Loyola of Los Angeles Law Review

Volume 53 | Number 3 Article 7

Spring 5-1-2020

Untangling the Privacy Law Web: Why the California Consumer Privacy Act Furthers the Need for Federal Preemptive Legislation

Jordan Yallen

UNTANGLING THE PRIVACY LAW WEB: WHY THE CALIFORNIA CONSUMER PRIVACY ACT FURTHERS THE NEED FOR FEDERAL PREEMPTIVE LEGISLATION

*Jordan Yallen**

I. INTRODUCTION

Between January 2013 and July 2018, six billion records were stolen in data breaches in the United States alone.[1] During this period of just over five and a half years, each American, on average, was a victim of data theft nineteen times.[2] Further, seven million data records[3] are compromised daily, and 85 percent of worldwide identity theft occurs in the United States.[4] Consequently, these data breaches cost businesses an average of $3.26 million per breach.[5]

As a response to cybersecurity threats running rampant across the globe, the European Union (EU) passed the General Data Protection Regulation (GDPR and the "Regulation"). While the Regulation remains in its infancy—having been implemented on May 25, 2018, after a two-year transitionary period—it represents a paradigm shift as to how modern privacy law will aim to combat data breaches and oversee data processing.[6] Most notably, California scurried in the EU's footsteps when former Governor Jerry Brown signed the

* J.D. Candidate, May 2020. Loyola Law School, Los Angeles. Thank you to *Loyola of Los Angeles Law Review* for the time and effort dedicated to editing this Note, and to Selene Houlis and the Executive Board for your immense dedication to the Law Review. I owe my utmost gratitude to Professor Thomas Riordan, whose guidance and patience over the past three years has been invaluable. Finally, I am eternally thankful to my parents and my sister, Lindsay, for inspiring me daily and being my biggest fans.

1. Rob Sobers, *The World in Data Breaches*, VARONIS (July 16, 2018), https://www.varonis.com/blog/the-world-in-data-breaches.

2. *See id.* With 326 million people, the ratio of data breaches to Americans is 19:1. *See id.*

3. Data records consist of information that can be traced to an individual such as a person's name, email address, physical address, IP address, or financial information.

4. Sobers, *supra* note 1.

5. *Id.*

6. *See, e.g.*, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*, OFFICIAL J. EUR. UNION L. 119, at 1 (2016) [hereinafter GDPR].

California Consumer Privacy Act of 2018 (CCPA and the "Act") in June 2018.[7]

Three months after the CCPA's passage, the first amendment to the Act was passed to address flaws and provide enforcement date flexibility of up to six months beyond the January 1, 2020, effective date.[8] While seven additional amendments to the CCPA were ultimately passed,[9] the United States Government Accountability Office, National Telecommunications and Information Administration,[10] Congress, and the some of the largest United States-based technology and telecommunications companies ("Big Tech") are pushing to preempt the widely criticized Act.[11] These bodies also fear that more states will follow in California's footsteps and implement new privacy laws of their own, potentially thrusting over fifty unique laws upon businesses.[12] Federal preemptive legislation would quell disruption to business and innovation that a flood of state laws would likely produce.[13]

This Note analyzes the current overall landscape of privacy law and proposes a framework for national privacy law regulation. Part II illustrates the complex timeline of how the GDPR and CCPA came to be. Part III examines existing privacy law with a focus on the GDPR and CCPA. Part IV addresses flaws in the CCPA, while Part V provides a proposal for federal preemptive legislation that uses the GDPR as its framework.

---

7. Mark G. McCreary, *The California Consumer Privacy Act: What You Need to Know*, LAW.COM: N.J. L.J. (Dec. 1, 2018, 10:00 AM), https://www.law.com/njlawjournal/2018/12/01/the-california-consumer-privacy-act-what-you-need-to-know; *see also* California Consumer Privacy Act of 2018, 2018 Cal. Legis. Serv. ch. 55, § 2(i) (West) (codified at CAL. CIV. CODE §§ 1798.100–1798.198).

8. McCreary, *supra* note 7; *see* Consumer Protection—Privacy, 2018 Cal. Legis. Serv. ch. 735 (S.B. 1121) (West) (amending the CCPA); *see also* California Consumer Privacy Act of 2018, 2018 Cal. Legis. Serv. ch. 55, § 2(i) (West).

9. *See CCPA Amendment Tracker*, IAPP, https://iapp.org/media/pdf/resource_center/CCPA_Amendment_Tracker.pdf. (last updated Oct. 16, 2019); *see also* Letter from Californians for Consumer Privacy to Ed Chau, Assemblymember, Cal. State Assembly (Jan. 16, 2019), https://drive.google.com/file/d/1wtjjlPnCYO9jltLLtjbjOqeOB5i28mhz/view.

10. *See* Nat'l Telecomm. & Info. Admin., *Developing the Administration's Approach to Consumer Privacy*, 83 FED. REG. 48,600, 48,600 (2018).

11. Jessica Guynn, *Amazon, AT&T, Google Push Congress to Pass Online Privacy Bill to Preempt Stronger California Law*, USA TODAY (Sept. 26, 2018, 5:17 PM), https://www.usatoday.com/story/tech/news/2018/09/26/amazon-att-google-apple-push-congress-pass-online-privacy-bill-preempt-stronger-california-law/1432738002/.

12. *Id.*

13. *Id.*

II. A TIMELINE OF EXISTING PRIVACY LAW: HOW THE GDPR AND CCPA CAME TO BE

This Note primarily focuses on the GDPR and CCPA because they are the most comprehensive and relevant examples of privacy law to date. State laws such as Illinois's Biometric Information Privacy Act, Massachusetts's Standards for the Protection of Personal Information of Residents of the Commonwealth, and New York's Cybersecurity Requirements for Financial Services Companies represent more concentrated efforts to regulate the privacy of residents within states.[14] Similarly, federal regulations such as the Gramm-Leach-Bliley Act and Health Insurance Portability and Accountability Act of 1996 represent federal laws that address the privacy of Americans in the banking and healthcare industries, respectively.[15] The following addresses the overall timeline for how the GDPR and the CCPA came to fruition, beginning with early-internet privacy law and ending with each law's most recent developments at the time of writing.

A. GDPR Background: A Thoroughly Vetted and Calculated Plan

The GDPR replaced Directive 95/46/EC (the "European Data Protection Directive"), which the EU adopted in 1995.[16] Among other principles, the European Data Protection Directive was based on seven principles for protecting EU citizens.[17] First, data subjects[18] needed to

14. *See* Jordan Yallen & Kevin D. DeBré, *Data Protection Laws Are Here, but What Do They Mean for California Businesses?*, 2018 BUS. L. NEWS, no. 4, at 14, 16–17 (2018); *see also* 740 ILL. COMP. STAT. ANN. 14/5 (West 2008) (regulating the usage, storage, and deletion of biometric identifiers such as fingerprints and facial geometry); 201 MASS. CODE REGS. § 17.05 (2010) (regulating ownership and licensing of personally identifiable information of Massachusetts residents); N.Y. COMP. CODES R. & REGS. tit. 23 § 500.00 (2017) (regulating the practices of financial institutions).

15. Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999) (regulating the banking industry and disclosure of nonpublic personal information); Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104–191, 110 Stat. 1938 (regulating healthcare, including data collection and privacy).

16. Margaret Rouse, *EU Data Protection Directive (Directive 95/46/EC)*, WHATIS.COM, https://whatis.techtarget.com/definition/EU-Data-Protection-Directive-Directive-95-46-EC (last updated Jan. 2008); *The History of the General Data Protection Regulation*, EUR. DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en# (last visited Feb. 23, 2020).

17. Rouse, *supra* note 16.

18. For the purposes of this Note, "data subjects" will refer to any individual whose data is collected by an entity.

be given notice about the collection of their data.[19] Second, data subjects were required to be informed about who was collecting their data.[20] Third, requirements for data storage were established to avoid possible identity theft or misuse.[21] Fourth, the transfer of information that could identify a particular person ("Personal Data") was forbidden without consent of the data subject.[22] Fifth, data subjects were allowed to view their collected data and rectify inaccuracies.[23] Sixth, collected data was only allowed to be used for the purposes that had been stated.[24] Seventh, collectors of Personal Data could be held liable for failing to protect the personal information of data subjects.[25]

After nearly sixteen years, a movement toward a more "comprehensive approach on personal data protection in the EU" gained momentum, resulting in a "proposal to strengthen online privacy rights" in January 2012.[26] For the next two years, political support for a privacy law overhaul grew, culminating with the European Parliament passing the GDPR with an overwhelming 621 out of 653 possible votes.[27]

Between the passage of the GDPR in March 2014 and the GDPR going into effect on May 25, 2018, the EU took numerous steps aimed to ensure the new law's successful implementation.[28] Throughout 2015, the Council of the European Union ("Council"),[29] the European Data Protection Supervisor (EDPS),[30] and the European Commission[31] negotiated terms of the GDPR, finally reaching an

19. Rouse, *supra* note 16.
20. *Id.*
21. *Id.*
22. *Id.*
23. *Id.*
24. *Id.*
25. *Id.*
26. *The History of the General Data Protection Regulation*, *supra* note 16.
27. *Id.*
28. *Id.*
29. The Council "sets the EU's policy agenda, traditionally by adopting 'conclusions' during European Council meetings which identify issues of concern and actions to take." *The European Council*, COUNCIL EUR. UNION, https://www.consilium.europa.eu/en/european-council (last visited Feb. 23, 2020).
30. The EDPS serves as the EU's "independent data protection authority." *About*, EUR. DATA PROTECTION SUPERVISOR, https://edps.europa.eu/about-edps_en (last visited Feb. 23, 2020).
31. The European Commission participates in the proposal and implementation of laws within the EU. *See What the European Commission Does in Law*, EUR. COMMISSION, https://ec.europa.eu/info/about-european-commission/what-european-commission-does/law_en (last visited Feb. 23, 2020).

agreement on December 15, 2015.[32] Six weeks later, the Article 29 Working Party[33] published "an action plan for the implementation of the GDPR."[34]

Finally, on April 27, 2016, the "GDPR was published in the Official Journal of the European Union as Regulation 2016/679" to supersede the European Data Protection Directive after a two-year transitional period.[35] Not only did this period allow for companies to work toward complying with the new regulation, but it provided an opportunity for the EU to establish the infrastructure needed for such a massive undertaking and ample time to make adjustments.[36]

B. The California Consumer Privacy Act's Timeline: From Wine and Pizza to Partisan Politics

1. A Voter's Vision and a Last-Minute Triage

As the GDPR neared implementation, Alastair Mactaggart, "a real estate developer and investor based in San Francisco,"[37] became curious about why consumer privacy was such a hot button issue.[38] A casual conversation over "wine and pizza" with a Google engineer sparked Mr. Mactaggart's mission to reform privacy law in California.[39] Rather than dismissing a lighthearted question about the extent of Google's knowledge of Mr. Mactaggart, his friend answered that "there was plenty to worry about," explaining, "If people really

32. *The History of the General Data Protection Regulation*, *supra* note 16.

