Catholic University Journal of Law and Technology

Volume 32
Issue 1 *Fall 2023*

Article 8

2023

One Size Does Not Fit All: How the California Privacy Rights Act Will Not Improve Employee Data Collection and Privacy Rights

Kayla N. Bushey
The Catholic University of America, Columbus School of Law

ONE SIZE DOES NOT FIT ALL: HOW THE CALIFORNIA PRIVACY RIGHTS ACT WILL NOT IMPROVE EMPLOYEE DATA COLLECTION AND PRIVACY RIGHTS

Kayla Nicole Bushey *

California emerged as a leader in privacy law with the passage and implementation of the California Consumer Privacy Act (CCPA) in 2018.[1] This legislation was the first comprehensive consumer privacy framework that granted California consumers, defined by the statute as natural persons who are California residents, the right to request, delete, and correct data collected by businesses operating within the state.[2] However, the CCPA provided an exemption for employee data that was set to expire on January 1, 2021, allowing employers additional time to update their data collection practices with the option for the California legislature to extend this period.[3] This exemption ended with the passage of the California Privacy Rights Act (CPRA), a 2020 ballot initiative that explicitly expanded the data privacy rights to employees beginning January 1, 2023.[4] After the California legislature failed to extend the deadline

* Columbus School of Law, Juris Doctor expected 2024; Bachelor of Arts, University of California, Santa Barbara, 2019; *The Catholic University Journal of Law and Technology*, Managing Note and Comment Editor, 2023-2024; Associate Editor 2022-2023. Thank you to my mentor and article advisor for their support and guidance while drafting this article. Thank you to my family, friends, and Patrick for their endless support and encouragement. Lastly, thank you to the JLT Volume 32 staff for their time and commitment to perfecting this issue's articles.

1 *See generally* California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE §§ 1798.100–1798.199.100 (Deering, amended 2023).

2 *See generally id.*

3 *See generally id.*

4 Sam Dean, *With Prop. 24, California is Trying to Rewrite the Rules of Online Privacy. Again.*, LA TIMES (Oct. 15, 2020, 6:00 AM), https://www.latimes.com/business/story/2020-10-15/prop-24-california-internet-privacy-

for businesses' compliance in the summer of 2022, businesses who fall within the scope of the CPRA are now required to comply with its employee data collection and retention practices after 2023.[5]

I will first argue that the CPRA's expansion of affirmative privacy rights to California employees is not as innovative as it has been for consumers, and the administrative burdens and costs that the expansion has placed on businesses has been disproportionate to its alleged benefits. I will then argue that Congress should pass a federal privacy law that upholds the integrity of the CPRA's consumer protections but preempts the law's employee data requirements.

I. BACKGROUND AND EVOLUTION OF CALIFORNIA PRIVACY LAW

In 2018, California established itself as a leader in the U.S. privacy sector by passing the California Consumer Privacy Act (CCPA), making it the first U.S. state to enact a comprehensive data protection framework for its consumers.[6] However, this was not the first time that California voters had acted to assert their own rights to privacy.[7] In 1972, California amended its constitution to provide its residents with the right to privacy through an initiative on the California state ballot.[8] Scholars argue that the 1972 amendment was the result of growing concerns about state surveillance due to the government's rise in using technological advances against citizens.[9] After the state constitutional amendment, the California Supreme Court interpreted the amendment as protecting an individual's right to privacy against both the government and private businesses in 1994.[10] Following the tech boom of the late 1990s and the rise of collecting and processing consumer data in the early to mid-2000s and 2010s, California privacy advocates sought to strengthen consumer data protections and privacy rights by statute.[11] By using the California ballot initiative procedure, like privacy advocates from 1972, CCPA advocates started a ballot petition to vote the CCPA into law without the risk of repeal by the state

---

ballot-measure.

5 F. Paul Pittman, *Upcoming California Privacy Rights Act: Key Compliance Tasks for California Employers*, WHITE & CASE (Oct. 11, 2022), https://www.whitecase.com/insight-alert/upcoming-california-privacy-rights-act-key-compliance-tasks-california-employers.

6 *See generally* CAL. CIV. CODE §§ 1798.100–1798.199.100.

7 *See* David A. Carrillo et al., *California Constitutional Law: Privacy*, 59 SAN DIEGO L. REV. 119, 166 (2023).

8 *Id.* at 119.

9 *Id.* at 130–31.

10 *See* Hill v. Nat'l Collegiate Athletic Ass'n., 865 P.2d 633, 644 (1994).

11 Dean, *supra* note 4.

legislature.[12] Before the ballot could be voted on, state lawmakers brokered a deal with the lead drafter of the CCPA, and the legislation was signed into law in 2018.[13]

However, the drafters of the original CCPA ballot initiative saw that the finished law had many loopholes, which allowed the legislature to undermine many of the sought-after protections.[14] The drafters also believed that by placing all the enforcement power in the Attorney General's office, it made the law difficult to enforce.[15] To ensure that the CPRA could not be weakened by the state legislature and lobbyist groups over time, privacy activists placed Proposition 24 on California's 2020 ballot.[16]

In November of 2020, California voters approved Proposition 24 to pass the California Privacy Rights Act (CPRA), which amended the CCPA to include key changes, such as the establishment of the California Privacy Protection Agency (the Agency) and new affirmative privacy rights.[17] In addition, the CPRA also expanded all of the privacy rights under the CCPA to employees of businesses subject to the CCPA.[18] The CPRA went into effect January 1, 2023, after the California legislature failed to extend the effective date before the end of their summer session in August of 2022.[19] This has impacted many businesses that either operate within California or retain California residents as employees.[20]

The CPRA reformed the CCPA's scope of information covered by differentiating between personal information (PI) and "sensitive" personal

---

12 John Myers & Jazmine Ulloa, *California Lawmakers Agree to New Consumer Privacy Rules That Would Avert Showdown on the November Ballot*, LA TIMES (June 21, 2018), https://www.latimes.com/politics/la-pol-ca-privacy-initiative-legislature-agreement-20180621-story.html.

13 Dean, *supra* note 4; *Editorial: With the Federal Government Missing in Action, California Should Set Its Own Rules for Internet Privacy*, LA TIMES (June 28, 2018, 4:10 AM), https://www.latimes.com/opinion/editorials/la-ed-internet-privacy-20180628-story.html.

14 Dean, *supra* note 4.

15 *See generally* William A. Tanenbaum & Kiyong Song, *Closing the CCPA Loopholes – California Approves Proposition 24*, MOSES & SINGER LLP (Nov. 18, 2020), https://today.westlaw.com/Document/Ib909277829c611ebbea4f0dc9fb69570/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0&firstPage=true.

16 CAL. CONST. art. II, § 8; *see also* Dean, *supra* note 4.

17 Cameron F. Kerry & Caitlin Chin, *By Passing Proposition 24, California Voters Up the Ante on Federal Privacy Law*, BROOKINGS (Nov. 17, 2020), https://www.brookings.edu/blog/techtank/2020/11/17/by-passing-proposition-24-california-voters-up-the-ante-on-federal-privacy-law/.

18 *Id.*

19 *See* Katharine Campbell, *CPRA: Six Key Impacts on Business*, 12 NAT'L L. REV. 27 (2022); *see also* Pittman, *supra* note 5.

20 Pittman, *supra* note 5.

information (SPI).[21] The original CCPA required all businesses operating within the state to provide notice to California consumers when it collects their PI.[22] Now, the Act requires heighted protection for SPI and provides a distinct list of what information is included.[23] PI is described as any information that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" and includes an extensive list of data encompassed by the Act.[24] SPI is described as:

> (1) Personal information that reveals:
>
> (A) A consumer's social security number, driver's license, state identification card, or passport number.
>
> (B) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.
>
> (C) A consumer's precise geolocation.
>
> (D) A consumer's racial or ethnic origin, religious, or philosophical beliefs, or union membership.
>
> (E) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.
>
> (F) A consumer's genetic data.
>
> (2)
>
> (A) The processing of biometric information for the purpose of uniquely identifying the consumer.
>
> (B) Personal information collected and analyzed concerning the consumer's health.
>
> (C) Personal information collected and analyzed concerning the consumer's sex life or sexual orientation. [25]

The CPRA's expansion of SPI also gives California residents a stronger right to limit a business's use of this subcategory of PI that did not exist in the CCPA.[26]

The CPRA did not amend the definition of businesses that was introduced in the CCPA.[27] The Act applies to for-profit businesses that (1) operate in

---

21 *Annotated Text of the California Privacy Rights Act*, CALIFORNIANS FOR CONSUMER PRIV., https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/ (Nov. 20, 2022).

22 *See generally* CAL. CIV. CODE §§ 1798.100–1798.199.100 (Deering, amended 2023).

23 *Id.* § 1798.140(ae).

24 *Id.* § 1798.140(v)(1).

25 *Id.* § 1798.140(ae).

26 *Id.* § 1798.121(a).

