitively fails the data stewardship element of this framework, since, beyond the most cursory tracking and recording of

41. CCPA § 1798.110(c).

42. *See, e.g.*, Mark Burdon, *Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 63 (2011).

43. *See generally* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737 (2018).

44. Jeewon Kim Serrato & Susan Ross, *And then There Were Five: CCPA Amendments Pass Legislature*, Data Protection Rep. (Oct. 14, 2019), https://www.dataprotectionreport.com/2019/10/california-governor-signs-all-5-ccpa-amendments.

personal data collected/sold, it provides essentially no guidance to (1) consumers with respect to the circumstances under which their personal data can be collected and (2) businesses with respect to minimum safeguards which they would need to implement in order to assure consumers that personal data will be adequately protected.

Balance of Harms

Once personal data has been collected, businesses are tasked with the difficult decision of what, exactly, they should (and oftentimes could) do with that data. For example, companies could (theoretically) choose to process that data themselves, sell the data to third parties, or simply store the data until a better opportunity presents itself. Accompanying all of these options, though, are potential harms, both to the consumers whose personal data is being used, and even to the company using that data. As such, any sufficient data protection law must lay out a system by which companies can balances the potential harms of data processing with the benefits and therefore determine the correct course of action to take.[45]

In enumerating these factors, a government must carefully balance the breadth of harms it chooses to specify, in order to avoid alienating potential businesses and consumers,[46] the benefits, to which companies themselves will almost always look at in as positive a light as possible, and thus could potentially give such benefits more weight than they are due.[47] This enumeration has the added benefit of allowing consumers themselves to correctly set their expectations, since it allows them to determine both the risks posed by collection and use of their personal data as well as the potential benefits a company stands to gain by use of that personal data, giving them leverage in potential negotiations.[48]

Of course, both the harms and benefits of data processing can depend heavily on the industry used, a fact implicit in the United States' current sector-specific approach to data protection.[49] Therefore another important consideration for any adequate data protection law is that it has in place appropriate safeguards to prevent, or at least regulate, cross-industry sharing of data. These safeguards prevent any type of "race to the bottom"

45. Palmieri, *supra* note 19, at 302.

46. *Id.* at 303.

47. *Cf.* ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW (2015).

48. *See* Ctr. for Info. Policy Leadership, The Role of Risk Management in Data Protection 13 (2014) https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_2_the_role_of_risk_management_16_february_2016.pdf.

49. *See* Burdon, *supra* note 42, at 83–86.

when it comes to data processing.[50] Without such a cross-industry shield, the least regulated industries would be free to sell sensitive personal data to more regulated industries who might otherwise have difficulty collecting such data in the first place.

Unfortunately, the CCPA again fails to adequately fulfill this element. In the first place, while it seems to implicitly recognize that personal data misuse can lead to various harm, it does nothing to address what these harms may be or how businesses can minimize them, although the CCPA is not alone in this failure.[51] There are likely various reasons for the California legislature's failure in the regard. First of all, the CCPA is specifically targeted to protect *consumers*, not quite to regulate business (although that is obviously a result of the law).[52] Therefore, the law should not be expected to set forth industry standards of safety so much as to empower citizens to protect their own personal data.

Second, the California legislature passed the CCPA relatively quickly, in order to prevent a similar measure from making its way to the California ballot, so legislators would be unlikely to have wanted to spend the time necessary to enumerate a list of myriad potential harms and benefits.[53] Finally, within the United States, exists the NIST Cybersecurity Framework, a nonbinding set of standards intended to help businesses maintain a certain minimum standard of data security.[54] The NIST Cybersecurity Framework suggests that businesses create their own system of balancing harms and benefits and provides minimal guidance to do so.[55]

Ultimately, the CCPA provides no guidance to businesses who deliberate whether on balance, certain processing activity is worth the risk. Without that guidance, businesses will likely continue to operate with

50. *See, e.g.*, Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE. J. INT'L L. 1 (2000).

51. *See* K.A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 1, 11 (2003).

52. Kevin F. Cahill, David J. Harris, Mark Browne, Hilary Bonaccorsi & Colleen Hespeler, *California Consumer Privacy Act: Potential Impact and Key Takeways*, 30 INTELL. PROP. & TECH. L.J. 11, 11 (2018).

53. *See* 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/.