33. The Article 29 Working Party contributed to privacy policymaking in the EU and was replaced by the European Data Protection Board after the GDPR went into effect. *See, e.g.*, *The Article 29 Working Party Ceased to Exist as of 25 May 2018*, EUR. COMM'N (Nov. 6, 2018), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492.

34. *The History of the General Data Protection Regulation*, *supra* note 16.

35. *Id.*; *EU General Data Protection Regulation—Background*, DLA PIPER, https://www.dlapiper.com/en/norway/focus/eu-data-protection-regulation/background (last visited Feb. 23, 2020).

36. *See The History of the General Data Protection Regulation*, *supra* note 16.

37. About page of Alastair Mactaggart, IAPP, https://iapp.org/about/person/0011a00000rimIxAAI/ (last visited Feb. 23, 2020).

38. *About Us*, CALIFORNIANS CONSUMER PRIVACY, https://www.caprivacy.org/about-us [https://web.archive.org/web/20191030202813/https://www.caprivacy.org/about-us] (last visited Oct. 30, 2019).

39. Nicholas Confessore, *The Unlikely Activist 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?rref=collection%2Fsectioncollection%2Fmagazine&action=click&contentCollection=magazine&region=rank&module=package&version=highlights&contentPlacement=2&pgtype=sectionfront.

knew what we had on them . . . they would flip out."[40] This "simple conversation" drove Mr. Mactaggart to determine that the amount of information Big Tech knew about individuals "was a problem that was getting much, much worse" and "that under current law, consumers were powerless."[41]

Soon after, Mr. Mactaggart concluded that the most efficient form of legislation was a California ballot initiative. He proceeded to establish Californians for Consumer Privacy, an organization to aid the pursuit of his initiative.[42] Rather than using the GDPR as precedent for the initiative, Mr. Mactaggart sought transparency by paralleling the consumer-business relationship with the citizen-government relationship protected through Freedom of Information requests.[43] In addition to transparency, Mr. Mactaggart and Californians for Consumer Privacy drafted the initiative based on two other principles: consumer control and business accountability.[44]

In the fall of 2017, Californians for Consumer Privacy submitted their ballot initiative and began collecting signatures in December 2017.[45] The organization—with Mr. Mactaggart at the helm—"spent nearly $3.5 million" over the course of two years merely in an effort to get the initiative on the ballot, ruffling the feathers of Big Tech and innumerable lawmakers along the way.[46] Facebook, Google, Comcast, Verizon, and AT&T led the fight, preparing to spend an estimated "$100 million to fight the measure" that they deemed "unworkable."[47]

In January 2018, the Committee to Protect California Jobs was formed to oppose the ballot initiative with Big Tech providing immediate and substantial funding.[48] While Mr. Mactaggart and Californians for Consumer Privacy were gathering signatures, the Committee to Protect California Jobs quickly became a vessel waging

40. *Id.*
41. *About Us*, *supra* note 38.
42. *See id.*
43. *Id.*
44. *Id.*
45. *Id.*
46. 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.
47. *Id.*; Confessore, *supra* note 39.
48. Confessore, *supra* note 39. The initial funding was comprised of "six-figure contributions from Facebook, Google and three of the country's biggest internet service providers: Comcast, Verizon and AT&T." *Id.*

war on the initiative.[49] The newly formed organization's leaders sought to prevent the measure from "limiting [Californians'] choices, hurting [California] businesses, and cutting [California's] connection to the global economy."[50] In addition to large corporations, they surrounded themselves with political specialists and law enforcement, claiming that the "'poorly-written-by-a-multi-millionaire's measure' . . . would make it harder for cops to foil kidnappings or quickly track down criminals like the San Bernardino shooter."[51]

As soon as Mr. Mactaggart and Californians for Consumer Privacy were "reminde[d] of how small [they] were," news of the Cambridge Analytica scandal broke, heavily tilting the scales in favor of the initiative.[52] Facebook became the focus of a legal, political, public relations, and media nightmare.[53] It "was forced to acknowledge that Cambridge had used voters' own Facebook data to" coerce voters through "deploying powerful 'psychographic' voter profiles."[54] Mark Zuckerberg appeared in front of Congress in April 2018, thrusting Facebook and the lack of privacy regulation further into the spotlight.[55] In order to survive the media feeding frenzy and preserve what was left of its image, Facebook and Mr. Zuckerberg admitted their "big mistake," announcing they would no longer fund the Committee to Protect California Jobs.[56]

Overnight, Mr. Mactaggart's canvassing campaign blossomed as the Cambridge Analytica news story gained momentum, leading Californians for Consumer Privacy to submit 629,000 signatures in the beginning of May 2018, officially qualifying the initiative for California's statewide election in November 2018.[57]

---

49. *Id.*

50. Comm. to Protect Cal. Jobs, *Statement by the Committee to Protect California Jobs on Submission of Signatures for Internet Regulation Ballot Measure*, PR NEWSWIRE (May 3, 2018, 4:06 AM), https://www.prnewswire.com/news-releases/statement-by-the-committee-to-protect-california-jobs-on-submission-of-signatures-for-internet-regulation-ballot-measure-300642494.html.

51. Confessore, *supra* note 39.

52. *Id.*

53. *Id.*

54. *Id.*

55. *Id.*

56. *Id.*

57. *About Us*, *supra* note 38; Confessore, *supra* note 39.

Despite acquiring nearly twice as many signatures as necessary, the proposal failed to garner support from key advocacy groups.[58] Over the next fortnight, Facebook and politicians separately strove to implement "an alternative to Mactaggart's proposal."[59] Unsatisfied with Facebook's counterproposal, Mr. Mactaggart began listening to offers for a compromise from California Senator Robert Hertzberg and Assemblymember Ed Chau.[60] Their proposed deal was contingent upon Mr. Mactaggart withdrawing the measure from the November ballot if the state legislature passed "a reasonable privacy bill by June 28, the legal point of no return for formally withdrawing [the] initiative."[61]

With weeks to spare to write an entire bill, Assemblymember Chau, the "designated . . . chief negotiator on a potential deal between industry and privacy advocates," spearheaded the undertaking.[62] He previously authored Assembly Bill 375 ("AB 375"), a bill that failed, was rewritten, and failed again.[63] Once again, Assemblymember Chau "resurrected his legislation, making a modified AB 375 the vehicle for a potential compromise with Mactaggart."[64]

Amid opposition from politicians and Big Tech, and only a few days before the withdrawal deadline, Assemblymember Chau and Senator Hertzberg tried to find a middle ground between parties on opposite ends of the privacy law spectrum.[65] California legislators preferred to keep a real estate developer out of lawmaking, with many declining to upset their tech-based financiers; Big Tech refused to consider a bill with the initiative's private right of action; and Mr. Mactaggart needed to see a bill with enforcement to shield consumers.[66] Yet, politicians and Big Tech dreaded "punting . . . a poorly drafted ballot measure to voters" and, despite his relative

58. *See* Confessore, *supra* note 39 ("The Electronic Frontier Foundation, the storied advocacy group based in San Francisco, did not endorse Mactaggart's proposal. Neither did the American Civil Liberties Union or Common Sense Kids Action, an influential group also headquartered in San Francisco, that has pressed for restrictions on the collection of children's data.").

59. *Id.*

60. Adler, *supra* note 46.

61. *Id.*; Confessore, *supra* note 39.

62. *See* Confessore, *supra* note 39.

63. *Id.* AB 375's second incarnation was "a bill that would have required cable companies and other internet service providers to obtain customers' consent before selling their browsing history and other sensitive personal data" in 2017. *Id.*

64. *Id.*

65. *Id.*

66. *Id.*

wealth, Mr. Mactaggart recognized an impending war of attrition against "a trillion-dollar Goliath" should the initiative come to a statewide vote.[67]

Although it seemed to be an impossibility in mid-June, Assemblyman Chau and Senator Hertzberg finalized a Mactaggart-approved version of AB 375 on Monday, June 25, 2018.[68] Facebook, leading Big Tech, faced a seemingly insurmountable quandary three days before the bill's withdrawal deadline as they maintained that both the bill and the initiative would stunt innovation and harm business.[69] If Mr. Mactaggart failed to pull the initiative, Big Tech—still in the midst of the Cambridge Analytica fallout—would be forced to engage in an ugly advertising campaign.[70] Further, if the initiative passed a statewide vote, "California lawmakers would need to muster an almost unobtainable supermajority to amend it."[71] However, even if the voters sided with Big Tech, persistent privacy advocates could propose another initiative the following year.[72] Ultimately, on June 26, 2018, Facebook and Big Tech laid down their arms, backing AB 375 "because it prevent[ed] the even-worse ballot initiative from becoming law," bought the industry time,[73] and was amendable.[74]

Once Assemblyman Chau and Senator Hertzberg had appeased Mr. Mactaggart and Big Tech, the compromise needed to "pass both houses and be signed by Gov. Jerry Brown" before June 28, 2018, for Mr. Mactaggart to withdraw the initiative.[75] The day of the deadline, both houses passed the legislation by an overwhelming majority, seemingly out of fear of being "on the wrong side of [the] issue" as Mr. Mactaggart watched from the respective galleries.[76] That same day, Governor Brown signed AB 375 into law, signaling an end for Mr. Mactaggart and Californians for Consumer Privacy's battle;