27 *See id.* § 1798.140(d); *see also Annotated Text of the California Privacy Rights Act*,

California; (2) collect consumer personal information; and (3) fulfills one or more of the prescribed requirements.[28] However, one drastic change to the CCPA comes in Section 3, stating:

> The privacy interest of employees and independent contractors should also be protected, taking into account the differences in the relationship between employees or independent contractors and businesses, as compared to the relationship between consumers and businesses . . . [i]t is the purpose of the intent of the Act to extend the exemption in this title for employee and business communications until January 1, 2023.[29]

As of January 1, 2023, businesses already within the scope of the statute must ensure they are compliant with the CPRA privacy requirements for their employees and independent contractors who are California residents.[30] Therefore, businesses need to ensure that they have the proper human resources and data governance to allow employees to exercise their new affirmative rights.[31]

II. WHAT PRIVACY RIGHTS EXTEND TO EMPLOYEES UNDER THE CPRA

The original CCPA sought to provide consumers with some ability to control how their data was collected, controlled, and used by businesses.[32] Following the regulatory framework of the European Union's General Data Protection Regulation (GDPR), the CCPA provided California consumers with positive rights to help them assert a form of ownership over their data.[33] However, the

---

supra note 21.

28 CAL. CIV. CODE § 1798.140(d) ("Business means: (1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized . . . for the profit . . . that collects consumers' personal information…determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:
(A) As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185;
(B) Alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households;
(C) Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.").

29 *Annotated Text of the California Privacy Rights Act*, *supra* note 21.

30 *Id.*

31 *See* Campbell, *supra* note 19.

32 *About Us*, CALIFORNIANS FOR CONSUMER PRIV., https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/ (last visited Nov. 9, 2023).

33 CAL. CIV. CODE § 1798.140(i) ("'Consumer' means a natural person who is a California resident . . . .").

CCPA's broad definition of "consumer" carved out an employer-employee exception that temporarily exempted employers from extending these new data privacy rights to their employee's personal data.[34] This was a drastic departure from the GDPR's definition of "data subject," which is a directly or indirectly identifiable natural person whose data is collected and processed under the extraterritorial scope of the Act, without exception.[35] The CPRA revised the CCPA's employee-employer exception by making the exemption inoperative after January 1, 2023.[36]

Nevertheless, it is still unclear exactly how this will impact employees because the CPRA does not explain how employers should balance their collection of PI, which is needed to distribute employee benefits and wages, against the employee's privacy rights.[37] This lack of clarity is likely the result of an expectation that the 2022 California legislature was going to extend the exemption period, since it had proposed two bills that would have done so.[38] However, both of these bills failed to pass before the legislature's session ended on August 31, 2022.[39] Therefore, employers and privacy experts monitoring the development to this feature of the CPRA lacked any guidance from the legislature and the statute about how to prepare for the Act's operative date.[40]

A. Notice Requirements

The CPRA requires businesses to provide consumers notice every time it collects PI or SPI, as well as when it sells and transfers a consumer's PI to a third party.[41] This remains true when a business collects its employees' PI as well.[42] Therefore, employers will need to consider and draft revised notice procedures for all the points at which it intends to collect its employee's PI.[43]

---

34 *See id.* § 1798.145(m)(1)(A).

35 *See* Regulation 2016/679 of the European Parliament and of the Council of 27 of April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 3–4, 2016 O.J. (L 119/1) [hereinafter GDPR].

36 CAL. CIV. CODE § 1798.145(m)(4).

37 *See* Pittman, *supra* note 5.

38 *Id.*

39 *Id.*

40 *See id.*

41 CAL. CIV. CODE § 1798.130.

42 *Id.* § 1798.145(m)(4).

43 Bret Cohen et al., *CPRA Countdown: How Businesses Can Comply With the CPRA*, HOGAN LOVELLS (Nov. 25, 2020), https://www.engage.hoganlovells.com/knowledgeservices/news/understanding-the-new-california-privacy-rights-act-how-businesses-can-comply-with-the-cpra.

B. The Right to Delete

The CPRA allows a consumer to submit requests to delete any PI the business has collected from her.[44] However, the Act provides extensive exceptions that allow the business to deny the request.[45] These exceptions will likely be very important in the employer-employee context, as it limits employees' ability to delete PI.[46] First, the law likely only applies to PI collected from the individual employee, not information that was created by the business about the employee.[47] Thus, information such as employee evaluations, investigation reports, or internal communications regarding the employee may not fit within the scope of this provision.[48]

Further, one of the exceptions under § 1798.105(d) allows for denial of a request to delete information if it would interfere with the business's ability to "[c]omply with a legal obligation."[49] Many requests to delete employee information under these exceptions would hinder the employer's ability to comply with a multitude of state and federal laws that require businesses to maintain records of their employees' information.[50] Ultimately, the exceptions permitted to businesses to refuse employees' exercise of their deletion rights may result in the provision not being as innovative in the employment context as it has been in the consumer context.[51]

C. The Right to Correct

A privacy right that was added under the CPRA is the right to correct inaccurate personal information.[52] Upon receiving a "verifiable consumer request to correct inaccurate personal information," businesses are required to take "commercially reasonable" steps to correct the designated information pursuant to the direction of the consumer.[53] The provision allows businesses to consider the "nature of the personal information" and "purposes of the processing of the personal information."[54] This is significant in correcting the

---

44 CAL. CIV. CODE § 1798.105(a).

45 *Id.* § 1798.105(d).

46 *See* Zoe Argento, *California Privacy Rights Act for Employers: The Rights to Know, Delete, and Correct*, LITTLER MENDELSON P.C. (Aug. 16, 2021), https://www.littler.com/publication-press/publication/california-privacy-rights-act-employers-rights-know-delete-and-correct.

47 *Id.*

48 *Id.*

49 CAL. CIV. CODE § 1798.105(d).

50 *See generally* Cohen et al., *supra* note 43.

51 CAL. CIV. CODE § 1798.105(d)(1)–(8).

52 *Id.* § 1798.106(a).

53 *Id.* § 1798.106(c).

54 Argento, *supra* note 46.

information because the employer should comply with requests to correct objectively wrong information upon request by the employee.[55] This could insulate subjective material from being within the scope of this privacy right, such as a supervisor's comment on the employee's performance or other opinions formed about the employee during the course of employment.[56] This is due to the way this information is produced because supervisor's comments and evaluations of employees are not PI that is voluntarily provided by the employee to the employer.[57] However, due to the lack of clarity of whether information like employee evaluations and supervisor comments fit within the statute, it is difficult to determine how a court or the Agency may interpret what data is encompassed under this section of the statute.[58]

It is also unclear how this new right is innovative to an employee's privacy rights since employees already have alternative routes to update inaccurate or false information during their employment.[59] Common examples, such as a change in address, may be the kind of personal information that fits within the scope of the right to correct; however, there may be more efficient procedures for employees to correct their personal data in an employer's human resources (HR) database(s).[60] This is especially true for information like an address or bank account information, since this directly impacts the employees' receipt of wages and other benefits, where employees would likely want the information changed much faster than the CPRA's mandated action period.[61]

Under the CPRA, any request submitted to a business under the statute requires the business to respond to the request within a 45-day action window.[62] The statute requires the business to "[d]isclose and deliver the required information to a consumer free of charge[,] correct inaccurate personal information, or delete consumer's personal information, based on the consumer's request within 45 days of receiving a verifiable consumer request from the consumer."[63] Therefore, an employee request to correct would need to be assessed, complied with, and provided to the employee within 45 days from the date the request is made.[64] The statute does allow for an additional 45-day extension when it is "reasonably necessary," however, the employee would still

---

55 *Id.*
56 *Id.*
57 *Id.*
58 *See* CAL. CIV. CODE § 1798.199.10.
59 Argento, *supra* note 46.
60 *Id.*
61 *Id.*
62 CAL. CIV. CODE § 1798.130(a)(2)(A).
63 *Id.*
64 *Id.*

need to be notified about this extension.[65] The statute also fails to define what is "reasonably necessary," which makes fulfilling particularly ambiguous requests difficult for the employer.[66]

D. The Right to Know

The CPRA's "right to know" can be divided into three subdivisions that allows residents to request: (1) the categories of information that will be collected by the business; (2) the PI that is being sold or transferred to a third party; and (3) access to PI that has already been collected.[67] Although these rights may be helpful for a consumer who is unsure of where their data goes beyond their interaction with an immediate business, these rights might not be beneficial to employees because the PI that an employer collect from employees is much different than PI collected from consumers.[68] Employers need to collect very specific PI and SPI from employees, such as full names, addresses, and social security numbers, in order to disburse wages and employee benefits.[69] This purpose is very different than a business's purpose in collecting consumers' PI and SPI for its commercial purposes, such as improving their marketing practices.[70]

1. Right to Know What Categories are Collected

The CPRA requires businesses to categorize both PI and SPI that they plan to collect from their consumers and its business purpose for doing so in their privacy notices to consumers.[71] The Act mentions how business should categorize the PI and SPI that it plans to collect.[72] It also instructs businesses on how to include these categories in their privacy policies to ensure they provide the adequate and required notice to consumers, which are the same categories recommended under the CCPA.[73] The Act describes the following categories:

> (1) The categories of personal information it has collected about consumers.

