November 21, 2022

Via electronic mail

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd.
Sacramento, CA 95834

Re: **Modified Proposed Regulations Under the California Consumer Privacy Act**

The Bank Policy Institute (BPI)[1] appreciates the opportunity to submit comments to the California Privacy Protection Agency on the Modified Proposed Regulations implementing the California Consumer Privacy Act, as amended by the California Privacy Rights Act.[2]

I. Executive Summary

BPI's members are financial institutions that have invested significant time and resources into building data protection and information security compliance systems that align with federal and state financial privacy laws. BPI members are committed to promoting robust privacy protections for California consumers.

Drawing on the experience of its members operationalizing privacy and security safeguards for their customers, BPI previously submitted comments on the initial Proposed Regulations implementing the CCPA.[3] Many of these comments relate to three key themes:

- First, the regulations should embody standards that are sufficiently flexible to enable businesses to promote consumer privacy effectively. Consumers are not always served by lengthy and technical disclosures or overly prescriptive requirements.

- Second, the regulations must operate within the parameters established by the legislature and California voters.

---

[1] The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost two million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

[2] Cal. Civ. Code § 1798.100 *et seq.*

[3] *See* Letter from BPI to California Privacy Protection Agency, Re: Proposed Regulations Under the California Consumer Privacy Act (Aug. 23, 2022).

- Third, the regulations should recognize the critical role of other federal and state privacy and consumer protection frameworks in protecting consumers.

We commend the Agency for amendments it made it to the Modified Proposed Regulations in service of these goals, although, as discussed further below, we urge the Agency to go further and address recommended changes that have not yet been addressed.

Today, BPI emphasizes a small number of technical corrections and clarifications that are necessary to avoid seemingly unintended consequences. In addition, BPI is writing to urge the Agency to delay enforcement as it relates to employee and business-to-business ("B2B") personal information. The Agency should not enforce general consumer data protection rules in the employment and B2B contexts without careful consideration of their impact and analysis of employment laws, existing commercial contracts, and other legal frameworks. Finally, BPI also reiterates its prior comments, including by urging the Agency to move away from highly prescriptive requirements for contracts with service providers and third parties.

II. Additional Technical Corrections and Clarifications Are Necessary.

In this Section, we identify several technical corrections and clarifications that are "low-hanging fruit" for the Agency to remedy. It is not clear that the Agency intends the harmful implications described below, and, in any event, these corrections are important to serve the statutory goals of "strengthening consumer privacy, while giving attention to the impact on business and innovation."[4]

a. Notice at Collection – Modified Proposed Regulations § 7012(f)

Section 7012(f) requires a business that collects personal information online to provide the notice at collection by providing a "link that takes the consumer *directly* to the specific section of the business's privacy policy that contains the information required in subsection (e)(1) through (6)." The section continues by stating that directing the consumer to the beginning of the privacy policy, or to any other section without the required information, will not satisfy the notice at collection requirement.

This requirement is overly prescriptive, burdensome, and impracticable, particularly for financial institutions that are managing disclosures to consumers that comply not only with a constellation of general privacy laws, but also federal and state financial privacy laws. While some businesses rely on an online privacy policy to provide a notice at collection, other businesses elect to link within their online privacy policy or a privacy center page to a California-specific notice to address the required disclosures. So long as businesses ensure that consumers have ready access to the relevant information, businesses should have the flexibility to deliver information to consumers based on the clearest presentation to the users.

[4] The California Privacy Rights Act of 2020, Cal. Prop. 24 § 3(C)(1) (2020); *see also* Cal. Civ. Code § 1798.199.40(l) (instructing the Agency to "seek to balance the goals of strengthening consumer privacy while giving attention to the impact on businesses").

Detailed prescriptions on the layering and organization of content within privacy notices are not necessary given that the Modified Proposed Regulations elsewhere address requirements to ensure that notices are provided conspicuously, *see* § 7003, and to ensure that consumers understand the choices available to them, *see* § 7004. Further, this level of prescription raises constitutional and administrative legal questions by burdening the ability of businesses to use a single interface to interact with users across states without directing non-California consumers *directly* to a California-specific privacy notice. Generalizing this requirement would permit businesses greater latitude to communicate effectively with consumers, both Californians and non-Californians alike.

We recommend deleting this provision or, in the alternative, making edits to remove the requirement to link directly to the *specific* section of the privacy policy that contains the required terms. Proposed language can be found in Appendix A to this letter.

b. Third Party Contracts – Modified Proposed Regulations § 7052(a)

We commend the Agency on edits that it has made to Sections 7052 and 7053, which bring the regulations closer to alignment with the statutory requirements for third parties, although, as described below, we continue to have concerns with some of the elements of the Modified Proposed Regulations. We also think that minor, clarifying edits are necessary for the new Section 7052(a), which reads that, "[a] third party that does not have a contract that complies with section 7053, subsection (a), shall not collect, use, process, retain, sell, or share the personal information that the business made available to it."