67. Adler, *supra* note 46.
68. Confessore, *supra* note 39.
69. *Id.*
70. *Id.*
71. *Id.*
72. *Id.*
73. It would not go into effect until January 1, 2020 at the earliest. *Id.*
74. *Id.*
75. Ben Adler, *Internet Privacy Deal Nears as Initiative Qualifies for California's November Ballot*, CAP. PUB. RADIO (June 26, 2018), http://www.capradio.org/articles/2018/06/26/internet-privacy-deal-nears-as-initiative-qualifies-for-californias-november-ballot [https://www.capradio.org/116719].
76. Confessore, *supra* note 39.

however, Governor Brown's signature spurred tech lobbyists across the country to start sharpening their axes.[77]

2. Big Tech's Two-Pronged Approach to Fight the California Consumer Privacy Act

The passage of AB 375, officially known as the California Consumer Privacy Act, marked the opening of a year-and-a-half-long window for the CCPA's "opponents to try to water the bill down or lobby for federal legislation to preempt it" before it went into effect on January 1, 2020.[78] In addition to Big Tech, the United States Congress, and several agencies joined the push to preempt the CCPA.[79] Meanwhile, the first of several amendments to clarify the CCPA, Senate Bill 1121 ("SB 1121"), was signed by Governor Brown within three months of the Act's passage, further fueling opponents' stance that the rushed bill was poorly written and impracticable.[80] Facebook, post-Cambridge-Analytica scandal, continued to concede that regulating consumer privacy was necessary.[81] The rest of Big Tech joined Facebook in advocating for a massive overhaul of the bill while simultaneously lobbying for federal preemptive legislation.[82]

In California, Big Tech and lawmakers met at the bargaining table once again to address "a law riddled with drafting errors and unresolved issues."[83] Big Tech countered privacy advocates, including the Electronic Frontier Foundation and the American Civil Liberties Union, as they pushed to further strengthen the CCPA by limiting data mining and expanding consumers' private right of action.[84] In total, nineteen Assembly and Senate bills modifying the CCPA were proposed.[85] The subject matter for these bills ranged from a "data

77. *See* Tyler Whitney, *Heavyweight Privacy Battle: California Legislators vs. Tech & Telecom Giants*, 96 DENV. L. REV. 176, 176 (2019).

78. *Id.*

79. *See* Confessore, *supra* note 39.

80. *See, e.g.*, Yallen & DeBré, *supra* note 14, at 18; Confessore, *supra* note 39; Comm. to Protect Cal. Jobs, *supra* note 50.

81. *See* Zack Whittaker, *Silicon Valley Is Terrified of California's Privacy Law. Good.*, TECHCRUNCH (Sept. 19, 2019, 9:00 AM), https://techcrunch.com/2019/09/19/silicon-valley-terrified-california-privacy-law; Confessore, *supra* note 39.

82. *See, e.g.*, Whittaker, *supra* note 81.

83. Tony Romm, *California Adopted the Country's First Major Consumer Privacy Law. Now, Silicon Valley Is Trying to Rewrite it.*, WASH. POST (Sept. 3, 2019, 8:26 AM), https://www.washingtonpost.com/technology/2019/09/02/california-adopted-countrys-first-major-consumer-privacy-law-now-silicon-valley-is-trying-rewrite-it.

84. *Id.*

85. *CCPA Amendment Tracker*, *supra* note 9.

broker registry," proposed by Assembly Bill 1202 ("AB 1202"), to entirely new legislation to replace the CCPA proposed by Assembly Bill 1760, the Privacy for All Act of 2019 (PAA).[86] Despite garnering "support of more than 30 privacy groups," most notably the American Civil Liberties Union of California,[87] the PAA stalled in committee.[88] Ultimately, California's new governor, Gavin Newsom, signed AB 1202, along with six other CCPA-related proposals, on October 11, 2019.[89] The Electronic Frontier Foundation responded to the signed amendments by claiming victory for privacy advocates after "provisions of [the] bills" supported by Big Tech failed to "make it through the legislature" despite a push on behalf of "technology giants . . . in the last days of the legislative session."[90]

The day before Governor Newsom signed seven of the CCPA's eight amendments, California's Attorney General, Xavier Becerra, released draft regulations for the CCPA.[91] "The Attorney General's draft regulations . . . are notable because they change and expand businesses' obligations under the CCPA in several key ways.[92] The draft regulation consists of seven articles that run 24 pages in length and relate to nearly every provision of the law."[93] Before becoming official, the draft regulations will be "subject to public comment and potential amendment."[94]

On the preemption front, fifty-four Big Tech chief executive officers signed an open letter to Congress urging for "a comprehensive consumer data privacy law that strengthens protections for consumers and establishes a national privacy framework to enable continued

86. *Id.*

87. Jazmine Ulloa, *California Has Become a Battleground for the Protection of Consumer Privacy Rules*, L.A. TIMES (Mar. 11, 2019, 12:05 AM), https://www.latimes.com/politics/la-pol-ca-california-privacy-law-battles-20190311-story.html.

88. *CCPA Amendment Tracker*, *supra* note 9.

89. *See id.*; Alysa Zeltzer Hutnik et al., *CCPA Update: California Governor Signs Seven Amendments to the CCPA*, ELECTRONIC FRONTIER FOUND. (Oct. 13, 2019), https://www.eff.org/deeplinks/2019/09/thanks-helping-us-defend-california-consumer-privacy-act.

90. Hutnik, *supra* note 89.

91. *See, e.g.*, Sarah A. Sargent & Andrew J. Schlidt III, *CCPA Alert: California Attorney General Releases Draft Regulations*, NAT. L. REV. (Oct. 14, 2019), https://www.natlawreview.com/article/ccpa-alert-california-attorney-general-releases-draft-regulations.

92. *See infra* Part III.B.3 for a discussion of the substance of the draft regulations.

93. Alexander Bilus et al., *CCPA Amendments and Draft Regulations Provide Some Clarity, Some Uncertainty, and Numerous Compliance Obligations*, JD SUPRA (Oct. 18, 2019), https://www.jdsupra.com/legalnews/ccpa-amendments-and-draft-regulations-51077.

94. *Id.*

innovation and growth in the digital economy."[95] While "[t]here [was] a congressional consensus that a patchwork of state data privacy laws is not efficient," regulation became a partisan issue.[96] Roughly one year before the CCPA's effective date, a national privacy law looked eminent as the White House National Economic Council, Commerce Department, and National Telecommunications and Information Administration appeared in agreement with Big Tech.[97] However, the legislation's momentum petered out after the White House failed to produce a "roadmap for protecting consumer data, and some key officials involved in the effort . . . left with no replacements announced."[98] Without direction from the administration, the Senate Commerce, Judiciary, and Banking Committees "staked claim to aspects of the privacy debate."[99]

At the time of writing, none of the committees were able to reach an agreement as the 2019 legislative calendar came to an end.[100] Senators on both sides of the aisle have expressed dismay over "Congress [] missing its 'critical window to legislate,'" calling the legislative delay, "'embarrassing' and 'disgraceful.'"[101] Failure to reach a resolution preventing the CCPA from going into effect on January 1, 2020, was caused by more than a lack of organization and unnecessary delay, however.[102] Three issues have plagued progress in Congress: (1) whether reform on a federal level should preempt a hodgepodge of state laws or establish a floor for data protection; (2) whether the Federal Trade Commission should be "the main federal agency that oversees corporate privacy practices"; and (3) whether consumers should have a private right of action against corporations

95. Letter from Business Roundtable to Mitch McConnell, Majority Leader, U.S. Senate, et al. (Sep. 10, 2019), https://s3.amazonaws.com/brt.org/BRT-CEOLetteronPrivacy-Finalv2.pdf.

96. Marisa A. Trasatti & Sean M. Fox, *Ready or Not, the Data Privacy Revolution Is Here*, IN-HOUSE DEF. Q., Summer 2018, at 20, 20; *see also* Lauren Feiner, *Two Silicon Valley Congresswomen Propose a New Federal Agency to Enforce Online Privacy Rights*, CNBC (Nov. 5, 2019, 2:25 PM), https://www.cnbc.com/2019/11/05/reps-lofgren-and-eshoo-propose-online-privacy-act.html ("Federal legislation that preempts state law would presumably be much easier for tech companies that operate in many regions to comply with since it could require they adhere to one general standard.").

97. *See, e.g.*, John Hendel, *'Embarrassing': Congress Stumbles in Push for Consumer Privacy Bill*, POLITICO (July 12, 2019, 5:51 PM), https://www.politico.com/story/2019/07/12/congress-consumer-privacy-bill-1582540.

98. *Id.*

99. *Id.*

100. *Id.*

101. *Id.*

102. *Id.*

for violations.[103] While congressional committees attempt to address these issues, two congresswomen from Silicon Valley proposed a new enforcement agency in the Online Privacy Act,[104] and Mr. Mactaggart launched a new ballot initiative for 2020.[105] Unsatisfied with the amended CCPA and threatened by new technologies that have "evolved in ways that . . . threaten[] our democracy," Mr. Mactaggart submitted the California Privacy Rights Act on November 13, 2019.[106] As of March 2020, "several . . . pieces of federal legislation" have been introduced, each "vying to create an overarching, federal data-privacy framework."[107] One such example, The Consumer Data Privacy and Security Act of 2020 (CDPSA), was presented by Senator Jerry Moran, the Chairman of the Senate Commerce Subcommittee on Consumer Protection.[108] The expressly preemptive CDPSA "integrates themes from the CCPA and GDPR" while "learning from the shortfalls of the current framework of privacy laws" and "attempts to strike a balance between the protections afforded to consumers . . . and costs of compliance."[109]

III. STATEMENT OF EXISTING LAW

This Part substantively examines the GDPR and CCPA as it stands at the time of writing. The analysis begins with a thorough examination of the GDPR's foundational principles, compliance protocols, consumer rights, and initial enforcement. Because this Note argues for federal preemptive legislation based on the GDPR in lieu of the CCPA, this Part surveys the Act's substance while emphasizing its critiques in Part IV.

103. *Id.*

104. *See* Feiner, *supra* note 96; *see also* Hendel, *supra* note 97.