54. NAT'L INST. OF STANDARDS AND TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2018).

55. *See* Palmieri, *supra* note 19, at 325–26.

impunity, using or selling personal data with little oversight, resulting in data abuse.[56]

Redressability

The final element of the three-part framework—redressability—examines what procedures and safeguards are in place to ensure consumers have access to personal data held by companies, which means exist to effectively respond to improper use of their data, and the ability to correct erroneously collected or stored data.[57]

Primarily existing to provide transparency to consumers, the CCPA excels at addressing redressability as it contains several provisions that allow consumers to not only see what data is held by companies, but also whom the data has been sold to and the use of the data.[58] The sweeping scope of the CCPA provisions allow consumers to determine which companies have purchased, collected, or used their personal data, at a relatively low cost and within a reasonable period of time. These provisions serve as a useful tool for consumers to ensure the safety and privacy of their data.

In addition to its ample transparency provisions, the CCPA also provides two additional means of redress. First, the CPPA grants consumers the right to request companies to delete,[59] any personal data that the company holds. While this right is incredibly important, within the context of the CCPA it loses some of its force. First of all, the CCPA allows for nine exceptions to the right to delete, which allow a business to retain personal data even after receiving a "verifiable request" for deletion.[60] One of these exceptions is most likely to be the source of most problems for consumers; the "Internal Use" exception[61] allows for noncompliance with a deletion request whenever the data is being used purely for internal uses that are aligned with the consumer's expectations. Under this exception, a business could, in theory, remain free to retain any personal data which it was using internally for its own processing, in spite of any deletion requests it receives.

56. *But see* Palmieri, *supra* note 19, at 325 (suggesting that, despite a lack of actual data protection regulation, the FTC has stepped forward as a *de facto* watch dog for data protection in the United States).

57. Palmieri, *supra* note 19, at 304–05.

58. CCPA §§ 1798.110, 1798.115, 1798.130.

59. *Id.* § 1798.105.

60. *Id.*

61. *Id.* § 1798.105(d)(7).

The right to deletion also loses much of its force when one realizes that it merely controls what a single company does. While a verifiable request for deletion does require a business to "direct any service providers" to also delete personal data,[62] there is no follow up necessary or assurance required on the part of the business. As far as a single business is concerned, once it passes along the request its obligation is met. This places a huge burden on the consumer, who must now follow up with every single company to whom their personal data has been sold to ensure their compliance with the deletion request. Increasing this cost essentially ensures that consumers will be unable or unwilling to properly see to the deletion of their personal data, resulting in mass proliferation of personal data which they will be almost powerless to stop.[63]

But the right to deletion is not a citizen's only means of redress. The CCPA also guarantees a right for consumers to "opt-out" of sale of their information to third parties.[64] Unlike the right to deletion, this provision is not riddled with myriad exceptions and a business is required to provide notice of sale to any third party as well as notice of the right to opt out of similar sales in the future.[65] In general, once a consumer has given direction to a business not to sell their personal data, a business is bound by that request.[66] However, opt out rights are far from an ideal solution.[67] Similar to the issues of informed consent discussed earlier, opt out provisions require a certain level of attention and proactive action on the part of consumers.[68] Creating this extra work for the *consumer* shifts the costs of data processing back to the consumer, rather than the business, who is in the best position both to manage personal data and to prevent its sale. Ideally, data protection laws should not unduly burden consumers with protection of their own data, rather they should focus on placing the burden of proper data protection on businesses, who often stand to gain the most from proper data processing techniques.[69]

62. *Id.* § 1798.105(c).

63. *See* Palmieri, *supra* note 19, at 305.

64. CCPA § 1798.120.

65. *Id.* § 1798.120(b).

66. *Id.* § 1798.120(c).

67. *See* Ryan C. Williams, *Due Process, Class Action Opt Outs, and the Right Not to Sue*, 115 COLUM. L. REV. 599, 615–16 (2015).

68. *See* Richard Lawne & Yuli Takatsuki, *CCPA Blog Series, Part 3: Confused over opt-out rights? You're not alone*, FIELDFISHER (Apr. 16, 2019), https://privacylawblog.fieldfisher.com/2019/ccpa-blog-series-part-3-confused-over-opt-out-rights.

69. *See* Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling,* 98 NW. U. L. REV. 63, 133–37 (2003).

Again, the CCPA amendments provide only minimal relief in this regard. A.B. 1564 does create additional guarantees that consumers will be able to determine what data companies have, but A.B. 1355 reverses the benefit of that slightly by putting further burdens on the consumers. First, consumer requests must be specific for what data they are seeking, creating an additional hurdle which they must overcome. In addition, for certain data, companies are able to demand a verified request by the consumer. This requirement, again, puts an extra burden on consumers and will likely stifle attempts by any but the most determined consumers to understand who has their data.