---

65 *Id.*
66 *Id.*
67 *Id.* § 1798.110(a)(1)–(3).
68 Argento, *supra* note 46.
69 *Id.*
70 *See* Arsen Kourinian et al., *CPRA Could Obstruct Existing Employment Rights*, INT'L ASS'N PRIV. PROS. (Sep. 28, 2021), https://iapp.org/news/a/cpra-could-obstruct-existing-employment-rights/.
71 CAL. CIV. CODE § 1798.110(a)(1)–(4).
72 *Id.* § 1798. 110(c).
73 *Id.*

> (2) The categories of sources from which the personal information it collects.
>
> (3) The business or commercial purpose for collecting, selling, or sharing personal information.
>
> (4) The categories of third parties to whom the business discloses personal information.
>
> (5) The specific pieces of personal information it has collected about that consumer.[74]

Many large businesses that are likely to obtain residents' SPI and PI have followed these recommendations by providing extensive lists or videos in their privacy policies.[75] Employers should be following these recommended categories in the privacy policies that are presented to employees.[76] Additionally, employers should be providing notice of the categories of SPI and PI they intend to collect and the business purpose for doing so.[77]

2. Right to Know What Personal Information is Sold or Transferred to Third Parties

This right enables consumers to request and understand where their data goes after the business has sold or shared it with a third party.[78] It also provides consumers with the ability to opt out of the sale and transfer of personal data.[79] Again, the application of this right to employee data is ambiguous since the Act does not delineate whether employee data is excluded under this provision.[80] Since many businesses use external HR software companies to store and classify employee data, the term "transferring" within the statute may encompass any data being passed from the employee to the employer and then to the third-party data vendor.[81]

However, Kourinian, Shelton Leipzig, and Knox argue that employee data does not fit within the scope of this right since employers "do not sell employee

---

74 *Id.*

75 *See, e.g.*, *Privacy Policy*, GOOGLE, https://policies.google.com/privacy?hl=en-US#infocollect (last visited Nov. 18, 2023); *Target Privacy Policy*, TARGET, https://www.target.com/c/target-privacy-policy/-/N-4sr7p#California%20Residents (last visited Nov. 18, 2023); *Privacy Policy*, SEPHORA (Mar. 17, 2023), https://www.sephora.com/beauty/privacy-policy#USWhatWeCollect.

76 *See* CAL. CIV. CODE § 1798.110(c).

77 *Id.*

78 Argento, *supra* note 46.

79 *Id.*

80 *See* CAL. CIV. CODE § 1798.115.

81 *See id.* § 1798.140(ad)(1).

data and do not track employees for targeting advertisements."[82] They further argue that California already provides employees in the state with laws that address employee data, therefore there is "no need to 'limit' the use of such data."[83]

Yet, the Act does not explicitly exempt employee data within the third-party sharing provisions.[84] Instead, the Act defines a "sale" as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration."[85] Although employers might not be transferring employee data for advertising purposes as Kourinin suggests, businesses are still transferring employee data for monetary consideration since the businesses pay for the HR software company's services.[86] The Act does not specify which direction the monetary consideration must go before the Act becomes applicable.[87]

The Act does not consider any person or entity to be a third party if they are "(1) The business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer's current interaction with the business under this title. (2) A service provider to the business. (3) A contractor."[88] Further, the Act defines a "service provider" as

> [A] person that processes personal information on behalf of a business and that receives from or on behalf of the business consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the person from:
>
> (A) Selling or sharing the personal information.
>
> (B) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business, or as otherwise permitted by this title.
>
> (C) Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the

---

82 Kourinian et al., *supra* note 70.
83 *Id.*
84 *See* CAL. CIV. CODE § 1798.140(ad)(1).
85 *Id.*
86 *Id.*
87 *Id.*
88 *Id.* § 1798.140(ai).

> business.
>
> (D) Combining the personal information that the service provider receives from, or on behalf of, the business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that the service provider may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this section and in regulations adopted by the California Privacy Protection Agency. The contract may, subject to agreement with the service provider, permit the business to monitor the service provider's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.[89]

Therefore, the employer's responsibility to respond to an employee's request to opt out would turn on whether an HR software company fits within the exceptions to the Act's definition of third party.[90] Employers will need to make sure that their contractual agreements with an HR software company meet the requirements of the CPRA by including the "business purpose" for transferring the employee data and provisions that restrict what the HR software company can use and do with the employee data. [91]

However, since the Act's definition of a third party has yet to be defined by the Agency,[92] it is difficult to determine whether or not these HR software companies will be considered exempted from the Act's definition. Currently, some HR software companies allow the employee to make a request to opt out directly.[93] Another HR software company states in its privacy policy that employees (or "individuals") who submit a request directly to the HR software company will forward the request to the employer (referred to as "Customer" in the privacy notice).[94] As employees start to make these requests, it may provide more clarity about whether the HR software companies find themselves responsible to fulfill any employee request to opt-out of the sale of their data, or

---

89 *Id.* § 1798.140(ag).

90 *See id.* § 1798.140(ad).

91 *See id.* § 1798.140(ag)(2).

92 *See* 11 Cal. Priv. Prot. Agency Rule §§ 7000–7304 (2023).

93 *See* CAL. CIV. CODE § 1798.140(ah)(2)(B); *see also BambooHR California Privacy Notice*, BAMBOO, https://www.bamboohr.com/california-privacy-notice/#seven (Dec. 30, 2022); *Privacy Policy*, GUSTO, https://gusto.com/about/privacy (Aug. 21, 2023).

94 *See Monday.com Privacy Policy*, MONDAY.COM, https://monday.com/l/privacy/privacy-policy/ (Oct. 25, 2023).

if employers themselves will be required to follow this limitation in the Act.

3. Right to Access Information

The CPRA also requires an employer to provide "specific pieces of personal information it has collected about that consumer" upon receiving a "verifiable consumer request."[95] However, despite the CPRA's extensive list of what is considered PI and SPI under the statute, it does not specify what is considered "specific pieces of personal information." This is another ambiguity that employers will need to think about when fulfilling requests for specific PI, to which they should determine whether the specific information would fit into the PI and SPI classifications described in the Act.[96]

If an employee submits a request to access specific information, employers will need to take certain steps in considering the scope of the request to determine whether it requires full action or a denial. First, the employer should determine whether the employee is making a request under the CPRA, or if she should be exercising a request for her personnel file under the California Labor Code.[97] It is important for employers to understand the difference in each request because each has a separate response time and will require different procedures to fulfill the request.[98]

Next, an employer should consider at the outset if the information requested nonetheless fits into a CPRA exception that would exempt the employer from fulfilling the request in whole or in part.[99] If there is no applicable exception under the CPRA, the employer must examine the request to determine what "specific information" is being requested and where this information is likely stored.[100] It is likely that the scope of the employee's request for PI or SPI will involve information that is commingled with information that does not fit within the scope of the statute.[101] Therefore, employee evaluations, applications, or other documents that contain information on other individuals or the company, may not be subject to the request as a whole.[102] In order to comply with the CPRA, the information that is not within the scope of the statute will need to be

---

95 CAL. CIV. CODE § 1798.110(a)(5), (b).

96 Argento, *supra* note 46.

97 CAL. CIV. CODE § 1798.110(a)(5); *cf.* CAL. LAB. CODE §1198.5(a) (Deering 2022) (outlining rights of employees to inspect their personnel records).

98 Kristen J. Mathews & Suhna N. Pierce, *A MoFo Privacy Minute Q&A: What PI Access Rights Will California Employees Have Under CPRA Starting January 1, 2023?*, MORRISON FOERSTER (July 18, 2022), https://www.mofo.com/resources/insights/220720-what-pi-access-rights.

99 *Id.*

100 *Id.*

101 *Id.*

102 *Id.*

redacted to preserve the privacy interests of other employees and the business itself.[103]

Next, the employer must consider whether additional "specific" pieces of information may be located in sources outside of the employee's personnel files, and if so, how those can be accessed and properly redacted to fulfill the request.[104] The business will need to determine whether the request fits within the scope of the CPRA, and if it does, it will need to "[d]isclose and deliver" the information within the 45-day window provided by the statute.[105] To avoid the risk of paying fines for failing to provide the information within the 45-day window, businesses should be prepared by creating efficient procedures to ensure they will be able to fulfill the request during the required time.[106]

E. Right to Non-Discrimination

The CPRA, like its predecessor, is careful to ensure that consumers are protected from any retaliation from businesses if they properly exercised their rights under the Act.[107] The right to non-discrimination makes it a violation of the CPRA to discriminate against consumers, and therefore employees, who exercise any of their affirmative privacy rights under the Act.[108] The right to non-discrimination also extends to employees who exercise their new rights after January 1, 2023.[109] Therefore, employers cannot retaliate against employees who choose to exercise their new privacy rights under the CPRA.[110]

F. What Does This Change for Employees?

The CPRA's ambitious extension of privacy rights to California employees may prove to be less impactful in practice than the drafters may have originally foreseen. The level of impact this legislation will have on employees' control over their PI and SPI depends on a few different variables.