105. Alastair Mactaggart, *A Letter from Alastair Mactaggart, Board Chair and Founder of Californians for Consumer Privacy*, CALIFORNIANS CONSUMER PRIVACY (Sept. 25, 2019), https://www.caprivacy.org/post/a-letter-from-alastair-mactaggart-board-chair-and-founder-of-californians-for-consumer-privacy.

106. *Id.*

107. *See, e.g.*, Gregory M. Kratofil, Jr. & Elizabeth Harding, *Federal Privacy Legislation Update: Consumer Data Privacy and Security Act of 2020*, NAT. L. REV. (Mar. 14, 2020), https://www.natlawreview.com/article/federal-privacy-legislation-update-consumer-data-privacy-and-security-act-2020.

108. *Id.*

109. *Id.*

A. GDPR Substance

1. Who, What, Where, and When: Understanding Personal Data, Processing, and the GDPR's Scope

A central focus of the GDPR is to protect any information that either directly or indirectly identifies a particular person ("Personal Data").[110] The Regulation recognizes data such as a person's name, address, email, IP address, identifying number (i.e., social security number or driver's license), and geolocation as Personal Data.[111] Further, the GDPR places additional emphasis on protecting "special categories of personal data."[112] This "sensitive data" is highly regulated; without an exception—such as explicit consent for specified purposes—companies are prohibited from processing "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."[113]

Processing of Personal Data consists of "any operation or set of operations which is performed on personal data . . . such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, [and] use," among other activities manipulating data manually or automatically.[114] When processing data, legal entities or individuals are considered either "controllers" or "processors."[115] Controllers "determine the purposes and means of the processing of personal data," while processors "process personal data on behalf of the controller."[116]

The GDPR applies to the processing of Personal Data by controllers and processors where: (1) a controller or processor's "establishment [is] located within the EU" ("Establishment Criterion"); or (2) a controller or processor's "offering of goods or services" is within the EU or it monitors the behavior "of data subjects

110. GDPR, *supra* note 6, art. 4(1) (defining Personally Identifiable Information as "personal data").
111. *See id.*
112. *Id.* recital 10.
113. *Id.* art. 9(1), recital 10.
114. *Id.* art. 4(1).
115. *See id.* art. 4.
116. *Id.* art. 4(7), (8).

who are in the EU," but the controller or processor is located outside the EU ("Targeting Criterion").[117] This Section examines each criterion and the elements needed under both in order for controllers, processors, and consumers to be within the GDPR's territorial scope.

a. Establishment criterion

Under the Establishment Criterion, the location of an entity's "establishment" concerns the physical location of the controller and processor, not where the processing occurs.[118] In order to determine whether a controller or processor has an establishment in the EU, "the degree of stability of the arrangements and the effective exercise of activities in the EU" are taken into consideration "in light of . . . the economic activities and the provision of services concerned."[119] Generally, controllers are subject to comply with the GDPR under the Establishment Criterion whether they are headquartered in the EU or merely have a minor physical presence such as a satellite office in the EU.[120] Even a "single employee or agent . . . may be sufficient to constitute a stable arrangement if that employee or agent acts with a sufficient degree of stability" under the Establishment Criterion.[121]

Because the Establishment Criterion is concerned with the physical location of the controller and processor, an EU-based controller that processes Personal Data of non-EU residents in non-EU countries is within the GDPR's territorial scope if the processing is conducted in the EU.[122] However, if the processing is conducted outside of the EU, the degree of establishment is considered too far removed to be within the Establishment Criterion, and therefore falls outside of the GDPR's territorial scope.[123] The degree of establishment is also too great if a non-EU based controller

117. *Id.* art. 3(1), (2).

118. EUROPEAN DATA PROT. BD., GUIDELINES 3/2018 ON THE TERRITORIAL SCOPE OF THE GDPR (ARTICLE 3)—VERSION FOR PUBLIC CONSULTATION 4 (2018), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf [hereinafter *Guidelines 3/2018*].

119. *Id.* at 5.

120. *Id.* at 4–7.

121. *Id.* at 5.

122. *Id.* at 8.

123. *See id.* at 9–10. However, the processing may still fall under the Targeting Criterion, making the controller or processor fall within the GDPR's territorial scope. *Id.*

exclusively processes Personal Data of non-EU residents in non-EU countries, regardless of whether or not the processor is EU based.[124]

b. Targeting criterion

Failure to satisfy the Establishment Criterion does not preclude controllers or processors from the GDPR's territorial scope. If the controller or processor is not considered to be established in the EU, they may still satisfy the Targeting Criterion and be subject to GDPR compliance. The two-part test for the Targeting Criterion is as follows: (1) "the processing relates to personal data of data subjects who are in the EU"; and (2) the processing "relates to the offering of goods or services or to the monitoring of data subjects' behaviour in the EU."[125]

The Targeting Criterion is not restricted to EU citizens; it encompasses any data subject present in the EU.[126] Irrespective of where the controller and processor are located, the first prong of the Targeting Criterion focuses on where the data subject's information originates.[127] Hence, if the processed data is generated within the EU, it satisfies the first prong of the test.[128]

In order to satisfy the second prong of the Targeting Criterion test, the information being processed must be a result of one of two elements: (1) the offering of goods or services; or (2) the monitoring of data subjects.[129] Both elements consist of a controller or processor targeting data subjects in the EU, but "mere accessibility of . . . [a] website . . . is insufficient to ascertain" the intent to target data subjects.[130] In order to have the intent to target data subjects through offering of goods or services, the controller or processor "envisages offering services to data subjects in one or more Member States in the Union."[131] Beyond direct solicitation, envisaging can be proven through various factors such as a website's language and currency options or "the mentioning of customers or users who are in the

124. *Id.* at 10–11.

125. *Id.* at 13.

126. *Guidelines 3/2018*, *supra* note 118, at 13.

127. *See id.* at 12–14. If an EU citizen resides in a non-EU country and a non-EU based business processes information of that individual, barring activities that would satisfy other elements of the Targeting or Establishment Criteria, the processing does not fall within the territorial scope of the GDPR. *Id.* at 14.

128. *See id.* at 12–14.

129. GDPR, *supra* note 6, art. 3.

130. *Guidelines 3/2018*, *supra* note 118, at 15 (citing GDPR *supra* note 6, recital 23).

131. *Id.* (citing GDPR *supra* note 6, recital 23).

Union."[132] However, the GDPR specifically notes that data subjects are not required to purchase any goods or services to be considered targeted.[133] Further, the second element of the second prong of the Targeting Criterion test is satisfied by a "broad range of [behavioral] monitoring activities" including tracking a data subject's behaviors on the internet and geolocation from a smartwatch.[134] While the requisite intent for monitoring a data subject's behavior is ambiguous, the targeting generally results in reuse and profiling for marketing or analytics purposes.[135] If a controller or processor is not considered established in the EU but satisfies the Targeting Criterion, they may be required to appoint an EU based representative.[136]

2. Compliance Standards: Protocols, Procedures, and Principles of GDPR Compliance

Controllers and processors within the GDPR's scope must have specific mechanisms in place in order to process Personal Data in compliance with the Regulation. Controllers and processors must receive a data subject's consent; must have measures in place to properly process, store, and remove a data subject's Personal Data; and may be required to designate data protection officers.

a. Consent

Acquiring Personal Data to process requires that a controller first receive the data subject's consent. The GDPR emphasizes that consent "must be clear, concise and not unnecessarily disruptive."[137] Consent consists of an "affirmative act establishing a freely given, specific informed and unambiguous indication of the data subject's agreement to the processing of [their] personal data."[138] This affirmative action may consist of "ticking a box when visiting [a] website . . . or another statement or conduct which clearly indicates . . . the data subject's acceptance of the proposed processing of his or her personal data."[139]

132. *Id.*
133. *Id.* at 14.
134. *Id.* at 18.
135. *See id.*
136. *See*, *e.g.*, Yallen & DeBré, *supra* note 14, at 15 (stating that "a representative in the EU" is required "unless the 'processing . . . is occasional' and does not consist of any sensitive 'special categories of data'").
137. GDPR, *supra* note 6, recital 32.
138. *Id.*
139. *Id.*

In other words, the GDPR demands that individual data subjects must know to what they are agreeing when checking a box for each agreement.[140]

For children, the GDPR provides an additional tier of protection. As a default, a parent or guardian must provide consent for children under the age of sixteen for online services.[141] However, EU member states have the discretion to decrease the parental consent threshold to as low as thirteen years of age.[142]

b. Data retention and storage

When consent is provided, not only must the purposes for which the data is collected be abundantly clear to the data subject, but the processing must also remain within the constraints of those purposes.[143] The GDPR prohibits processing Personal Data "in a manner that is incompatible with those [original] purposes"[144] and requires erasure of Personal Data when it is "no longer necessary in relation to" fulfilling those original purposes.[145] In order to comply with the GDPR's data retention requirements, controllers and processors are forced to adopt policies for handling data and procedures for adhering to the Regulation's standards. The "implementation of the appropriate technical and organisational measures" are necessary "in order to safeguard the rights and freedoms of the data subject."[146] In addition to controllers and processors implementing guidelines and mechanisms to properly store and erase data, they must also have the external and internal abilities to comply with data subjects exercising their rights.

140. Generally, these consist of Terms of Use Agreements or Privacy Policies when creating an account or making a purchase online. It is a violation if boxes on consent forms come pre-checked or if checking a single box corresponds to agreeing to several agreements. *Id.*

141. *Id.* art. 8(1).

142. *Id.* While the consent protocols and privacy rights of children are a central focus to the GDPR and other privacy laws, further discussion of privacy law in relation to children is beyond the scope of this Note.

143. *Id.* art. 6(1).

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

145. *Id.* art. 17(1)(a).

146. *Id.* art. 5(1)(e). These measures include the anonymization and pseudonymization of Personal Data, however, further analysis of these principles and their procedures is beyond the scope of this Note. *See, e.g.*, *id.* recital 26.

c. Data protection officers

Depending on a business's activities, GDPR compliance may entail the designation a specific person, a data protection officer, to be responsible for the Regulation's standards.[147] Controllers and processors are required to appoint a data protection officer when: (1) "a public authority or body" processes data; (2) a controller or processor's "core activities . . . require regular and systematic monitoring of data subjects on a large scale"; or (3) a controller or processor's "core activities . . . consist of processing" sensitive Personal Data as described in Part III.A.1.[148] The following summarizes the three activities that mandate the naming of data protection officers.