Looking at the CCPA as a whole, it is clear that it functions primarily as a transparency law. Doing little to regulate how businesses collect personal data or what they may do with that data once it is collected, the law focuses greatly on allowing consumers to determine what personal data is being held by various businesses. While the law does, in theory allow for consumers to both request deletion of particular data and the opt out of the sale of their data, these rights are severely limited by both exceptions to those rights as well as the creation of undue burdens on consumer to exercise those rights. Ultimately, though, while the CCPA is not perfect and is not nearly as comprehensive as the GDPR, it is a step in the right direction and American consumers are likely to desire such a transparency law to be active in their everyday lives.

Potential Constitutional Challenges to the CCPA

Now that the CCPA has been analyzed on its own, this paper will address particular constitutional challenges most likely to target California's new law. Before analyzing those challenges, though, it is important to consider *who* would bring those challenges in the first place. The first primary challenger would be the Federal government itself. Either because the government wishes to enact its own federal law or because it simply doesn't wish for states to regulate the area of data protection, the federal government is currently the most likely to target the CCPA in an attempt to invalidate it. The second, less likely, challengers, would be large businesses, who do not wish to comply with the new regulation. However, the types of large, multinational corporations with the resources to truly challenge the CCPA are also already subject to the (much more stringent) provisions of the GDPR.[70] Therefore, from a publicity point of view, it is much more useful for large companies to now support the CCPA, since

70. *How Google, Amazon, Facebook, and More are Addressing GDPR*, LINEATE (Mar. 23, 2018), https://lineate.com/how-google-amazon-facebook-and-more-are-addressing-gdpr/.

they are already under harsher restrictions within the European Union and support of the CCPA will show consumers that these companies truly care about protecting personal data.[71]

Moving to the actual constitutional challenges now, the first constitutional doctrine to be levied against the CCPA is likely to be the Dormant Commerce Clause (DCC). The primary purpose of the DCC is to prevent the states from creating significant barriers to interstate trade in the absence of action by Congress.[72] While the Age of the Internet has made it much more prevalent for state laws to have effects in different areas,[73] that does not mean that all state regulations are preempted by the DCC. The second constitutional challenge to the CCPA will likely come in the form of a First Amendment challenge. While regulations that specifically target consumers with special interests, in particular minors, are often constitutional,[74] since the CCPA targets all consumers, restriction on commercial speech in that context faces harsher obstacles.[75]

The Dormant Commerce Clause

Under the Supreme Court's precedent, the primary purpose of the Dormant Commerce Clause (DCC) is to prevent state laws which discriminate against out-of-state actors.[76] Laws which facially discriminate against out-of-state actors are presumptively invalid.[77] However, if the law

71. *See* Andrea O'Sullivan, *Sundar Pichai: Google Supports American Data Privacy Law*, REASON (Dec. 18, 2018), https://reason.com/archives/2018/12/18/sundar-pichai-goog le-supports-an-america; *see also* Nicole Lindsey, *Why the Tech Industry is Pushing for a Federal Privacy Law*, CPO (Oct. 18, 2018), https://www.cpomagazine.com/data-privacy/w hy-the-tech-industry-is-pushing-for-a-federal-privacy-law/; *see also 24 Tech Companies Back CCPA Amendment to Make It Stronger: Privacy for All Act of 2019*, SPREADPRIVACY (Apr. 16, 2019), https://spreadprivacy.com/ccpa-privacy-for-all-act/ (arguing that companies have begun to show support for a single national data protection law within the United States because they would rather comply with a single nationwide law than fifty individual state laws).

72. Petragnoni, *supra* note 20, at 1215-16.

73. *See* American Library Ass'n v. Pataki, 969 F. Supp. 160, 169-70 (S.D.N.Y. 1997) (suggesting that the "nature" of internet communications is interstate).

74. *See* Campbell *supra* note 23, at 584–85.

75. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 563–566 (1980) (laying out a four-part analysis for determining the constitutional of commercial speech regulations).

76. CTS Corps. V. Dynamics Corp. of Am., 481 U.S. 69, 87 (1987).

77. *See* Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 788–89 (2001); *see also* Astringer, *supra* note 23, at 279 (stating that facially discriminatory state laws are "per se invalid"); *but see* Dean Milk Co. v. City of Madison, Wis., 340 U.S. 349 (1951) (suggesting that strict scrutiny is the proper standard for facially

is not facially discriminatory, then the law is subject to the so-called *Pike* Balancing test, which considers four questions: (1) does the statute regulate evenhandedly?; (2) Does the statute effectuate a legitimate purpose; (3) Are its effects on interstate commerce incidental?; (4) Is the burden created clearly in excess in relation to the local putative benefits?[78] Additionally, regardless of the *Pike* balancing test, state legislation can still be invalidated where the "practical effect of the regulation is to control conduct beyond the boundaries of the State."[79]