---

103 *Id.*; Tess Macapinlac, *CPRA Employee Privacy Rights Moving Ahead*, ONETRUST (Sept. 8, 2022), https://www.onetrust.com/blog/cpra-employee-privacy-rights/.
104 Mathews & Pierce, *supra* note 97.
105 CAL. CIV. CODE § 1798.130(a)(2)(A) (Deering, amended 2023).
106 *Id.*
107 *Id.* § 1798.110(a)(5).
108 *Id.* § 1798.125(a).
109 *Id.*
110 *Id.*

1. Employees' Existing Right to Request Personnel Files

Employees in California already have the right to access their personnel files.[111] Under the California Labor Code § 1198.5 ("Labor Code"), employees maintain the right to access their personnel records from their current and former employers.[112] This provision differs from the CPRA in both its deadline to complete a request and the contents that an employer is required to provide to the employee.[113] The Labor Code gives employers 30 days to fulfill this request, whereas the CPRA provides for an additional 15 days.[114] Yet, the requirements for what a request must contain are quite different, in that under the Labor Code, employees maintain the right to "inspect and receive a copy of the personnel records that the employer maintains relating to the employee's performance or to any grievance concerning the employee."[115] Therefore, employees looking for subjective data points created by their employers should likely make a request for their personnel files under the Labor Code instead of requests for PI or SPI that the business has collected from the employee.[116]

There is no indication that the CPRA trumps the Labor Code in terms of enforcement for an employer, or vice versa.[117] Therefore, an employee could likely submit a request under both provisions to obtain a more holistic view of the files that her employer maintains regarding her PI and personnel file.[118] Further, there is no indication that an exception under the CPRA would also be an exception to this Labor Code provision; therefore, it is unlikely that businesses could use the same provision to block adherence to both requests.[119]

Another difference between the Labor Code and the CPRA is that a violation of the Labor Code results in a penalty of $750 per violation for an employer who fails to comply with a request within the allotted timeframe, as compared to the $2,500 fine for each violation or $7,500 fines for each intentional violation of the CPRA.[120] The Labor Code only mandates that an employee can make a request under the Labor Code once a year, whereas the CPRA does not put a limit on how many submissions an employee can make under the Act.[121] Therefore, the costs of a CPRA violation can be much steeper for businesses if they are unable to respond to the appropriate requests in the 45-day window the

---

111 CAL. LAB. CODE § 1198.5 (Deering 2022).
112 *Id.*
113 *Id.*; *cf.* CAL. CIV. CODE § 1798.125(a).
114 CAL. LAB. CODE § 1198.5(b)(1).
115 *Id.* § 1198.5(a).
116 *See id.* § 1198.5(b)(1).
117 *See id* § 1198.5; *see also* CAL. CIV. CODE § 1798.145.
118 *See* CAL. LAB. CODE § 1198.5; *see also* CAL. CIV. CODE § 1798.145.
119 *See* CAL. LAB. CODE § 1198.5(h); *see also* CAL. CIV. CODE § 1798.145.
120 CAL. LAB. CODE § 1198.5(k); *see also* CAL. CIV. CODE § 1798.155(a).
121 *See* CAL. LAB. CODE § 1198.5(d).

Act provides.[122]

2. Will Employees Actually Exercise Their Rights?

Another factor to consider is whether employees will actually assert one or more of these rights. As the CPRA's message to strengthen data privacy rights grows in popularity, along with the data privacy rights movements across the U.S. in general, some employees may begin submitting requests under the CPRA in 2023.[123] However, it is not clear how many employees will actually take advantage of these rights and for what purposes.[124] Employees are more likely to trust employers with their PI and SPI for purposes of obtaining and maintaining employment benefits and receiving compensation, than employees may be regarding workplace surveillance.[125]

Nonetheless, the second factor to consider is how informed employees will be about their new rights. Employees will only be able to submit these requests if businesses provide their employees with clear instructions and accessible mechanisms to enable them to submit these requests.[126] Further, since businesses will need to take action for each request received from any employee under the CPRA, businesses should make sure they also have adequate internal procedures that will help them receive, review, deliver, or deny each request within the mandated timeframe.[127]

III. HOW THE CALIFORNIA PRIVACY RIGHTS ACT WILL IMPACT

---

122 *See* CAL. CIV. CODE § 1798.155.

123 *See generally* Mark Sullivan, *How the Tech Industry Is Sowing Confusion About Privacy Laws*, FAST COMPANY (Apr. 9, 2021), https://www.fastcompany.com/90622991/alastair-mactaggart-california-privacy-law-interview (discussing with the lead drafter of the CCPA/CPRA why he believes that Californians voted for the CPRA and how this new provision will satisfy their needs for data privacy regulations).

124 *See generally id.* ("We've done our research, and people really do care about it, but they don't know what they can do. [In California] I think people had that sense before our laws that there was nothing they could do. I think when people have an easy way to enable that right . . . they will. Not everybody. Some people won't care, but the people who do will enable that right.").

125 Jon Hyman, *Do Employers Have a Duty to Protect Employees' Personal Information?*, WORKFORCE (June 27, 2019), https://workforce.com/news/do-employers-have-a-duty-to-protect-employees-personal-information.

126 *See* Cynthia J. Larose, *California Privacy Rights Act: Key Compliance Tasks for Employers*, MINTZ (Oct. 17, 2022), https://www.mintz.com/insights-center/viewpoints/2826/2022-10-17-california-privacy-rights-act-key-compliance-tasks.

127 *Id.*

EMPLOYERS

Due to the enactment of the CPRA, employers must conform their data collection policies with the Act or face enforcement actions from the California Privacy Protection Agency or the California Attorney General's office.[128] Now, as of January 2023, businesses who are slow to comply with the Act or commit unintentional or willful violations of the Act could face fines ranging from $2,500 to $7,500 for each violation.[129] These penalties could easily add up if employers are not attentive to the new requirements of the Act and how it applies to employee data.

This is a serious concern for any business that operates with employees in California. Although businesses have shifted their policies and practices to appease new consumer rights provisions, the lenient provisions regarding employee data did not require businesses to restructure their employee data governance after the CCPA went into effect in 2020.[130] The CPRA eliminated this leniency when it came into effect in 2023, and businesses had to reconfigure their employee data collection and retention practices to avoid being investigated.[131] In the two-year period from the CPRA's passage to its effective date of January 1, 2023, businesses should have taken steps to figure out their data collection and retention policies, such as what will be collected, how it will be categorized, and how long it will be kept.[132]

A. Administrative Burdens

The CPRA's expansion to employee data will, no doubt, significantly increase administrative burdens for all businesses in its scope. This will likely include hiring personnel to roll out the new compliance mechanisms and procedures, as well as hiring or appointing permanent administrators who specialize in addressing compliance issues under the CPRA.[133] However, unlike other data protection regulations like the General Data Protection Regulation (GDPR), the

---

128 Bryan Hawkins, *Deadline for California Employers to Comply with California Privacy Rights Act*, JD SUPRA: STOEL RIVES LAB. & EMP. BLOG (Sept. 9, 2022), https://www.jdsupra.com/legalnews/deadline-for-california-employers-to-2053077/.

129 CAL. CIV. CODE § 1798.145(m)(4) (Deering 2023).

130 *See* Jennifer Mitchell et al., *Countdown to the CPRA*, BAKERHOSTETLER: CPRA (Feb. 15, 2022), https://www.bakerdatacounsel.com/cpra/countdown-to-the-cpra/.

131 CAL. CIV. CODE § 1798.145(n)(3).

132 *See* Alan Friel et al., *HR and B-to-B Data Compliance Deadline Looming – Legislative Efforts to Extend California Consumer Privacy Act Exemptions Fail*, SQUIRE PATTON BOGGS (Sept. 8, 2022), https://www.consumerprivacyworld.com/2022/09/hr-and-b-to-b-data-compliance-deadline-looming-legislative-efforts-to-extend-california-consumer-privacy-act-exemptions-fail/; *see also* Larose, *supra* note 126.

133 *See* Larose, *supra* note 126.

CPRA does not require businesses to hire a specified privacy officer.[134] Therefore, businesses will need to consider whether they want to hire additional management officials or train current managers on how to conform to the new CPRA requirements.

Additionally, many businesses will need to obtain better data collection software in order to properly categorize employee data, allow HR administrators to meet any privacy rights requests submitted by their employees under the CPRA, and to protect employees' PI covered under the Act.[135] However, as aforementioned, it is still ambiguous as to whether these HR software companies will be considered a third party under the Act, or if they will be considered a "service provider" and exempted under the CPRA.[136] Some other administrative burdens will likely include the following.

1. Data Mapping

In order to implement their new compliance procedures, businesses should conduct some data diagnostics to determine what PI they maintain and where data is stored, either internally or with a vendor or other database that may contain their employees' PI.[137] After determining what categories of data the business traditionally collects, and what it would like to continue to collect, it should clearly write these categories into a privacy policy that will be distributed to its employees.[138] This procedure will satisfy the notice requirement under the CPRA and allow employees to know what categories will be collected should they decide to exercise any of the new positive rights.[139]

2. CPRA Contracting Agreements and Negotiations with Vendors

The CPRA now requires all businesses within its scope who sell or transfer consumer data to a third party or service provider to make sure that these third parties are also compliant with the CPRA provisions.[140] This new provision seeks to close the loopholes from businesses transferring personal data out of

---

134 GDPR, art. 37(5), 2016 O.J. (L 119); GDPR, art. 39, 2016 O.J. (L 119); *cf.* CAL. CIV. CODE §§ 1798.100–1798.199.100.

135 *See* Larose, *supra* note 126.

136 CAL. CIV. CODE § 1798.140(ag) ("'Service provider' means a person that processes personal information on behalf of a business and that receives from or on behalf of the business a consumer's [or employee's] personal information for a business purpose pursuant to a written contract . . . .).

137 *See* Friel et al., *supra* note 132*; see also* Macapinlac, *supra* note 103.

138 *See* Friel et al., *supra* note 132; *see also* Larose, *supra* note 126.