First, "a public authority or body" concerns government entities "carrying out functions of public administration," with the exception of courts.[149] This is a much more concrete description than the other two classes that require data protection officers. Both remaining categories of activities triggering the need to appoint a data protection officer rely on the meaning of "core activities."[150] "Core activities" are the main intentions of a controller's or processor's business endeavors.[151] This definition sheds light on the concept of processing sensitive Personal Data as a core activity of a controller or processor, yet the second classification's concept of "regular and systematic monitoring of data subjects on a large scale" remains elusive. The European Data Protection Board (EDPB) adopted guidelines for determining what constitutes these activities.[152] The EDPB's standard considers "all forms of tracking and profiling" in relation to the magnitude of the processing.[153] To determine whether

147. A data protection officer may be a "dedicated position within the organization" or outsourced to a third-party "[a]s long as the data protection officer can fulfill the obligations to inform, advise, and monitor a company's compliance with the GDPR." Yallen & DeBré, *supra* note 14, at 15.

148. GDPR, *supra* note 6, art. 37. The GDPR also specifically includes Personal Data pertaining to criminal records as part of the third classification. *Id.* art. (1)(c).

149. *Id.* art. 37(1)(a); *Public Task*, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task (last visited Feb. 23, 2020).

150. *See Data Protection Officers*, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/ (last visited Feb. 23, 2020).

151. *Id.*

152. *Id.*

153. *Id.*

processing is on a large scale . . . the following factors [are taken] into consideration:

- the numbers of data subjects concerned;
- the volume of personal data being processed;
- the range of different data items being processed;
- the geographical extent of the activity; and
- the duration or permanence of the processing activity.[154]

While controllers and processors that do not fall into one of the three categories described above are not mandated to designate a data protection officer, they may choose to do so in order to navigate ambiguities within the GDPR.[155] While appointing a data protection officer may serve as an additional layer of GDPR compliance, the role is regulated by statutory standards whether its implementation was required or at the election of the business.[156]

3. Rights Granted by the GDPR

Data subjects within the territorial reach of the GDPR are granted specific rights. The Regulation aims to protect consumers by creating policies and rights so that data subjects may exert control over how their information is used. The GDPR grants the following individual rights: (1) the right to be informed; (2) the right of access; (3) the right of portability; (4) the right to rectification; (5) the right to erasure; (6) the right to object; (7) the right to restrict processing; and (8) the right to object to automated decision-making.

a. Right to be informed

Due to the GDPR's deeply rooted emphasis on transparency, it prioritizes keeping consumers informed about what data is collected and how it is used so data subjects may exert specified rights over their data's usage.[157] Under the GDPR, the following information must be available to data subjects at the time their Personal Data is collected: (1) the purposes for which the information is collected; (2) the length

154. *Id.*

155. *Id.*

156. *Id.* The scope of data protection officers' duties is beyond the scope of this Note. See *id.*, for a summary of the statutory requirements surrounding data protection officer appointment.

157. *Right to Be Informed*, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed (last visited Feb. 23, 2020).

of time it is stored; and (3) the additional parties with whom it is shared.[158] Further, controllers must provide additional information at that time "to ensure fair and transparent processing" such as the existence of the data subject's various rights under the GDPR and contact information for the controller and their representatives.[159] Controllers must disclose this information in a clear and comprehensive nature, which often takes the form of a privacy policy on a website.[160]

b. Right of access

The GDPR provides a right for data subjects to access their Personal Data.[161] This allows data subjects to confirm whether their Personal Data is being processed and, if so, to obtain copies of their records.[162] Controllers are required to provide a copy of the data being processed free of charge but "may charge a reasonable fee" for additional copies.[163] The right of access also tasks processors with providing additional resources for data subjects such as information about the safeguards in place, "the source of the data, where it was not obtained directly from the individual," and the criteria for determining how long data will be stored.[164] All of the information provided to data subjects must be presented in a clear and concise manner that is easily accessible.[165] The GDPR does not specify protocols for which data subjects are to make requests, so they may be made in writing or verbally.[166]

158. *Id.*; GDPR, *supra* note 6, art. 13(1).

159. GDPR, *supra* note 6, art. 13(2).

160. *See id.* art. 13(1); *see also* LAURA JEHL ET AL., CCPA AND GDPR COMPARISON CHART (2018), https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf [hereinafter CCPA/GDPR COMPARISON CHART]; *Privacy Framework Comparisons*, CTR. DEMOCRACY & TECH. (Dec. 2018), https://cdt.org/wp-content/uploads/2018/12/2018-12-12-CDT-CCPA-GDPR-Chart-FINAL.pdf [hereinafter *Privacy Framework Comparisons*].

161. *See, e.g.*, GDPR, *supra* note 6, art. 15.

162. *Id.*; *Right of Access*, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access (last visited Feb. 23, 2020).

163. GDPR, *supra* note 6, art. 15(3). The data may be provided in a print form or other commonly used electronic form. *Id.*

164. *Right of Access*, *supra* note 162.

165. *Id.*

166. *Id.*

c. Right of portability

Controllers must be able to provide Personal Data in a portable form to enable data subjects to exercise their rights. Portability ensures that data subjects are able "to move, copy or transfer personal data easily from one [information technology] environment to another in a safe and secure way, without affecting its usability."[167] Data subjects may choose to obtain their information in conjunction with the right of access as discussed above, or request for a controller to send their data to another controller.[168] The data must be transmitted in a form that is (1) structured; (2) commonly used; and (3) machine readable for a data subject's own review or for another service that will process the data.[169] The right of portability provides data subjects with a mechanism to exercise their power to confirm the accuracy of and rectify their Personal Data and to exercise their freedom to change controllers, such as an internet service provider, with ease.[170]

d. Right to rectification

Due to a data subject's right to access their Personal Data in a portable form, the GDPR also grants data subjects the right to correct any inaccurate or missing Personal Data that a controller may have.[171] Controllers are required to comply with rectification requests "without undue delay" as long as "the purposes of the processing" are not considered "manifestly unfounded" or exorbitant.[172] Controllers must address each rectification "request on a case-by-case basis" within one month of receipt of the request.[173]

e. Right to erasure

The right to erasure, also known as the right to be forgotten, may be exercised through automatic or manual means. Processors and

167. *Right to Data Portability*, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability (last visited Feb. 23, 2020).

168. *Id.*

169. *Id.*

170. *Id.*

171. GDPR, *supra* note 6, art. 16.

172. *Id.*; *Right to Rectification*, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/ (last visited Feb. 23, 2020).

173. *Id.* In the case of a dispute, controllers may delay compliance for up to two months. *See id.*

controllers are required to delete Personal Data when (1) it is "no longer necessary in relation to the purposes for which they were collected or otherwise processed"; (2) the data subject withdraws consent; or (3) the data subject objects and the processor does not have a legitimate interest that overrides the objection.[174] The GDPR places obligations upon businesses to only keep data for as long as necessary—and not any longer—and to comply with data subject requests.[175] Like the right of access, the right to erasure may be requested through oral or written means; however, once a processor or controller receives notice of the request for erasure, they must respond within one month.[176]

f. Right to object

A data subject's right to object varies upon the basis for which their Personal Data is justified.[177] Individuals may object to the processing of their data when it is: (1) being "processed for direct marketing purposes"; (2) being processed for scientific, historical research, or "statistical purposes"; and (3) in a processor's legitimate interests or "carried out in the public interest."[178] The ability to object to data being used for direct marketing is absolute and may be exercised at any time.[179] Similarly, a data subject may object to processing of their Personal Data for scientific research, historical research, or statistical purposes unless "the processing is necessary . . . for reasons of public interest."[180] On the other hand, data that is in the processor's legitimate interests or in the public's interest, is subject to more stringent guidelines.[181] Upon the data subject's objection, the

174. GDPR, *supra* note 6, art. 17(1). A processor's legitimate interests remain a key element for the justification of processing; however, further discussion of legitimate interests is beyond the scope of this Note. *See, e.g.*, RUTH BOARDMAN ET AL., BIRD & BIRD, GUIDE TO THE GENERAL DATA PROTECTION REGULATION 11–12 (2019), https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird—bird—guide-to-the-general-data-protection-regulation.pdf?la=en.

175. *See* BOARDMAN ET AL., *supra* note 174, at 11.

176. *Right to Erasure*, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ (last visited Feb. 23, 2020).

177. *See, e.g.*, BOARDMAN ET AL., *supra* note 174, at 32.

178. GDPR, *supra* note 6, art. 21; *Right to Object*, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/ (last visited Feb. 23, 2020).

179. GDPR, *supra* note 6, art. 21(1); *Privacy Framework Comparisons*, *supra* note 160.

180. BOARDMAN ET AL., *supra* note 174, at 32.

181. *Id.*

"processing of the personal data" must cease "unless [the controller] can demonstrate compelling legitimate grounds which override the interests of the data subject," or the processing "is for the establishment, exercise or defence of legal claims."[182] Ultimately, once a data subject exercises their right to object, the burden rests on "the controller to establish why it should . . . be able to process personal data on [each justified] basis."[183]

g. Right to restrict processing

Data subjects may exercise their right to restrict processing when: (1) "the accuracy of the Personal Data is contested by the data subject"; (2) "the processing is unlawful and the data subject opposes the [data's] erasure . . . and requests [its] restriction . . . instead"; (3) "the controller no longer needs the" information, "but the individual requires the personal data to establish, exercise, or defend legal claims"; and (4) a data subject objects to processing while "the controller verifies the grounds for processing."[184] Exercising the right to restrict processing still allows a processor to store Personal Data, but they are forbidden from processing it.

h. Right to object to automated decision-making

The GDPR establishes the right for data subjects to object to profiling solely based on automated decision-making that has legal or similar significant effects on an individual.[185] This right is subject to exceptions where automated processing is: (1) "necessary for entering into, or performance of, a contract"; (2) authorized by law and is subject to "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests"; or (3) "based on the data subject's explicit consent."[186]

4. Enforcement and Penalties

In order to enforce and monitor GDPR compliance, every EU member state must establish at least one independent "supervisory authority."[187] The Regulation states that the public supervisory