Applying the *Pike* test to the CCPA, it would likely be able to pass constitutional scrutiny. Regarding the first question, the CCPA clearly regulates evenhandedly. It would apply identically to both out-of-state and in-state actors and does not treat data protection differently based on the location of that data, rather focusing on protection of California based *consumers*. With respect to the second question, the protection of personal data is certainly a legitimate state interest.[80] Especially here, where the legislature has specifically set out that a right to privacy is fundamental to all Californians.[81] The CCPA does encounter some issues when considering the third question, whether its effects are incidental. The effects here are more than merely incidental, they would in fact be a primary part of the legislation. Companies seeking to do business in California, whose massive economy most companies would wish to utilize, must comply with this act, meaning effects on interstate commerce would likely be primary, not incidental.[82] The final question would also weigh heavily against the CCPA, since burden imposed by the law might be found to be clearly excessive in relation to its benefits. As discussed earlier, there are actually very few real benefits that the CCPA creates for California consumers. While transparency in data collection and processing is an important goal, it truly imparts very few actual benefits on consumers without also

discriminatory state laws). An argument might be made that any state law attempting to regulate the internet is facially discriminatory, such an argument is beyond the scope of this paper and will not be discussed at length.

78. Pike v. Bruce Church, Inc., 397 U.S. 137(1970); *see also* Petragnani, *supra* note 20, at 1218–19; *see also* Astringer, *supra* note 23, at 279–80.

79. Healy v. Beer Inst., Inc., 491 U.S. 324, 336 (1989); *see also* Campbell, *supra* note 23, at 598–99.

80. *See* Glosson, *supra* note 21, at 418 (arguing courts are generally very deferential to a state's determination of legitimate interests of its residents).

81. Cal. Civ. Code § 1798.10 § 2.

82. City of Philadelphia v. New Jersey, 437 U.S. 617, 623–24 (1978) (stating courts have given some leeway to this question in the past, since significant incidental burdens on interstate commerce may be unavoidable where the state is attempting to safeguard the safety of its people, as would be the case here).

providing a greater means of control over that data. As such, the CCPA burdens companies inside and outside California by requiring: the recording, storage, and protection of various personal data; forcing companies, large and small, to collect, respond to, and act on various consumer requests for deletion or access; and the tracking of sales or transfer of personal so that companies can properly forward deletion requests to the appropriate third-parties.[83] This significant burden could easily be found to be excessive when compared with the relatively paltry benefit conferred to consumers.

Additionally, beyond the *Pike* balancing test, there is a third test which courts may apply when considering the DCC. As stated by the court in *Healy*, state legislation can also be invalidated where the "practical effect . . . is to control conduct beyond the boundaries of the State."[84] Here, it could be argued by those opposed to the legislation that the actual effect of the CCPA is to regulate the conduct of businesses outside California. Since the CCPA is primarily focused on protecting consumers and applies to most companies which "do business in California,[85]" a large percentage of the companies that will be affected and must alter their conduct may be located outside the state's boundaries. This reflects inherent problems with the internet. First, since the internet is global, it is accessible from anywhere,[86] allowing consumers in California to access the website (and in turn data collecting sphere) of businesses that may not have anticipated serving Californians. Second it is usually difficult, if not impossible, for users (and in turn companies) to identify the location of visitors to various websites or online services.[87] As such, in order to be safe, most companies would have to implement procedures designed to comply with the CCPA.

As a caveat to the second problem, the use of geolocation data and technologies has become prevalent by online businesses. Such technologies allow a company to determine a visitor's location, so in theory it is possible to know whether or not a visiting consumer is from California, and whether or not the company will be required to comply with the CCPA. However, this technology is rife with issues. First, assessment of geolocation technologies requires collection of particular data in the first place, not only requiring companies to still comply with the CCPA (albeit to a lesser degree) but also bringing forth further constitutional issues, since forcing

83. *See supra* Part I.

84. Healy v. Beer Inst., Inc., *supra* note 79, at 336.

85. Cahill et al., *supra* note 52, at 12.

86. *See* Campbell, *supra* note 23, at 598–99.