139 CAL. CIV. CODE § 1798.130(a)(5).

140 *Id.* § 1798.100(d).

state to avoid liability.[141] This provision will have an extraterritoriality that impacts businesses that are not covered directly by the CPRA, requiring them to conform with the provision in order to continue doing business with CPRA-subjected businesses.[142] Within the employee data context, this means that any vendor or third-party service that a business uses in conjunction with employee data will need to also be CPRA compliant.[143]

3. Policies for Responding to Individual Requests

Further, businesses are now required to provide two methods for employees to submit a request under the CPRA.[144] Therefore, employers need to draft clear procedures for employees to follow when they want to exercise their new privacy rights.[145] After businesses have decided how to categorize their employee's data, they can inform their employees on the HR procedures that allow them to exercise their new privacy rights.[146] As mentioned in the previous section, businesses are now required under the CPRA to take action within a 45-day window, instead of providing employees with a response that their request was received.[147] Under the prior law, businesses had to respond to a resident's request within a 45-day period, however, the response did not have to include the information or denial of the request submitted.[148] Now, businesses that were slow to respond to consumers under the prior law will need to quickly transition their response model to avoid triggering a violation for failing to act in a timely manner.

4. Creating and Implementing Data Retention Schedules

In an effort to build a better data governance program, businesses should roll out new data retention schedules to track the timing and oversight of their data intake. This will help businesses make proper responses to any employee request under the CPRA within the 45-day window.[149] Additionally, the new law requires businesses to disclose how long it intends to retain a category of data or

---

141 *Annotated Text of the California Privacy Rights Act*, CALIFORNIANS FOR CONSUMER PRIV., https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/ (last visited Nov. 19, 2023).

142 Jennifer Mitchell et al., *A Road Map of CPRA Compliance*, BAKERHOSTETLER: CPRA (Mar. 8, 2022), https://www.bakerdatacounsel.com/cpra/a-road-map-for-cpra-compliance/.

143 *See* Friel et al., *supra* note 132.

144 CAL. CIV. CODE § 1798.130(a)(1)(A).

145 *See* Friel et al., *supra* note 132; *see also* Larose, *supra* note 126.

146 *See* Larose, *supra* note 126.

147 CAL. CIV. CODE § 1798.130(a)(2)(A).

148 *See id.* § 1798.130(a)(2)(A).

149 *Id.*

criteria for determining how long the company will store the data.[150] The Act is explicit that businesses should not retain data "for longer than is reasonably necessary for [its] disclosed purpose."[151] However, making these retention determinations is not easy for businesses to do, especially those with a geographically dispersed employee base.[152] Businesses with employees both inside and outside of California will need to decide whether they are going to govern the two groups' data differently.[153]

After businesses have properly categorized the data sets they intend to collect for employees and the associated business purpose(s), businesses will then need to determine a reasonable retention time for each category.[154] They will also need to determine whether to treat non-California employee data separately from their California employees.[155] This will require management to consider all its legal obligations for employee data retention under state, federal, and international laws, as well as informed business decisions about what information needs to be continually stored.[156] Businesses may opt for automated software to help keep track of these retention dates for their employee data, but this will ultimately add to their administrative costs.[157]

5. Creating an Incident Response Procedure

Traditionally, state privacy laws aim to reduce the risk of data breaches that put individuals' PI at risk of unauthorized access or use by bad actors.[158] Under a customer records statute, California law already required business to "implement and maintain reasonable security procedures and practices appropriate . . . to protect the personal information from unauthorized access,

---

150 *Id.* § 1798.130.

151 *Id.* § 1798.100(a)(1)(A).

152 Elaine Atwell, *CPRA Will Transform How Your Company Treats Employee Data*, KOLIDE, https://www.kolide.com/blog/cpra-will-transform-how-your-company-treats-employee-data (last visited Nov. 19, 2023).

153 *Id.*

154 Joe Shepley & Jeff Phillips, *Defining Retention Periods to Comply with CPRA*, JDSUPRA (Mar. 25, 2022), https://www.jdsupra.com/legalnews/defining-retention-periods-to-comply-6636558/.

155 Atwell, *supra* note 152.

156 Shepley & Phillips, *supra* note 154.

157 Ben Karenas, *Your Guide to Using OneTrust for CPRA Compliance in 2023*, KENWAY CONSULTING (Oct. 25, 2022), https://www.kenwayconsulting.com/blog/guide-to-using-onetrust-for-cpra-compliance/.

158 *See generally Data Breach Notifications Laws by State*, IT GOVERNANCE USA, https://www.itgovernanceusa.com/data-breach-notification-laws (last visited Nov. 19, 2023) (summarizing each state's data breach notification requirements as of July 2018).

destruction, use, modification, or disclosure."[159] The CPRA now requires more from businesses than just "implementation and maintenance of reasonable security procedures and practices pursuant to Section 1798.81.5 following a breach…"[160] The provision also eliminates the safe harbor that the CCPA originally provided by making every breach under this provision a per se violation for which the business can be fined, regardless of their attempts to improve their security procedures.[161]

6. Hiring and Training Compliance Personnel

In order to fulfill all these new requirements, businesses should consider hiring dedicated data compliance personnel or train existing employees to implement their new data governance. Although not required under the CPRA, businesses should contemplate having a privacy expert handle CPRA requests and other issues that arise under the Act.[162] By having a designated officer or officers within management to focus its attention on all issues that arise under the CPRA, the business may be less likely to commit an unintentional or willful violation of the Act.[163] For example, the GDPR requires entities within the regulation's scope to appoint a Data Privacy Officer (DPO) who possesses "expert knowledge of data protection law and practice" and provides a framework for the tasks that the DPO must fulfill to be GDPR compliant.[164] Appointing a designated privacy officer or training a current employee to take on CPRA compliance will allow the business to make sure that it is following proper CPRA protocol and to conduct yearly audits of its data governance systems.[165]

---

159 CAL. CIV. CODE § 1798.81.5(b) (Deering 2023).

160 *Id.* § 1798.150(b).

161 *Id.*; *see also Annotated Text of the California Privacy Rights Act*, CALIFORNIANS FOR CONSUMER PRIV., https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/ (last visited Nov. 19, 2023).

162 Jeffrey Dennis & Kyle Janecek, *Comparing Privacy Laws: GDPRA v. CCPA & CPRA*, NEWMEYER & DILLION LLP (Jan. 2022), https://www.dataguidance.com/sites/default/files/gdpr_v_ccpa_and_cpra_v6.pdf; *see also* GDPR, art. 37(1) ("The controller or processor shall designate a data protection officer . . . .").

163 *See generally* Scott Clark, *4 Ways a Chief Privacy Officer Can Help Your Company*, CMSWIRE (Dec. 1, 2020), https://www.cmswire.com/information-management/4-ways-a-chief-privacy-officer-can-help-your-company/; George B. Hanna & Roy E. Hadley, Jr., *The Chief Privacy Officer: The New "Must Have,"* ASSOC. CORP. COUNS., (Dec. 1, 2018), https://www.acc.com/sites/default/files/resources/20190314/1493964_1.pdf.

164 GDPR, art. 37(5), 2016 O.J. (L 119/1); GDPR, art. 39, 2016 O.J. (L 119/1).

165 *See generally* Clark, *supra* note 163; Hanna & Hadley, Jr., *supra* note 163.

B. Administrative Costs

1. Costs under the GDPR

Businesses that take the proper steps to comply with the CPRA will likely spend a lot of money doing so. To anticipate what administrative costs businesses may face after the CPRA's effective date, it may be helpful to look at how much businesses spent to comply with the GDPR. After the European Union enacted the GDPR in 2016, many American, European, and other international businesses scrambled to make sure they complied in order to avoid massive financial penalties.[166] Under the GDPR, companies who collect data from data subjects in the EU could face up to €20 million in fines for severe violations of the regulations, or up to €10 million for less severe violations.[167] This led to several large British firms spending an estimated $1.1 billion combined to comply with the legislation, and American companies followed with approximately $7.8 billion combined.[168] These staggering numbers highlight the lengths businesses were willing to go in order to avoid potential GDPR fines and the sense of urgency in compliance-related activities for businesses that collect data about European users or offer goods and services in the EU.[169]

However, after the GDPR became enforceable on May 25, 2018, privacy professionals were underwhelmed by the fines levied against companies in the first year.[170] From May 2018 to May 2019, there were only sixteen fines issued for non-compliance, with the highest fine issued for roughly €100,000.[171] Fines began to rise as EU Member States' data protection authorities started enforcing the GDPR against larger companies like Google, H&M, and Telecom Italia, imposing fines of €50 million, €20 million, and €20 million, respectively.[172] In 2021, Amazon was hit with a €746 million fine by the Luxembourg data protection authority for GDPR violations, which stood as the largest penalty

---

166 Oliver Smith, *The GDPR Racket: Who's Making Money from This $9 Billion Business Shakedown*, FORBES (May 2, 2018, 2:30 AM), https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/?sh=57fc067634a2.

167 *What Are the GDPR Fines?*, GDPR.EU, https://gdpr.eu/fines/ (last visited Nov. 19, 2023).

168 *See* Smith, *supra* note 166.

169 *Id.*

170 *See generally* Ilse Heine, *3 Years Later: An Analysis of GDPR Enforcement*, CTR. STRATEGIC & INT'L STUDS. (Sept. 13, 2021), https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement.