182. *Id.*
183. *Id.*
184. GDPR, *supra* note 6, art. 18; BOARDMAN ET AL., *supra* note 174, at 35.
185. GDPR, *supra* note 6, art. 22.
186. *Id.*
187. *Id.* art. 51(1).

authorities serve "to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union."[188] These enforcement bodies are designed to "cooperate with each other" in order to achieve an efficient and "consistent application of" the GDPR.[189]

While the GDPR streamlines cooperation among supervisory authorities, it explicitly emphasizes that each body "shall act with complete independence" regarding enforcement, administration, infrastructure, and technical duties.[190] These supervisory authorities are responsible for imposing fines, which may total the higher of €20 million or "up to 4% of the total worldwide annual turnover of the preceding financial year."[191] After one year in effect, €55 million in fines were imposed for violations of the GDPR.[192]

B. CCPA Substance: A Survey of the CCPA, Its Eight Amendments, and the California Attorney General's Draft Regulations

1. CCPA Principles

This Section summarizes the core principles of the CCPA as approved on June 28, 2018. It begins by examining the scope of the Act, the consumer rights enumerated in the Act, and the enforcement of the Act. Sections 2 and 3 summarize the Act's amendments and the attorney general's draft regulations, respectively.

a. Scope

The CCPA was drafted, and titled, with an emphasis on consumer privacy. "Consumer" is defined as "a natural person who is a California resident,"[193] and a California resident includes "(1) every individual who is in [California] for other than a temporary or transitionary purpose, and (2) every individual who is domiciled in [California] who is outside [California] for a temporary or transitionary purpose."[194] This definition "leads to much broader coverage for the CCPA than the term 'consumer' usually implies" and

188. *Id.*
189. *Id.*
190. *Id.* art. 52.
191. *Id.* art. 83(6).
192. *See, e.g.*, Andrea Little Limbago, *Lessons Learned from the GDPR's First Year*, VIRTRU (May 14, 2019), https://www.virtru.com/blog/gdpr-one-year.
193. CAL. CIV. CODE § 1798.140(g) (West 2019).
194. CAL. CODE REGS. tit 18, § 17014 (2019).

will likely incorporate employees and "[c]ontacts from business customers or vendors" as long as they are California residents.[195]

The CCPA takes a similarly broad approach to Personal Data, defined in the Act as "personal information."[196] The definition considers any data "that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer" as personal information.[197] The CCPA, however, makes one noteworthy distinction in its definition of "personal information" by including "households" but fails to define the term.[198] The Act considerably expands upon the prior meaning of personal information from the California Online Privacy Protection Act by providing "a non-exclusive list of categories" that must be disclosed whether the data is "collected online or offline, in any format and from any source."[199]

The CCPA's application extends to any "for-profit entity" doing business in California that (1) participates in the collection of "personal information"; (2) participates in the determination of the purposes for which it is processed; and (3) either (i) "[h]as annual gross revenues in excess of twenty-five million dollars"; (ii) participates in transactions involving "personal information of 50,000 or more consumers, households, or devices"; or (iii) "[d]erives 50 percent or more of its annual revenues from selling consumers' personal information."[200]

b. Consumer rights

Like the GDPR, the CCPA establishes certain individual enforceable rights. The Act groups these rights into five categories: (1) the right to know; (2) the right to access; (3) the right to disclosure;

195. Practical Law Data Privacy Advisor, *Understanding the California Consumer Privacy Act (CCPA)*, W-017-4166 (2019) [hereinafter *Understanding the CCPA*].

196. CAL. CIV. CODE § 1798.140(o)(1) (West 2019).

197. *Id.* This is similar to the GDPR's coverage of Personal Data for data subjects.

198. *Id.*; *Understanding the CCPA*, *supra* note 195 (citing CAL. CODE REGS. tit. 11 § 999.301(h) (draft)) ("While the CCPA does not define the term household, the CAG's draft CCPA Regulations propose defining the term as a person or group of people occupying a single dwelling.").

199. Catherine D. Meyer et al., *Countdown to CCPA #3: Updating Your Privacy Policy*, PILLSBURY (July 8, 2019), https://www.pilsburylaw.com/en/news-and-insights/ccpa-privacy-policy.html.

200. CAL. CIV. CODE § 1798.140(c) (West 2019); *Understanding the CCPA*, *supra* note 195.

(4) the right to restrict the sale of personal information; and (5) the right to be free from discrimination for exercising one's rights.[201]

The right to know and right to access are substantially similar to the GDPR's corresponding rights discussed in Part III.A.3.[202] The right to know grants consumers the ability to be informed about the general collection and processing of their information.[203] The CCPA's broad right to access overlaps with its right to disclosure, providing a means for consumers to exercise their rights to receive the specific "personal information a business collected, sold, or disclosed about them."[204] The CCPA limits the right to disclosure by restricting the access to the collected information to two requests every twelve months.[205] Further, the disclosed personal information is regulated in two additional ways: its scope is restricted to the calendar year prior to the request, and consumers must "verify their identity reasonably in light of the nature of the personal information requested."[206]

The combination of the rights to know, to access, and to disclosure provide a foundation for additional consumer rights mirroring the GDPR, such as data portability and erasure; however, the CCPA lacks the ability to rectify errors and omissions in personal information.[207] Additionally, while the CCPA's right to restrict the sale of personal information takes a narrower approach than the GDPR's restriction rights, the CCPA does not provide for additional rights to restrict and object to processing as does the GDPR.[208] The consumer rights established by the CCPA impose obligations for businesses to comply with information requests, identity verifications, disclosure requirements, and appropriate responses by implementing systems and procedures to prior to the Act's enforcement date.[209]

201. California Consumer Privacy Act of 2018, 2018 Cal. Legis. Serv. ch. 55, § 2(i) (West). It is important to note that these five enumerated consumer rights differ from source to source, including the Act itself, Californians for Consumer Privacy, and analysis of the CCPA. *E.g.*, *id.*; *About Us*, *supra* note 38; *Understanding the CCPA*, *supra* note 195.

202. The CCPA's right to know is referred to as the right to be informed, whereas the right to access has the same name for both laws.

203. *Understanding the CCPA*, *supra* note 195.

204. *Id.*

205. *Id.*

206. *Id.*

207. *Id.*; CCPA/GDPR COMPARISON CHART, *supra* note 160.

208. CCPA/GDPR COMPARISON CHART, *supra* note 160.

209. Bilus et al., *supra* note 93.

c. Enforcement

California's attorney general is responsible for enforcing CCPA violations.[210] While California consumers may sue businesses, they can only do so in connection to data breaches:

> Businesses within the scope of the CCPA are liable for civil damages when a failure "to implement and maintain reasonable security procedures" results in a breach involving the personal information of California residents. One way a company may be able to minimize this potential liability would be to demonstrate that it made a reasonable effort to implement the CCPA's standards. A business can seek the opinion of the Attorney General for guidance on how to comply with the provisions of the CCPA. Taking reasonable steps to comply, following up with the Attorney General, and following any advice the Attorney General provides may serve as a mitigating factor in adjudicating a company's liability.[211]

Further, under the CCPA, businesses are granted a thirty-day window to cure violations before receiving fines and incurring liability for statutory damages.[212] For private rights of action, courts may impose injunctive or declaratory relief under the CCPA with consumers pursuing "the greater of actual damages or statutory damages ranging from $100 to $750 per consumer per incident."[213]

2. The Eight Amendments

From the CCPA's passage on June 28, 2018, through October 11, 2019, eight amendments were approved in two tranches.[214] SB 1121 was signed by former Governor Edmund Gerald Brown on September 23, 2018, less three months after he initially approved the bill.[215] The amendment addresses flaws in the CCPA and allows for

210. *See* CCPA/GDPR COMPARISON CHART, *supra* note 160; *Privacy Framework Comparisons*, *supra* note 160.

211. Yallen & DeBré, *supra* note 14, at 17–18 (citations omitted).

212. CCPA/GDPR COMPARISON CHART, *supra* note 160.

213. *Id.*

214. *See*, *e.g.*, Stuart P. Ingis et al., *100 Days Out: The CCPA and What You Need to Know*, VENABLE LLP: INSIGHTS (Sept. 26, 2019), https://www.venable.com/insights/publications/2019/09/100-days-out-the-ccpa-and-what-you-need-to-know?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original; *CCPA Amendment Tracker*, *supra* note 9.

215. *See* Consumer Protection—Privacy, 2018 Cal. Legis. Serv. ch. 735 (S.B. 1121) (West).

flexibility to extend the enforcement date to July 1, 2020.[216] Just over one year later, on October 11, 2019, Governor Newsom signed a second batch of seven amendments: Assembly Bill 25 ("AB 25"), Assembly Bill 874 ("AB 874"), Assembly Bill 1130 ("AB 1130"), Assembly Bill 1146 ("AB 1146"), Assembly Bill 1202 ("AB 1202"), Assembly Bill 1355 ("AB 1355"), and Assembly Bill 1564 ("AB 1564").[217] Approved less than three months before the CCPA's effective date, the amendments address: "(A) clarifications and technical fixes; (B) changes to definitions; (C) exemptions and exceptions; and (D) new regulatory authority and concepts."[218] Thorough examination of the amendments is beyond the scope of this Note; therefore, the seven additional amendments to the CCPA passed in October 2019 are summarized only briefly.

AB 25 temporarily restricts the definition of personal information to exclude employee and other business-related contacts for the first year of the CCPA's implementation.[219] AB 874 excludes anonymized and "'publicly available information' from the definition of 'personal information.'"[220] AB 1130 also amends the definition of personal information, only in regards to data breaches, however, to include biometric data and tax, passport, military, and other unique identifying numbers.[221] AB 1146 provides exemptions for car warranty and recall purposes so that ownership and vehicle data may be utilized.[222] AB 1202 establishes a new "'data broker' registry with the California attorney general."[223] AB 1355 clarifies that anonymized and aggregated data are excluded from the definition of personal information, that differential treatment of consumers based on the value of their data is permitted, and that businesses must to disclose rights to consumers.[224] Finally, AB 1564 outlines the methods for consumer requests that businesses must make available to consumers.[225]

216. *Id.*
217. *See CCPA Amendment Tracker*, *supra* note 9.
218. Ingis et al., *supra* note 214.
219. Zeltzer Hutnik et al., *supra* note 89.
220. *CCPA Amendment Tracker*, *supra* note 9.
221. *Id.*; Zeltzer Hutnik et al., *supra* note 89.
222. *CCPA Amendment Tracker*, *supra* note 9; Zeltzer Hutnik et al., *supra* note 89.
223. *CCPA Amendment Tracker*, *supra* note 9.
224. AB 1355; *CCPA Amendment Tracker*, *supra* note 9.
225. Zeltzer Hutnik et al., *supra* note 89.