87. *See* Campbell, *supra* note 23, at 598–99.

use of geolocation is discriminatory on its face.[88] The use of geolocation data also adds an extra burden to smaller companies who do not already have the infrastructure in place to implement geolocation technologies, since now they will be forced between implementing these strict CCPA guidelines for all customers or putting into place a potentially expensive new procedure for determining user locations.[89]

The First Amendment

Under the standard set forth by the Supreme Court in *Central Hudson Gas & Electric v. Public Service Commission of New York*, regulation of commercial speech is governed by a four-factor test:[90] (1) the regulated speech concerns lawful activity, (2) the regulation is supported by a substantial government interest, (3) the regulation directly advances the interest, and (4) the regulation is not more extensive than necessary to serve that interest.[91] The court in *Sorrell v. IMS Health* later heightened the scrutiny for regulations concerning personal data,[92] but even under this less exacting standard the CCPA will encounter significant hurdles in this area.

The first factor poses little issue. The collection and use of personal data is certainly a lawful, though often criticized, behavior. Under current U.S. law, collection of a consumer's personal data after obtaining consent (even if that consent is not properly informed[93]) is certainly legal, especially considering the low threshold for valid consent.[94] The CCPA should also have no issue with the second factor since, as discussed above, protection of personal data is certainly a substantial government interest. Although targeted at a broad range of consumers, a general privacy interest has been recognized throughout the United States.

The third factor is where the CCPA will run into serious issues. The CCPA's main focus is transparency, and while important, transparency by itself does little to directly advance the government's interest in protecting personal data. While it is true that the CCPA contains other means of

88. Glosson, *supra* note 21, at 421–23.

89. Glosson, *supra* note 21, at 427–32.

90. 447 U.S. 557 (1980).

91. *Id.* at 564.

92. 564 U.S. 552 (2011).

93. *See generally* Peter H. Schuck, *Rethinking Informed Consent*, 103 YALE L.J. 899 (1994).

94. *See, e.g.*, Christopher Hopkins, *Florida Court Rules on Enforceability of "Browsewrap" vs. "Clickwrap" Website Terms and Conditions*, BUS. ADVOCATE (Feb. 17, 2017), https://mcdonaldhopkins.com/Insights/Blog/Litigation-Trends/2017/02/17/Florida-court-rules-on-enforceability-of-browsewrap-vs-clickwrap-website-terms-and-conditions.

redress for consumers,[95] such means are relatively ineffective in their current form. This means that the only true direct advancement of data protection the CCPA contains are its transparency provisions.[96]

Finally, with regard to the fourth factor, the CCPA again falls short. It broadly applies to essentially all businesses, imposing rather strict punishments and fines for failure to comply in addition to requiring implementation what could be relatively burdensome infrastructure requirements. All of this, though, doesn't properly serve the government's interest, and to the minor amount that it does, overbroadly affects not only California businesses and consumers but also out-of-state actors.

Overall, when considering the issue of commercial speech, which in this situation is related to the use and sale of personal data, it would appear that the CCPA again fails to overcome the constitutional issue. Since the collection and sale of personal data is, generally, legal, businesses are free to use that information as they see fit and the CCPA does not narrowly tailor its solutions to fit within the confines of the Constitution.

The Spread of Data Protection Laws

Thus far, this paper has analyzed the CCPA in two distinct ways. First, it analyzed whether the CCPA as currently written provides adequate and desirable data protection. Although, under the three-part framework used, the CCPA shows clear deficiencies with regard to actually protecting consumer data. Second, this paper also analyzed potential constitutional challenges that the CCPA, in its current form, will likely face. Once again, the CCPA showed clear deficiencies, as there are very severe doubts as to whether or not it could withstand those constitution challenges.

Putting those two Parts aside, this Part will analyze how laws like the CCPA could potentially spread throughout the United States.[97] First, this Part will analyze how comparable laws, laws regarding data breach notification, spread throughout the United States after California spearheaded the effort. Next, this part will predict likely changes that would be made to the CCPA should the state choose to adopt similar legislation.

95. *See* CCPA §§ 1798.105, .120.

96. *Id.* §§ 1798.110, .115, .130.

97. For the moment, this paper ignores the question of whether or not consumers *want* a law like the CCPA to spread. It will take for granted (for this Part) that laws like the CCPA are desirable throughout the United States and proceed from there.

The Spread of Data Breach Notification Laws

Much like with the CCPA, California was the first state to enact a data breach notification law, S.B. 1386, in 2002.[98] Not long after this, the law was put to the test, as various companies were forced to disclose breaches of consumer data.[99] Under this law, a breach was defined as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information[100] maintained by the person or business."[101] In the event of a breach, notification must be provided promptly, in either writing or electronically.[102] Since passage of a data breach notification law by Alabama in 2018, all 50 states have passed their own data breach notification laws.[103]

Most of these laws are modeled after California's law, since California was the "pioneer,"[104] but many states have crafted specific differences into their laws as well.[105] While a comprehensive discussion of all the differences in data breach notification laws throughout all fifty states is beyond the scope of this article,[106] some of the major deviations will be explained as they will inform on possible deviations that states will take with respect to the CCPA.