171 *See generally id.*

172 *See generally id.*

until Meta was fined €1.2 billion by the Irish Data Protection Commission in May of 2023.[173]

The common thread for these fines, and many fines like them, is that they have been levied against larger companies.[174] However, in order to reach compliance, many small businesses had the burden of spending thousands of dollars before the GDPR enforcement period to make sure they were not facing potential fines that could result in insolvency.[175] One option American and other non-European companies had was to completely stop operations in Europe to avoid coming into compliance.[176] This will likely not be an option under the CPRA for small or larger businesses alike.[177]

For many American businesses, shutting off California as either a consumer base or employment arena is not an option.[178] As of 2022, California was on track to become the fourth largest economy in the world, surpassing Germany.[179] This is partially attributable to some of the most profitable companies in the world being headquartered within the state, such as Apple, Inc., Alphabet Inc., and Intel Inc.[180] California is also home to 4.1 million small businesses, which

---

173 *Recent GDPR Fines Against Amazon and WhatsApp Set New Records*, JDSUPRA (Oct. 6, 2021), https://www.jdsupra.com/legalnews/recent-gdpr-fines-against-amazon-and-6369820/; Jedidiah Bracy, *Meta Fined GDPR-Record 1.2 Euros In Data Transfer Case*, INT'L ASS'N PRIV. PROS. (May 22, 2023), https://iapp.org/news/a/meta-fined-gdpr-record-1-2-billion-euros-in-data-transfer-case/.

174 *See generally 20 Biggest GDPR Fines So Far [2023]*, DATA PRIV. MANAGER (Sep. 19, 2023), https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/; Alexis Porter, *Lessons Learned from GDPR Fines in 2023*, CPO MAGAZINE (Aug. 2, 2023), https://www.cpomagazine.com/data-protection/lessons-learned-from-gdpr-fines-in-2023.

175 *See* Pete Swabey, *GDPR Costs Businesses 8% of Their Profits, According to a New Estimate*, TECH MONITOR, https://techmonitor.ai/policy/privacy-and-data-protection/gdpr-cost-businesses-8-of-their-profits-according-to-a-new-estimate (Mar. 15, 2022, 11:02 AM).

176 Jeff South, *More Than 1,000 U.S. News Sites Are Still Unavailable in Europe, Two Months After GDPR Took Effect*, NIEMANLAB (Aug. 7, 2018, 12:05 PM), https://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/.

177 *See What Businesses Outside of California Should Know About the California Consumer Privacy Act*, TANNENBAUM HELPERN SYRACUSE & HIRSCHTRITT LLP (Mar. 20, 2019), https://www.thsh.com/publications/what-businesses-outside-california-should-know-about-the-california-consumer-privacy-act (discussing how the scope of the CCPA prior to the CPRA could reach approximately "500,000 U.S. businesses, many of these small and medium-sized companies").

178 *See id.* (discussing how the scope of the CCPA prior to the CPRA could reach approximately "500,000 U.S. businesses, many of these small and medium-sized companies").

179 Matthew A. Winkler, *California Poised to Overtake Germany as the World's No. 4 Economy*, BLOOMBERG, https://www.bloomberg.com/opinion/articles/2022-10-24/california-poised-to-overtake-germany-as-world-s-no-4-economy (Oct. 25, 2022, 8:22 AM).

180 Michael Wittner, *Fortune 500: These California Companies Make 2021 List*, PATCH (June 3, 2021, 3:13 PM), https://patch.com/california/across-ca/fortune-500-these-

employ over 48.5 percent of the state's private workforce.[181] All these companies will need to make sure they are in compliance with the CPRA if they qualify as a "business" under the law's definition.[182]

The rise of remote work may have also led to more California residents being employed by out-of-state businesses. This is not unlikely, since California has a population of 40 million, and continues to attract the attention of businesses for its talented labor force.[183] However, out-of-state employers will need to make sure that the data collection and retention practices for their California employees comply with the CPRA if they also qualify as a "business" under the law.[184]

It is not yet known how quickly the Agency will start enforcing the CPRA expansions, since enforcement does not occur until July 1, 2023.[185] Still, the drafters of the CPRA expansions were likely aware of what caused the GDPR authorities to only issue sixteen fines during the first year of its enforcement period.[186] For the GDPR, enforcement is determined by the individual member countries, and some countries have taken stronger initiatives to enforce the data regulations.[187] The regulation requires each member country to develop a supervisory authority and allows the member to designate the authority with its own rules and procedures.[188] However, this autonomy has led to a decentralization of the GDPR's enforcement power and a patchwork of member countries that have been more litigious than others.[189] This is likely what caused the delayed impact on enforcing the provision against violators.[190]

Unlike the CPRA, the Agency could have begun enforcement against any violators as early as July 2023, since it does not rely on multiple enforcement agents.[191] Although the monetary values for a breach under the CCPA remained

---

california-companies-make-2021-list.

181 STATE OF CAL. OFF. OF SMALL BUS. ADVOC., ANNUAL REPORT TO THE GOVERNOR AND LEGISLATURE FISCAL YEAR 2019-2020, https://calosba.ca.gov/wp-content/uploads/2021/07/CalOSBA-Annual-Report-October-2019-September-2020-1.pdf.

182 *See* CAL. CIV. CODE § 1798.140(d) (Deering 2023).

183 *See* Adam Uzialko, *How to Run a Business in California*, BUS. NEWS DAILY, https://www.businessnewsdaily.com/8729-the-state-of-small-business-california.html (June 22, 2023).

184 *See* CAL. CIV. CODE § 1798.140(d).

185 *Id.* § 1798.145(m)(4).

186 *See generally* Sullivan, *supra* note 123 (statement of Alastair MacTaggart, lead drafter of CPRA) ("One way to look at the CPRA, the 2020 law, is we just recreate the General Data Protection Regulation (GDPR), materially and in all respects, in California.").

187 GDPR, art. 51, 2016 O.J. (L 119/1).

188 *See* GDPR, art. 8, 10, 36, 51, 2016 O.J. (L 119/1).

189 *See generally* Heine, *supra* note 170.

190 *See generally id.*

191 CAL. CIV. CODE § 1798.145(m)(4) (Deering 2023).

the same in the CPRA, violations cost $2,500 per violation and $7,500 per each intentional violation.[192] If employers were unwilling to get their employee data into compliance before January 1, 2023, the Agency could administer large penalties as early as July 1, 2023.[193] Also, the CPRA does not cap the amount of penalties the Agency can levy against a business; therefore, businesses should do their best to avoid intentional violations, especially in employee data, where the penalties could add up quickly.[194]

C. Enforcement Mechanisms under the CCPA

One critique of the CCPA was that it placed all the enforcement power on California's Attorney General's Office, in addition to the Office's other responsibilities.[195] During the first year of the CCPA's enactment, former California Attorney General Xavier Becerra submitted written testimony to the U.S. Senate Committee on Commerce, Science, and Transportation to discuss the need for an additional enforcement mechanism.[196] In his testimony, former AG Becerra wrote, "[W]e cannot do this work alone. While we endeavor to hold companies accountable for violations of privacy law, trying to defend the privacy rights of 40 million people in California alone is a massive undertaking. Violators know this."[197]

It was not until August 2022 that the Attorney General's Office took its first enforcement action under the CCPA in a settlement agreement with Sephora, Inc., which was required to pay $1.2 million for failure to disclose that it was selling its online consumers' data to third parties.[198] Although this was the first

---

192 Anas Baig, *Ultimate Guide to CPRA for U.S. Businesses*, TRIPWIRE (Apr. 11, 2022), https://www.tripwire.com/state-of-security/ultimate-guide-to-cpra-for-us-businesses (with one exception that is inapplicable to employee data).

193 *Id.*

194 Alysa Hutnik, *GDPR v. CCPA/CPRA Compliance: What's the Difference?*, KETCH (May 17, 2021), https://www.ketch.com/blog/gdpr-ccpa-cpra-compliance-what-the-difference#:~:text=Depending%20on%20the%20severity%20of,those%20concerning%20minors%20personal%20data.

195 Cathy Cosgrove, *CCPA Update: Calif. Attorney General Comments, New Amendments Signed into Law*, INT'L ASSOC. OF PRIV. PROS. (Oct. 19, 2020), https://iapp.org/news/a/ccpa-update-calif-attorney-general-comments-and-new-amendments-signed-into-law/.

196 *See Revisiting the Need for Data Privacy Legislation: Hearing Before the U.S. Senate Comm. on Com., Sci., and Transp.*, 116th Cong. 6 (2020), https://oag.ca.gov/sites/default/files/Testimony%20of%20Xavier%20Becerra%2C%20CA%20Attorney%20General%5B2%5D%5B1%5D%20copy_0.pdf (written testimony of Xavier Becerra, Cal. Att'y Gen.).