3. AG Draft Regulations and Rulemaking

The CCPA authorizes and directs the California attorney general to implement regulations in furtherance of the Act's purposes.[226] Attorney General Xavier Becerra released a draft of the proposed regulations on October 10, 2019, less than three months before the CCPA's effective date.[227] The draft regulations "address some of the open issues raised by the CCPA and would be subject to enforcement by the Department of Justice with remedies provided under the law."[228] While the amendments to the CCPA preserved the January 1, 2020, enforcement date, they extended the attorney general's deadline to publish the regulations and postponed enforcement.[229] After the amendments, the attorney general's "enforcement action start date" was deferred to the earlier of "July 1, 2020 or six months after publication of the final regulations."[230] With the finalized draft regulations expected several months into 2020, July 1, 2020, will serve as the date "the Attorney General's office will be empowered to enforce the provisions of the CCPA," which includes "penaliz[ing] violations of the CCPA that occur" in the six months between the effective and enforcement dates.[231]

Attorney General Becerra's draft regulations emphasize "three main areas: 1) notices to consumers, 2) consumer requests 3) verification requirements."[232] Unexpectedly, the attorney general's proposal contained "surprising new requirements," including the following:

- New disclosure requirements for businesses that collect personal information from more than 4,000,000 consumers[;]
- Businesses must acknowledge the receipt of consumer requests within 10 days[;]
- Businesses must honor "Do Not Sell" requests within 15 days and inform any third parties who received

226. *Understanding the CCPA*, *supra* note 195.

227. *Attorney General Becerra Publicly Releases Proposed Regulations Under the California Consumer Privacy Act*, OFF. ATT'Y GEN. XAVIER BECERRA (Oct. 10, 2019), https://oag.ca.gov/news/press-releases/attorney-general-becerra-publicly-releases-proposed-regulations-under-california [hereinafter *Proposed Regulations Released*].

228. *Id.*

229. *Understanding the CCPA*, *supra* note 195.

230. *Id.*

231. Bilus et al., *supra* note 93.

232. Sargent and Schlidt, *supra* note 91.

the personal information of the request within 90 days[; and]

- Businesses must obtain consumer consent to use personal information for a use not disclosed at the time of collection.[233]

While the draft regulations clarify certain aspects of the CCPA, they also add new variables that influence—and potentially alter—CCPA compliance weeks before the Act's effective date.[234] Before finalizing the draft regulations sometime "in the spring of 2020," Attorney General Becerra and his office will hear public comments.[235]

IV. CRITIQUE OF THE CCPA

The CCPA arose from the good intentions of a concerned citizen but came to life as a Frankenstein's-monster-like piece of legislation. Instead of using the GDPR, the groundbreaking and most comprehensive privacy law to date, as precedent, the CCPA was hastily composed and poorly drafted. After the patchwork of eight amendments and the California attorney general's draft regulations, the Act remains fundamentally flawed both in its practical application and its substance.

Beginning with Mr. Mactaggart's ballot initiative, the CCPA was founded on an ideology of policing Big Tech's misappropriation of collected Personal Data, but the Act missed its target. While the $25 million gross revenue threshold for CCPA enforcement targets Big Tech, in reality, "as many as 75% of California businesses earning less than $25 million in revenue would be impacted by the legislation."[236] Jay Edelson, the founder of "one of the country's most prominent privacy class action firms,"[237] protects consumers from "tech companies that play fast and loose with consumer privacy."[238] He calls

233. *Id.*

234. *See, e.g.*, *id.*

235. *Id.*; *Proposed Regulations Released*, *supra* note 227.

236. Lauren Feiner, *California's New Privacy Law Could Cost Companies a Total of $55 Billion to Get in Compliance*, CNBC (Oct. 5, 2019, 10:15 AM), https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html.

237. Jeff John Roberts, *Here Comes America's First Data Privacy Law: What the CCPA Means for Business and Consumers*, FORTUNE (Sep. 13, 2019, 3:30 AM), https://fortune.com/2019/09/13/what-is-ccpa-compliance-california-data-privacy-law.

238. About page for Jay Edelson, EDELSON, https://edelson.com/team/jay-edelson/ (last visited Nov. 30, 2019); Jeff John Roberts, *Big Tech vs. Big Privacy Lawsuits*, FORTUNE (Feb. 23, 2019, 7:00 AM), https://fortune.com/2019/02/23/big-tech-vs-big-privacy-lawsuits.

the CCPA "a disaster of a law because it . . . costs [businesses] a ton of money in compliance" and is "totally toothless."[239] The CCPA's enforcement remains in question due to the Act's thirty-day cure period for violations and an unrealistic expectation that the attorney general will "have the resources to police such a wide-ranging law."[240] Ultimately, small businesses will serve as the CCPA's cannon fodder as they "take on a disproportionately large share of compliance costs compared to larger firms."[241]

As a result of an online presence, a global economy, and precaution, most small businesses have already assumed the financial burden of complying with the GDPR's regulations as a gold standard.[242] While already being GDPR-compliant may reduce some costs for businesses, "[independent] researchers estimated that firms with fewer than 20 employees might have to pay around $50,000 at the outset to become compliant."[243] When considering all of the businesses within the CCPA's scope, compliance costs are expected to reach $55 billion in initial costs with up to an additional $16 billion to maintain compliance over ten years.[244]

"[L]awyers are in consensus that companies will just apply the CCPA nationwide" in addition to the GDPR.[245] But rather than a gold standard,[246] the Act represents an initial wave in a flood of state privacy laws drowning small businesses with financial burdens. Although the CCPA only protects California residents, its enforcement reaches every state.[247] New York, Washington, and other states have begun to propose new privacy laws to protect their own residents, moving one step closer to fifty unique state privacy laws,

239. Roberts, *supra* note 237.

240. Allen L. Lanstra, *Exploring the New California Consumer Privacy Act's Unusual Class Action Cure Provision*, SKADDEN (Apr. 23, 2019), https://www.skadden.com/insights/publications/2019/04/quarterly-insights/exploring-the-new-california-consumer-privacy-act.

241. Feiner, *supra* note 236.

242. *See id.* ("Since many businesses in California that operate in Europe already had to make changes to comply with the GDPR, the report's authors said compliance costs for California's law would be reduced.").

243. *Id.*

244. *Id.*

245. Roberts, *supra* note 237.

246. "While the law continues to take shape, Senator Hertzberg sees the potential for a national impact, similar to how California's tailpipe emission standards became de facto nationwide industry standards." Jason Tashea, *Leading the Way: Inspired by Europe's Sweeping GDPR, California's New Data Privacy Law Could Change How Companies Do Business in the Golden State*, A.B.A. J., Jan.–Feb. 2019, at 34, 35.

247. *See supra* Part II.B.1.i (discussing the scope of the CCPA).

each with intricacies that must be considered to ensure compliance.[248] Further, the possibility of a federal statute that fails to preempt state laws merely represents an additional financial burden while leaving the floodgates open to allow states and concerned citizens like Mr. Mactaggart to continue to propose legislation in an endless cycle.

Substantively, the CCPA falls short, even after the attorney general's regulations. The CCPA's proponents[249] have lauded the attorney general's regulations' similarities to the GDPR, yet the Act fails to be the GDPR's counterpart in several areas including clarity, implementation, and protection of consumer rights. As a result of this uncertainty, one study suggests that a mere twelve percent of businesses are able to comply, and thirty-eight percent will need an additional year in order to be compliant.[250] Rather than resolving the CCPA's definitional and practical enigmas, "the regulations layer on new requirements while sprinkling in further ambiguities."[251] In addition to adding new subject matter for businesses to consider weeks before the Act's effective date,[252] the draft regulations further muddy the water by altering standards.[253] For instance, the regulations decrease the forty-five days permitted to implement opt out requests to fifteen days.[254]

Further, the definitions of several key terms remain uncertain. In some cases, these ambiguities may result in companies failing to protect consumers in order to comply with the Act. For example, businesses and attorneys are grappling with which activities make a

248. *See, e.g.*, Allison Grande, *NY Lawmakers Say Time Is Now for Consumer Privacy Law*, LAW360 (Nov. 22, 2019, 10:12 PM), https://www.law360.com/articles/1222713/ny-lawmakers-say-time-is-now-for-consumer-privacy-law; Frank Ready, *As Privacy Laws Proliferate, All-Inclusive Compliance Tools Are Small Targets*, LAW.COM (Nov. 25, 2019, 9:30 AM), https://www.law.com/legaltechnews/2019/11/25/as-privacy-laws-proliferate-all-inclusive-compliance-tools-are-small-targets.

249. These proponents include Mr. Mactaggart, Assemblymember Chau, the Electronic Frontier Foundation, and the American Civil Liberties Union.

250. Nicole Lindsey, *Study Shows Only 12% of Companies Are Ready for New CCPA Data Privacy Regulation*, CPO MAG. (Nov. 27, 2019), https://www.cpomagazine.com/data-protection/study-shows-only-12-of-companies-are-ready-for-new-ccpa-data-privacy-regulation.