The first major deviation from California S.B. 1386 is the categorization of what *type* of data must be subject to a security breach in

98. *See* CAL. CIV. CODE §§ 1798.29, 1798.80–.84 (West 2017).

99. Joerling, *supra* note 24, at 468–70 (2010) (describing disclosure of data breaches by various companies, including ChoicePoint, Bank of America, PayMaxx, DSW, and LexisNexis).

100. "Personal information" is itself defined as "an individual's first name or first initial and last name in combination with [their] . . . Social security number . . . [d]river's license number . . . credit or debit card number . . . [m]edical information . . . [h]ealth insurance information . . . [or] data collected through . . . an automated license plate recognition system." CAL. CIV. CODE § 1798.29(e) (West 2017).

101. CAL. CIV. CODE § 1798.82(d).

102. Joerling, *supra* note 24, at 472.

103. Caleb Saketh & Brooke Kahn, *State Data Breach Notification Laws: 2018 in Review*, COVINGTON: INSIDE PRIVACY (Dec. 31, 2018), https://www.insideprivacy.com/data-security/data-breaches/state-data-breach-notification-laws-2018-in-review/; *see also* DAVIS WRIGHT TREMAINE LLP, SUMMARY OF U.S. STATE DATA BREACH NOTIFICATION STATUTES (Mar. 26, 2018), https://www.dwt.com/files/Uploads/Documents/Publications/State%20Statutes/BreachNoticeSummaries.pdf.

104. Brandon Faulkner, *Hacking into Data Breach Notification Laws*, 59 FLA. L. REV. 1097, 1105 (2007).

105. Joerling, *supra* note 24, at 473.

106. *See generally* DAVIS WRIGHT TREMAINE LLP, *supra* note 103 (discussing the data breach notification laws of all fifty states).

order to trigger notification duties.[107] Under the California law, only data stored electronically is subject to notification requirements.[108] However, several states (including North Carolina and Hawaii) have expanded the requirement to non-electronic means of storage, including paper records.[109] This expansion of applicability has a major advantage over California's law: comprehensiveness. Particularly, in the Big Data context, data in the aggregate, even where individual pieces may be harmless, can easily be used to identify (and in turn harm) an individual.[110] Therefore, notification of breaches regarding a wider swath of data (though this may be more expensive)[111] helps to give notice to consumers whose (non-electronically stored) data has now been disseminated and which could, in combination with other freely available possibly also leaked data could result in harm to them.

The second major deviations that states have made from the California data breach notification law refer to the *exemption*s that are included within the law.[112] The most prominent exception[113] is for a breach of encrypted data.[114] States in general seem to assume that, so long as data in encrypted, a security breach involving that data need not be disclosed to the consumers whose data is encrypted. Unlike with anonymized data,[115] encrypted data is incredibly difficult (and in some cases practically impossible[116]) to crack without access to its encryption key.[117] But a second major exemption, not shared by all states, is an exemption for breaches which "[have] not resulted or [are] unlikely to result in harm" to the

107. Joerling, *supra* note 24, at 473.

108. CAL. CIV. CODE § 1798.29(a)-(d).

109. Joerling, *supra* note 24, at 474 n. 37.

110. *See* Paul Ohm, *Broken promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1704–06 (2010).

111. *See* Kathryn E. Picanso, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, *363,* 387 (2006).[DELETE]

112. Joerling, *supra* note 24, at 475.

113. *Id.* (clarifying that the most prominent exemption refers to all data breach notification laws and not just California Data Breach Notification laws).

114. *See, e.g.*, MASS. GEN. LAWS ch. 93H, § 1 (2007); *see also* N.Y. GEN. BUS. LAW § 899-aa (McKinney 2009).

115. *See Generally* OHM, *supra* note 104 (stating that anonymized data, in the aggregate, can be used to identify an individual).

116. Shubham Barot, *Why Hackers Can't Hack Encrypted Datas?*, QUORA (Apr. 20, 2016), https://www.quora.com/Why-Hackers-cant-hack-encrypted-datas.

117. Cassie Philips, *Is Encryption Enough To Protect Yourself?*, DATAMOTION (NOV. 11, 2016), https://www.datamotion.com/2016/11/encryption-enough-protect/.

affected individuals.[118] While, on its face, such an exemption would seem to make sense, when considered in the broader context of data protection, the exemption again exposes consumers to unnecessary risks.