197 *Id.*

198 Sara Merken, *Sephora to Pay $1.2 MLN in Privacy Settlement with Calif. AG Over Data Sales*, REUTERS, https://www.reuters.com/legal/litigation/sephora-pay-12-mln-privacy-settlement-with-calif-ag-over-data-sales-2022-08-24/ (Aug. 24, 2022, 5:12 PM).

time the CCPA was used against a corporation since the law's enactment in 2020, California Attorney General Rob Bonta stated his hope that the settlement "sends a strong message to businesses that are still failing to comply with California's consumer privacy law."[199]

Now, establishing the Agency will lessen the administrative burden placed on the Attorney General's Office.[200] The Agency is governed by a five-member board, with two seats appointed by the Governor, one by the Attorney General, one by the California Senate Rules Committee, and the final by the Speaker of the California Assembly.[201] This body is tasked with enforcing the provisions of the CPRA and initiating its own rulemaking.[202]

On March 29, 2023, the Agency issued its final regulations, with provisions indicating that it plans to take aggressive measures for investigations and enforcement.[203] One regulation allows individuals to file sworn complaints about potential violations of the CPRA.[204] This allows a consumer or employee to raise any suspicions about a business she believes is committing violations under the CPRA by either an electronic complaint system or submitting a complaint in person or by mail.[205] Although unclear how many consumers will file sworn complaints, the expansion of the investigative arm of the law may be able to address any violators early in the CPRA's lifetime.[206] In the employee data context, this method allows employees to submit complaints and evidence that their employer is out of compliance with the regulation directly to the Agency.[207] Although this is unlikely to be abused by aggrieved employees or consumers, since the filing must be signed under threat of perjury, businesses should be aware that this regulation empowers employees to serve a watchdog function.[208]

The Agency is also empowered to act on its own initiative and open an investigation into a business's conduct.[209] The Agency may open these proceedings after receiving information from "government agencies or private organizations, and nonsworn or anonymous complaints."[210] This should put businesses with any reason to suspect that they may be a business of interest to

---

199 *Id.*
200 CAL. CIV. CODE § 1798.199.90(c).
201 *Id.*
202 *Id.* § 1798.199.40(a).
203 11 Cal. Priv. Prot. Agency Rule §§ 7300–04 (2023).
204 *Id.* § 7300(a).
205 *Id.*
206 *Id.* § 7301(a).
207 *See id.* § 7300(a).
208 *See id.*
209 *Id.* § 7301(a).
210 *Id.*

the Agency on notice that they must quickly make sure they are in full compliance with both the consumer and employee side of the law.[211]

The final method that the Agency can use to investigate and enforce the regulations under the CPRA is by auditing a business within the scope of the statutes.[212] The Agency is authorized to audit and "investigate possible violations of the [CPRA]" if "the subject's collection or processing of personal information presents significant risk to consumer privacy or security or if the subject has a history of noncompliance with the [CPRA] or any other privacy protection law."[213] This sweeping authority would allow the Agency to keep any previous violators on a short list of companies to audit and enforce compliance with the law.[214] The language of the March 29 regulations shows that businesses need to ensure their practices fully conform with the intricacies of the law to avoid paying massive penalties.[215]

However, on June 30, 2023, a day before the CPRA and its regulations were to be open to enforcement, the Superior Court of California ruled that the Agency's regulations could not go into effect until March 29, 2024.[216] The court reasoned that the text of the CPRA required the Agency to promulgate its rules by July 1, 2022, supporting the theory that voters intended for the regulations to begin enforcement one-year after their publication.[217] Therefore, the aforementioned channels of reporting and investigation will be withheld until March 29, 2024, likely creating further incentive for the Agency to enact aggressive enforcement measures.[218] Additionally, the Agency is partially funded by its fines, which may provide an incentive for an increased enforcement of the law.[219] However, the actual rate of enforcement will remain

---

211 *Id.*

212 *Id.* § 7304(a).

213 *Id.* § 7304(b).

214 *Id.*

215 *See* Roger Wilks, *CCPA Becomes CPRA – How Will That Impact How We Do Business with the U.S.*, QUANTUM MKTG. GRP., https://www.quantummarketing-group.com/post/ccpa-becomes-cpra-how-will-that-impact-how-we-do-business-with-the-us (last visited Nov. 19, 2023).

216 Minute Order at 5, Cal. Chamber of Com. v. Cal. Priv. Prot. Agency, No. 34-2023-80004106-CU-WM-GDS (Cal. App. Dep,t Super. Ct. July 2023), https://www.wileyconnect.com/assets/htmldocuments/Final%20Order%2034-2023-80004106-CU-WM-GDS.pdf.

217 *Id.* at 4.

218 Steven M. Millendorf, *CPRA Enforcement Delayed Until At Least March 29, 2024*, FOLEY (July 7, 2023), https://www.foley.com/en/insights/publications/2023/07/cpra-enforcement-delayed-march-29-2024; *See* Steven M. Millendorf et al., *CCPA Business-to-Business and Employment Information Exceptions Ending*, FOLEY (Sept. 6, 2022), https://www.foley.com/en/insights/publications/2022/09/ccpa-b2b-employment-information-exceptions-ending.

219 *Changes to California's Privacy Law – Consumer Privacy Rights Act*, VOYER, https://voyerlaw.com/blog/tag/privacy-law (last visited Nov. 19, 2023); *see also* Baig, *supra*

a mystery until the enforcement period begins.[220]

Nevertheless, Attorney General Bonta made clear that he still intends to enforce the new measures explicitly articulated by the CPRA in the investigative letters sent to large companies to inquire about their employee data collection practices on July 14, 2023.[221] Since the language of the CPRA expanded the CCPA's rights to employee data and does not rely on the Agency's regulations for enforcement, AG Bonta may still be able to move forward with the enforcement of the CPRA's requirements for employee data collection and retention.[222] In a press release, AG Bonta stated that

> The California Consumer Privacy Act is the first-in-the-nation landmark privacy law, and starting this year, the personal information of employees, job applicants, and independent contractor[s] received greater data privacy protections because of it. . . . We are sending inquiry letters to learn how employers are complying with their legal obligations. We look forward to their timely response.[223]

It is clear that both the CPRA enforcement and protection of employee data are at the forefront of the Attorney General's agenda for the remainder of 2023 and 2024.[224]

D. Potential Impact of a Federal Privacy Law

In 2022, a federal data privacy bill called the American Data Privacy and Protection Act (ADPPA) garnered bipartisan support and made it out of the House Energy and Commerce Committee.[225] Like the CPRA and other state laws, the ADPPA takes a consumer approach to safeguarding a person's data

---

note 192.

220 Baig, *supra* note 192.

221 Press Release, Att'y Gen. Bonta Seeks Info. from Cal. Emps. on Compliance with Cal. Consumer Priv. Act, Off. of Att'y Gen. Rob Bonta (July 14, 2023) (on file with author).

222 *See generally* Robert Blamires et al., *Employee Data Increasingly in the Crosshairs of Data Privacy Enforcement*, LATHAM & WATKINS LLP (July 20, 2023), https://www.globalprivacyblog.com/privacy/employee-data-increasingly-in-the-crosshairs-of-data-privacy-enforcement/.

223 Press Release, Att'y Gen. Bonta Seeks Info. from Cal. Emps. on Compliance with Cal. Consumer Priv. Act, *supra* note 221.

224 *See* Kathleen E. Scott et al., *California AG Initiates CCPA Investigations, Despite Setback in Court*, WILEY (July 19, 2023), https://www.wileyconnect.com/California-AG-Initiates-CCPA-Investigations-Despite-Setback-in-Court; *see also* Blamires et al., *supra* note 222.

225 *House Committee Passes Comprehensive Federal Privacy Legislation*, HUNTON ANDREWS KURTH (July 26, 2022), https://www.huntonprivacyblog.com/2022/07/26/house-committee-passes-comprehensive-federal-privacy-legislation/.

from businesses.[226] However, the federal law had notable exemptions to categories of data, including employee data, making it a much weaker privacy law than the CPRA.[227] Therefore, many California congressional members, like former Speaker of the House Nancy Pelosi, declined to offer support for the measure, as it would preempt the CPRA.[228]

The tension between supporters and opponents of the ADPPA highlights why the United States has been slow to enact any comprehensive data privacy and protection framework.[229] With over 80 percent of Americans calling for data privacy protection, both political parties want to enact a federal framework to protect their constituents in states without any state-specific data privacy laws.[230] However, California privacy advocates have repeatedly stated their goals to strengthen privacy legislation in the state over time and a federal privacy law like the ADPPA could derail these efforts.[231]

Therefore, the potential costs under federal legislation could be immense or slight depending on what state laws the legislation preempts. If the federal law mirrors the CPRA, then businesses who have already wrangled their operations into compliance will have lower costs than those that had previously been exempted.[232] The exempted businesses will experience the same administrative burdens that businesses in California are experiencing now, making this a costly federal law to impose.[233] Yet, a federal law that preempts the CPRA and other state laws would still likely raise costs for businesses operating in states like Oklahoma, which lack any data privacy regulations.[234]

However, if Congress does not act within the next few years and states continue to pass piecemeal data privacy legislation, businesses will be no better off.[235] One 2022 study estimated that the patchwork of state privacy laws could

---

226 Anne Godlasky, *American Data Privacy and Protection Act (ADPPA) Didn't Pass but Got Further Than Ever*, NAT'L PRESS FOUND., https://nationalpress.org/topic/data-privacy-act-adppa-us-lacks-law-eu-standard/ (Dec. 28, 2022).

227 *See* Joseph Duball, *State Views on Proposed ADPPA Preemption Come into Focus*, INT'L ASS'N OF PRIV. PROS. (Sept. 27, 2022), https://iapp.org/news/a/state-level-views-on-proposed-adppa-preemption-come-into-focus/.

228 *Id.*

229 Brandon Vigliarolo, *National Data Privacy Law for the U.S. Clears First Hurdle*, THE REGISTER (July 21, 2022, 7:01 PM), https://www.theregister.com/2022/07/21/us_adppa_privacy/.

230 *See A Majority of Americans Are Concerned About the Safety and Privacy of Their Personal Data*, IPSOS (May 5, 2022), https://www.ipsos.com/en-us/news-polls/majority-americans-are-concerned-about-safety-and-privacy-their-personal-data.