251. Sargent and Schlidt, *supra* note 91.

252. See *supra* Part III.B.3, for examples of new standards in the attorney general's regulations.

253. Angelique Carson, *Critics Say Attorney General's Proposed CCPA Regulations Add Confusion, Not Clarity*, IAPP: PRIVACY ADVISOR, (Oct. 11, 2019) https://iapp.org/news/a/critics-say-ags-proposed-ccpa-regulations-add-confusion-not-clarity. It is suggested that ninety days is a more practical amount of time. *Id.* This results in a nearly impractical practice where "businesses must communicate to all third parties the do-not-sell request" within fifteen days of the request being made by a consumer. *Id.*

254. *Id*.

party a "service provider."[255] Most business have approached the CCPA from the perspective of complying with the law as a service provider, but in order to use the collected data for a purpose other than which it was collected would be considered a "sale" of the data, disqualifying the business as a service provider.[256] While intended to provide consumers with the right to disallow businesses from selling their personal information, in reality, this could prevent businesses from enlisting third parties to provide cybersecurity monitoring.[257] Attorneys fear that unclear and counterintuitive definitions and requirements "creat[e] a disincentive for companies to engage in normal business activities that are actually to protect people from fraud."[258]

These problematic definitions and uncertainties result in further issues with consumer rights. While the CCPA highlights these rights, it falls short of the GDPR's standards by failing to "give consumers complete ownership of their data" and ignoring "data minimization standards."[259] While a thorough analysis of the CCPA, its eight amendments, and the attorney general's proposed draft regulations would demonstrate how the Act departs from the GDPR, doing so would be akin to hitting a moving target. The full scope, effect, and understanding of the CCPA hinges on the attorney general finalizing the draft regulations and is merely speculative until consumers exercise their rights after the CCPA is effective and the attorney general is able to enforce the law—assuming other legislation does not preempt the Act.

The GDPR required, and still requires, implementation in order to fully understand its effect; businesses, attorneys, and the European Data Protection Board spent two years interpreting and providing insight while compliance processes and procedures were implemented.[260] In less than two years, Mr. Mactaggart collected signatures for his initiative, a deal to withdraw the initiative was struck, the CCPA was born, eight amendments were passed, and the

255. *See id.*
256. *See id.*
257. *See id.*
258. *Id.*
259. Tashea, *supra* note 246. Data minimization limits the personal information companies "to only use as much user data as needed to complete as task." *Id.*
260. *See generally* Yallen & DeBré, *supra* note 14 (describing the implementation and interpretation of the GDPR).

attorney general submitted preliminary draft regulations.[261] The CCPA has consistently diverged from existing precedent, and rather than picking up where the GDPR left off, it resulted in a flawed legislation with rushed implementation.

V. PROPOSAL

In order to cure the CCPA's deficiencies and potential consequences, federal legislation that expressly preempts the Act and uses the GDPR as a foundation should be adopted. Focusing on uniformity, adaptability, and accountability will allow the United States to effectively and efficiently become a leader in privacy law regulation while protecting consumers and encouraging innovation. This proposal addresses how developing federal privacy law based on the GDPR clarifies ambiguities and reduces compliance expenses, allows the law and technology to evolve together, and establishes a multi-tiered system for enforcement and compliance.

A. Uniformity

Due to a global economy and the ubiquity of the internet, privacy law should be addressed by a coalition of nations, not by individual countries or states. The GDPR is the optimal candidate to be adopted globally because it is the most comprehensive privacy law to date, it has already been implemented, and companies across the world are already in compliance. Further, privacy law uniformity is practical, reduces compliance costs, and provides clarity.

Rather than reinventing the wheel, transferring the GDPR's principles to federal preemptive legislation will allow Congress to implement a law already functioning successfully across borders while making slight adjustments for it to operate within the United States. Businesses in the United States are either familiar with the GDPR or have already implemented compliance measures, so the transition will be far less burdensome than complying with the CCPA. Uniformity entails adopting consumer rights with identical names and the same mechanisms for data transfers and storage as provided by the GDPR. Adjustments should be primarily focused on remaining ambiguities and redefining the jurisdictional scope so that any processor of data is required to comply with the legislation regarding any user, irrespective

261. *See* Confessore, *supra* note 39; Zeltzer Hutnik et al., *supra* note 89.

of where the processor and user reside. Establishing online borders, whether domestic or international, disadvantages consumers and businesses alike by restricting commerce and allowing for exploitation of jurisdictional loopholes. Uniformity eliminates a flood of legislation from several states, and encourages additional countries to join the EU and United States in an "International Uniform Privacy Coalition" by providing an efficient and affordable avenue to implement cohesive privacy law globally.

The GDPR is not a perfect law;[262] however, adopting its framework provides an opportunity to address ambiguities within the Regulation and its enforcement. If the GDPR's key terms are carried over to new legislation, it is inevitable that certain language would require clarification and expansion. For example, the GDPR discusses a company's "annual turnover of the preceding financial year" in reference to potential fines.[263] Whether turnover refers to gross sales, net profits, or another metric, the legislative process requires interpretation of provisions and confirmation that they are applicable and easily understood by United States businesses but still hold to the principles of the GDPR.

B. Adaptability

For privacy law to be effective long term, it must be adaptable in the ever-changing landscape of technology. Applying a uniform privacy law that is already in existence not only saves money and quenches fears stemming from CCPA's new requirements but also allows the law to evolve with the rest of the world through cooperation among international governing bodies. Under this proposal, the United States should establish a supervisory authority,[264] just as each EU member did in compliance with the GDPR.[265] The leaders of each country's supervisory authority should periodically meet as part of maintaining status in the International Uniform Privacy Coalition.[266]

262. *See, e.g.*, Limbago, *supra* note 192.

263. GDPR, *supra* note 6, art. 83.

264. See *supra* Part III.A.4, for a discussion of supervisory authorities in greater detail.

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

266. The need for communication between supervisory authorities to ensure enforcement is apparent. "Ireland's commitment for enforcing the GDPR has come into question due to zero enforcement actions for the over 2,000 data privacy violations complaints issued." Limbago, *supra* note 192. "This imbalance between notifications and fines has surfaced a core collective action problem when it comes to accountability; it only works as long as all participants equally adhere to and enforce compliance mechanisms." *Id.*

As issues arise, enforcement occurs, and courts rule on privacy matters in each respective country, the International Uniform Privacy Coalition would be able to observe trends and serve as an advisory board while drafting model rules to amend the law as necessary with changes in technology.

C. Accountability

Under this proposal, accountability is manifested in a three-tiered system of checks and enforcement. This approach begins with businesses instituting data protection officers, is followed by the United States establishing a national supervisory authority, and concludes with the International Uniform Privacy Coalition instituting an international court.

Complying with privacy law requires each business to appoint a data protection officer.[267] This position functions as the first level of compliance, monitoring, and enforcement. Data protection officers are responsible for ensuring that protocols are in place to comply with the law, including overseeing consumer rights request responses and ensuring that consent to process Personal Data is properly acquired. This officer is also responsible for continued compliance as the company and law evolves, while simultaneously monitoring for data breaches. Finally, a data protection officer acts as the first level of enforcement in a scheme that allows for multiple levels of fines for varying degrees of non-compliance and enforcement.[268] At the lowest level, data protection officers are able to self-impose fines for low-grade violations and cooperate with authorities to resolve issues while reducing administrative costs.

Nationally, the supervisory authority could be established through expanding the Federal Trade Commission (FTC)[269] or, ideally, established as a new entity with a sole purpose to enforce and monitor the privacy law on a federal level. While a thorough analysis of the required budget to establish a government agency is beyond the

267. The size of a business is irrelevant. Much like an agent for service of process or a corporate officer, the data protection officer position can be accomplished by a third party or the owner of a sole proprietorship. With the availability of GDPR-compliant ecommerce platforms such as Shopify, the cost to control customer data can be minimal.

268. By adhering to the principles of uniformity and adaptability, Congress would be able to implement this scheme.

269. Many critics argue that the Federal Trade Commission would be unable to enforce privacy laws given its current form. *See, e.g.*, Feiner, *supra* note 96.

scope of this Note, the new supervisory authority could be, at a minimum, at least partially self-funded from fines collected.[270] Further, a national supervisory authority eliminates the need for the private right of action through pursuing penalties for severe violations and data breaches. Rather than a large portion of the money spent on a class action lawsuit going toward attorney fees and litigation expenses on both sides, a supervisory authority is able to represent consumers that are harmed by a processor's negligence or nefarious actions. Under this proposal, consumers are compensated for actual damages, and any excess funds from penalties go toward funding the new entity. Whether the supervisory authority resides within the FTC or becomes its own organization, it monitors and enforces the federal privacy law domestically while participating internationally in the International Uniform Privacy Coalition and in the implementation of an international court for disputes between countries.

An international court should be established to resolve cross-border jurisdictional issues that may arise when processors in one country violate the rights of consumers in another country. Under this proposal, if a supervisory authority within the International Uniform Privacy Coalition determines that a processor in another country is in breach of its laws, it may bring action in an international court. The court is comprised of three judges, one appointed by the supervisory authority bringing the action, one appointed by the supervisory authority against whom the action is brought, and a third neutral judge nominated by a majority vote of the remaining non-interested supervisory authorities.[271] This cooperation among supervisory authorities is made possible by adopting uniform privacy law and is necessary due to the amorphous nature of the intersection of technology and privacy law.

270. *See* Charles Kruly, *Self-Funding and Agency Independence*, 81 GEO. WASH. L. REV. 1733, 1735, n.6 (2013) ("Congress has empowered a number of agencies to collect fees and fines that the agencies then use to fund their operations. For instance, Congress has authorized the Federal Communications Commission ('FCC') to 'assess and collect regulatory fees to recover the costs' of the FCC's enforcement and rulemaking activities." (quoting 47 U.S.C. § 159(a)(1) (2006))).

271. If multiple supervisory authorities bring an action against the same processor, then a majority vote should decide which judge they will nominate. Any tie in voting could be resolved by conducting a vote of the non-interested supervisory authorities.

VI. CONCLUSION

At the time of writing, Mr. Mactaggart, politicians from both sides of the aisle, and Big Tech have all expressed dismay over the CCPA. Despite eight amendments and the California attorney general's draft regulations, the Act remains far too ambiguous and rushed for businesses to comply beginning January 1, 2020. If express federal preemptive legislation is not enacted before the CCPA's enforcement date, businesses—especially small businesses—will be subject to insurmountable compliance expenses and potential liability.

In place of the CCPA, federal preemptive legislation should be grounded in the GDPR's principles. Using the GDPR as the foundation for a federal privacy law implements a superior law based on precedent that is widely known and already practiced. Adopting a law based on uniformity, adaptability, and accountability balances the consumer-business relationship and creates a cohesive, enforceable law capable of handling technology's fluid landscape.