While a single piece of data, on its own, may pose very little risk of harm, data in the aggregate (as previously discussed) can create a new and much more serious risk of harm.[119] Businesses simply cannot keep track of which various piece of personal data that already exist in cyberspace; therefore, they cannot accurately access the risk that breach of a single piece of innocuous data can cause since they don't know how that single bit of information may be aggregated with other information.[120] So allowing this exemption for pieces of data which a business has determined to be unimportant creates new risks, because now enough data could be released piecemeal by various businesses to cause consumer harm, while at the same time the consumers themselves are not made aware of *any* breaches, since each one on its own does not pose a significant risk.

The final major variation between state data breach notification laws is their enforcement mechanisms.[121] California's law, for example, allows a private right of action by individuals whose data has been subject to a security breach and who were not properly notified.[122] On the other hand, some states (like Florida) only allow for an administrative fine and do not create a separate, private right of action.[123] In the context of data breaches, though, where security breaches can affect hundreds of thousands (or even millions) of people,[124] the ability to bring a private cause of action is vital, especially the ability to bring a class action lawsuit.[125] Class actions are

118. Joerling, *supra* note 24, at 475.

119. *See* Ohm, *supra* note 110, at 1729–30.

120. *See* Nehf, *supra* note 29, at 22.

121. These differ significantly from the federal government's approach to enforcement, where the FTC has taken on a role as the de facto regulatory agency for cybersecurity. Marcus, *supra* note 17, at 579; *see also* GINA STEVENS, DATA SECURITY BREACH NOTIFICATION LAWS (2012).

122. CAL. CIV. CODE § 1798(b), (e).

123. Joerling, *supra* note 24, at 479.

124. *See* David McCandles, Tom Evans, Paul Barton & Stephanie Tomasevic, *World's Biggest Data Breaches & Hacks*, INFO. is beautiful, https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ (last updated Apr. 1, 2019); *see also* Jonathan Stempel, *Yahoo Strikes $117.5 Million Data Breach Settlement After Earlier Accord Rejected*, REUTERS (Apr. 9, 2019), https://www.reuters.com/article/us-verizon-yahoo/yahoo-in-new-117-5-million-data-breach-settlement-after-earlier-accord-rejected-idUSKCN1RL1H1.

125. Craig A. Newman, *The Next Big Thing: Data Breach Securities Class Action Litigation*, PATTERSON BELKNAP: DATA SECURITY LAW BLOG (Feb. 20, 2018), https://

important for two reasons. First, an individual consumer rarely has the resources to bring a suit on their own and oftentimes have mixed success in court.[126] Second, security breaches are inherently a class related harm. As previously mentioned, it is rare that a single individual's data is leaked, but usually on the order of hundreds of thousands of individuals. Allowing class action in the event of data breaches thus makes it significantly easier to establish the fact of injury, since it can build upon the aggregate experiences of an entire class.[127]

While these three deviations are particular to the data breach notification context, they can certainly help inform on how states may approach variations to data protection laws (like the CCPA) should they choose to adopt them in the future.

Potential Variations to the CCPA

As the last section (briefly) discussed, while all states have adopted similar data breach notification laws, there are a few significant variations between those laws which can make a huge difference to the proper protection of consumers' data.[128] There is little reason to suspect that states 'will not make similar deviations from data protection laws as those laws spread throughout the states.[129]

Regarding applicability of such laws, this is the area where one expects the least variation in state practice. While it is true that some data may still be stored on paper, in the modern world almost all data is stored electronically.[130] The CCPA specifically targets electronically stored data as well, since it is the location and transmission of such information that the law seeks to target. The ubiquity of such data storage has only increased since 2002, when the California data breach notification law was

www.pbwt.com/data-security-law-blog/the-next-big-thing-data-breach-securities-class-action-litigation.

126. *See, e.g.*, Katz v. Pershing, LLC, 806 F. Supp. 2d 452, 455 (D. Mass. 2011).

127. *See generally* Nicholas Green, *Standing in the Future: The Case for a Substantial Risk Theory of "Injury In Fact" in Consumer Data Breach Class Actions*, 58 B.C. L. REV. 287 (2017).

128. *See* Burdon, *supra* note 42, at 73–79.

129. In fact, some states have already begun consideration of data protection laws, so this spread may occur sooner than we imagine, though none have had the same fanfare as the CCPA. *See* JONATHAN G. CEDARBAUM, D. REED FREEMAN, JR. & LYDIA LICHLYTER, WILMERHALE, PRIVACY AND DATA SECURITY ALERT: STATES CONSIDER PRIVACY LEGISLATION IN THE WAKE OF CALIFORNIA'S CONSUMER PRIVACY ACT (2019).