231 Duball, *supra* note 227.

232 *See generally id.*

233 *See id.*

234 DANIEL CASTRO ET AL., THE LOOMING COST OF A PATCHWORK OF STATE PRIVACY LAWS 16, 18 (Jan. 24, 2022), https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/.

235 *Id.* at 1–2.

"impose out-of-state costs of $98 billion to $112 billion annually."[236] Additionally, the study stated that over a ten-year period, the costs could "exceed $1 trillion" with a substantial burden falling on small businesses within the nation.[237] Therefore, Congress will likely need to act on passing a federal data privacy law soon, especially amid calls from President Biden.[238]

IV. RECOMMENDATIONS

Although the CPRA, like its predecessor, is an effective consumer protection provision, it was not drafted with the consideration that employee data is distinct from consumer data. Both iterations of California's consumer privacy law are unlike the GDPR because the GDPR was a blanket provision for all "data subjects" within the EU's border.[239] However, the CCPA's employer-employee exemptions explicitly told businesses that it would only apply to consumers.[240] Now, this leaves many businesses at an imposition since businesses that were compliant under the CCPA will still have to shift their employee data models.[241] This places huge costs and administrative burdens on a category of data that does not fit within the Act's original purpose of strengthening consumers' rights.[242] To resolve this disconnect, it may be beneficial to roll back the employee data provisions in the CPRA and address other privacy concerns employees have.[243]

However, since the CPRA was passed by a ballot initiative, the only way for the employee data coverage to be repealed or revised by the California legislature is through another ballot measure to amend the CPRA.[244] This may be difficult, as privacy advocates would likely not want to weaken the privacy protections extended to employees.[245] Additionally, it may be difficult to get this

---

236 *Id.* at 2.

237 *Id.*

238 Joe Biden, Opinion, *Republicans and Democrats, Unite Against Big Tech Abuses*, WALL ST. J. (Jan. 11. 2023, 12:00 PM), https://www.wsj.com/articles/unite-against-big-tech-abuses-social-media-privacy-competition-antitrust-children-algorithm-11673439411?mod=hp_opin_pos_3#cxrecs_s.

239 *See* GDPR, art. 9–11, 2016 O.J. (L 119/2); *see also* CAL. CIV. CODE §1798.140(i) ("'Consumer' means a natural person who is a California resident . . . .").

240 CAL. CIV. CODE §1798.145(m)(1)(A)–(C).

241 *See generally* Sullivan, *supra* note 123.

242 *Annotated Text of the California Privacy Rights Act*, CALIFORNIANS FOR CONSUMER PRIV., https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/ (Nov. 20, 2022).

243 *See generally* Emily Belton, *78% of Employers Engage in Remote Work Surveillance, Express VPN Survey Finds*, EXPRESSVPN, https://www.expressvpn.com/blog/expressvpn-survey-surveillance-on-the-remote-workforce/#ethics (Mar. 11, 2023).

244 *See* CAL. CONST. art. II, § 10(c).

245 *See generally About Us*, CALIFORNIANS FOR CONSUMER PRIV., https://www.caprivacy.org/about-us/ (last visited Nov. 19, 2023).

type of amendment on the ballot given that California employees may not want to give up these positive rights under the CPRA, even if they are not fully aware of what rights are given to them due to the statute's convoluted language and application. Therefore, a repeal of this specific provision seems unlikely, especially as consumers and employees covered by the Act become more aware of the rights they are able to exercise.

One solution is a federal privacy law that maintains the CPRA's integrity for consumer protection provision but exempts the employee data requirements. This preemption for employee data would alleviate businesses' burden of having to spend thousands to millions of dollars a year in restructuring and maintaining their employee data. Yet, it would also allow the California legislature and privacy advocates to think of improved employee privacy provisions that encompass the larger concerns from employees. Although this approach askes employee-centric groups to draft privacy regulations for employee data from a blank slate, this method would allow the regulations to be crafted through a labor perspective, as opposed to the consumer viewpoint. This method could produce more articulate, clarified regulations that describe to employers how they should balance their employee data and their employees' privacy interests, while potentially addressing larger privacy concerns of employees.

CONCLUSION

The CPRA's expansion of the CCPA's safeguards reinforces the notion that Californians are concerned about their data privacy.[246] However, the CPRA's extension to employee data may be more underwhelming than privacy advocates had hoped because the legislation was not specifically drafted to cover employee data. Therefore, the plain language of the CPRA fails to recognize how employee data is distinct from the data it collects from consumers.[247] The Act also fails to address how it can be incorporated with a request for an employee's personnel files, a right that California employees already maintain under the state's Labor Code.[248]

Further, it is still unclear whether employees will begin making requests under the CPRA, as much of the state-level and national discussion around data privacy has been aimed more towards consumer protection, which was the original intent of this bill.[249] For an employee to make a meaningful request under this Act, she will need to be aware of what she can request and how she is

---

246 *See generally* Sullivan, *supra* note 123.
247 *See generally* CAL. CIV. CODE §§ 1798.100–1798.199.100 (Deering, amended 2023).
248 *See* CAL. LAB. CODE §1198.5(a) (Deering 2023).
249 *See* Biden, *supra* note 238.

able to submit her request.[250] This will require affirmative action from businesses to make their CPRA notices clear and understandable to their employees.[251]

In addition to the underwhelming expansion, the new requirements will place even more administrative burdens and costs on businesses that are striving to make sure that they are not fined for improperly collecting and storing their employee data or failing to meet requests.[252] Many businesses must update their privacy terms, their data collection and storage methods, and contractual agreements with vendors in order to handle the new requirements for employee and nonemployee data under the CPRA.[253] Businesses also need to make large improvements to their request, incident response, and data retention procedures and timelines to ensure compliance with the law.[254]

One of the most important questions is how the Agency will begin enforcing the Act after July 2023, or if it will begin enforcement at all.[255] Since the Act provides the Agency with broad enforcement power, businesses that lagged to get their policies into compliance under the previous laws may face vigorous enforcement before the end of 2023.[256] The Agency's publication of its final rules seem to indicate that it will likely take its investigative and enforcement role seriously as the enforcement period approaches; however, the Superior Court's mandate may slow down any plans for robust enforcement.[257]

Further, the rise in a national discussion about passing a federal privacy regulation could dramatically change how the CPRA is enforced. A federal privacy framework could entirely preempt the CPRA's provisions, both for consumers and employees, or the framework could align with the CPRA's provisions and goals.[258] If Congress settles on the latter, then businesses that already conformed to CPRA requirements will likely not have to worry about getting themselves into compliance with a new federal law.[259] However, a lax

---

250 *See generally* Sullivan, *supra* note 123.

251 *See generally id.*

252 *See* Jeff Phillips et al., *Defining Retention Periods to Comply with the CPRA*, JDSUPRA (Mar. 25, 2022), https://www.jdsupra.com/legalnews/defining-retention-periods-to-comply-6636558/.

253 *See* CAL. CIV. CODE § 1798.110(c) (Deering 2023).

254 *See generally* Friel et al., *supra* note 132; *see* Larose, *supra* note 126; Mitchell et al., *supra* note 142.

255 CAL. PRIV. PROT. AGENCY, *General Information*, https://cppa.ca.gov/faq.html (last visited Nov. 19, 2023).

256 CAL. CIV. CODE § 1798.199.90(c).

257 *See generally* 11 Cal. Priv. Prot. Agency Rule §§ 7300–04 (2023).

258 *See generally* Biden, *supra* note 238.

259 *State Views on Proposed ADPPA Preemption Come Into Focus*, INT'L ASS'N OF PRIV. PROS. (Sep. 27, 2022), https://iapp.org/news/a/state-level-views-on-proposed-adppa-preemption-come-into-focus/.

federal privacy law could preempt both the employee data requirements and the consumer privacy provisions that California privacy advocates sought.[260]

There is some silver lining regarding the expansion to employee data, because it requires businesses to improve their data governance for employees and consumers.[261] This could eventually lead to a better data ecosystem, where businesses are more strategic and mindful of the data they collect and sell.[262] This may also encourage employers to be more transparent with their employees, and encourage stronger relationships of trust between employees and employers.

California continues to advocate for the privacy of its residents and maintains a belief that data privacy protections should strengthen over time.[263] This may conflict with moving forward to pass new federal privacy legislation, as Californian privacy advocates will want a law that does not preempt the CPRA.[264] Nonetheless, California has started an important national conversation about data privacy and the empowerment of individuals to exercise control over how their data is collected.[265]

---

260 CASTRO ET AL., *supra* note 234.

261 *See* Campbell, *supra* note 19.

262 Kendra Clark, *CPRA Takes Effect in January: Experts Warn That Ad Ecosystem Is About to Change*, THE DRUM (Dec. 7, 2022), https://www.thedrum.com/news/2022/12/07/with-cpra-become-active-2023-privacy-pros-warn-paradigm-shift.

263 *About Us*, CALIFORNIANS FOR CONSUMER PRIV., https://www.caprivacy.org/about-us/ (last visited Nov. 19, 2023).

264 Joseph Duball, *State Views on Proposed ADPPA Preemption Come Into Focus*, INT'L ASS'N OF PRIV. PROS. (Sep. 27, 2022) https://iapp.org/news/a/state-level-views-on-proposed-adppa-preemption-come-into-focus/.

265 Clark, *supra* note 262.