130. *See Dittman v. UPMC*, 196 A.3d 1036, 1043 (Penn. 2018) (acknowledging that most data is stored electronically).

passed.[131] Therefore, there is no reason to expect the same deviation for *written* data that is seen in the data breach notification context.

Regarding exemptions, the second major state deviation for data breach notification laws and data protection laws face a very different set of risks and considerations. Unlike data breaches, where encryption can help protect individuals' data, in the data protection context, exceptions for encrypted data do not tackle the fundamental issue with improper collection and use. Even where data is encrypted, states should not (although they very well might) allow for the free sale and use of such personal data, not because of the risk to consumers, but rather because it violates the rights of consumers (regardless of encryption). The other major exemption which states might adopt is an exemption for *de minimis* data, which would again be trivial in a data protection context. The underlying purpose of the CCPA is to ensure transparency and (minimal) control of personal data. It is meant to allow for a consumer to know, correct, and if necessary, delete all personal data held by companies. Allowing for a *de minimis* exemption would essentially defeat the purpose since, apart from a few big players,[132] many companies only collect and use only relatively small amounts of data on their own and often use it in connection with other companies.[133]

The final deviation that state data protection acts will likely take regards enforcement. The CCPA, as it currently stands, only allows for a private right of action after notifying (and denial by) the State Attorney General.[134] Not only does this create an unnecessary delay, but it also allows for the Attorney General to essentially short-circuit potential claims by informing business who may be out of compliance of the potential lawsuit, which grants them a grace period to correct the conduct in order to escape liability. Should other states begin adoption of data protection laws, they should certainly not follow the CCPA's example. Instead, they should either implement administrative fine systems, which create punishments for

131. *See* Loren F. Selznick & Carolyn LaMacchia, *Cybersecurity Liability: How Technically Savvy Can We Expect Small Business Owners to Be*, 13 J. BUS. & TECH. L. 217 (2018).

132. *See, e.g.*, Aaron Brown, *The Amount of Data Facebook Collects from Your Photos Will TERRIFY You*, EXPRESS (Jan. 6, 2017, 12:12 PM), https://www.express.co.uk/life-style/science-technology/751009/Facebook-Scan-Photos-Data-Collection.

133. *See* Amy Talbot, *Infographic, Most Companies Are Collecting Data, But Aren't Using Big Data Solutions*, ZDNET (Sept. 1, 2017, 1:12 PM).

134. Although this requirement may soon be changing as California politicians seem to have realized the harm that could come of such a convoluted system. *See* Joseph J. Lazzarotti, Jason C. Gavejian & Maya Atrakchi, *California AG Announces Amendment to the CCPA*, NAT'L LAW REVIEW (Feb. 26, 2019).

each individual violation (with no actual grace period for exemption), or allow solely for private causes of action, without oversight from the Attorney General. Within the data protection context, class actions are much less important. Unlike data breaches, which almost always implicate a large number of consumers, data protection is a much more personal concern. The ability of a single individual to much more easily bring forth a claim against a company is vitally important—especially in combination with potential administrative fines for relatively simple to prove violations.

Conclusion

For the foregoing reasons, this paper comes to two primary conclusions. First, while the CCPA is a step in the right direction with regard to data protection within the United States, it still has a long way to go before it can adequately protect the personal data of consumers. As such, the law in its current form acts merely as a transparency law for Californian consumers and is truly not a system that consumers would want the country to adopt, at least as the law currently stands. Second, even if the law were to provide adequate safeguards, it could also face significant constitutional challenges. As the law currently stands, there is little certainty that it could overcome these challenges, although ultimately, it is difficult to say with certainty how such constitutional discussions would resolve themselves.

That being said, these critiques do not necessarily mean the end of the CCPA or of laws like it. Other states, following California's lead many still adopt data protection laws of their own. Following a similar trend as when the states adopted data breach notification laws, these data protection laws will likely contain the same broad principles as the CCPA but with some very important variations. While the deviations are important in the data breach context, they do not perfectly map onto a data protection context, but would still provide very important and necessary protections. These deviations, however, might also cause more problems than they solve, since they may put into place disparate requirements, making compliance with all laws incredibly difficult, and consequently leading again to Dormant Commerce Clause concerns should such laws be adopted throughout the country.[135]

135. *See* Marcus, *supra* note 17, at 575–80; *see also* Selznick & LaMacchia, *supra* note 125, at 224–29.

***