At best, this is not drafted clearly. At worst, it seems to contemplate a contract between businesses and *every* third party—not just those to which personal information is sold or shared. Such a requirement is not consistent with the statutory design.[5] It also would limit consumers' control over their personal information, as it would limit the disclosure of personal information by a business to a third party in circumstances in which a consumer directs the business to intentionally disclose the information. In such a case, the recipient would be prohibited from collecting the personal information made available to it.

We recommend amendments to clarify that the provision only applies to third parties to which personal information is sold or shared. Proposed language can be found in Appendix A to this letter.

c. Requests to Know – Modified Proposed Regulations § 7024(h)

We continue to have concerns about Section 7024(h) of the Modified Proposed Regulations, even after the Agency's modifications. The section contemplates that businesses, in response to a request to know, will provide all personal information collected or maintained about the consumer on or after January 1, 2022, including *beyond the 12-month period* before the

[5] *See* Cal Civ. Code 1798.100(d) (contemplating contracts between businesses and third parties to which personal information *is sold or shared*).

receipt of the request, unless the consumer requests data for a specific time period or doing so proves impossible or would involve disproportionate effort. In contrast, the plain language of the statute contemplates that businesses will provide information for a 12-month period unless consumers request additional information beyond the 12-month period.[6]

In its initial Explanation of Modified Text of Proposed Regulations, the Agency recognized the need to "conform the regulation to the language of Civil Code § 1798.130(a)(2)(B)." However, the Modified Proposed Regulations still do not address the 12-month look-back period in a manner consistent with the statutory text. To ensure consistency with the statute, the Proposed Rules should be clear that there is no requirement to provide information beyond the 12-month period unless the consumer specifically requests it.

We recommend amendments to conform with the statutory text by specifying that a business must provide information only for the 12-month period preceding the request, unless the consumer requests otherwise. Proposed language can be found in Appendix A to this letter, which mirrors the changes that we recommended in our letter dated August 23, 2022.

III. Enforcement Should Be Delayed For Employee and Business-to-Business Personal Information.

As described below, the Agency should move forward with providing clearer guidance with respect to employee and B2B personal information. In the meantime, however, the Agency should clarify that the CCPA and its implementing regulations will not be enforced with respect to employee and B2B personal information.

The wholesale importation of general consumer protection principles to the employee and commercial context fails to account for important differences between a business's relationship with traditional consumers, as compared to those with whom a business interacts in an employment or commercial context. Not only are expectations of privacy significantly different in the employment and commercial contexts, but these areas already are heavily regulated. Indeed, there are federal and state laws that reflect policy judgments about the rights that job applicants and employees should have to access their personnel records and similar personal information.[7] These legal frameworks reflect relevant policy judgments that the CPRA should not be construed to displace in the absence of more clear intent. For example, Cal. Lab. Code § 1198.5 includes various exceptions to the circumstances in which employers must afford employees with access to their personnel records, including in the context of a lawsuit filed by a current or former employee that relates to a personnel matter against the employer.

---

[6] *See* Cal. Civ. Code § 1798.130(a)(2)(B) ("The disclosure of the required information shall cover the 12 month period preceding the business's receipt of the verifiable consumer request, provided that, upon the adoption of a regulation pursuant to paragraph (9) of subdivision (a) of Section 1798.185, a consumer may request that the business disclose the required information beyond the 12 month period and the business shall be required to provide such information unless doing so proves impossible or would involve a disproportionate effort.").

[7] *See* Cal. Lab. Code § 1198.5; Cal. Lab. Code § 226(b); Cal. Lab. Code § 432; Cal. Civ. Code § 1786 *et seq.*; and Cal. Civ. Code § 1786.53.

Likewise, the CPRA should not be construed to displace or interfere with rights and obligations governed by commercial business relationships absent clear intent to do so. Yet, this would be the practical impact of the currently contemplated application of wholesale general consumer protection principles to the commercial context without clear guidance that accounts for important differences between a business' relationships with its customers in these context.

For these reasons, we appreciate comments made during the October 28 and 29, 2022 Board meetings relating to the importance of the Agency providing clear guidance and exceptions for the employee and B2B contexts. When the Agency provides more specific guidance on these issues, BPI's members are happy to work with the Agency to provide further comments about the application of the CPRA in these contexts. Among other important points, the Agency should ensure that its rules are consistent with other relevant legal frameworks and construe the "specific pieces" of personal information definition appropriately to exclude, for example, confidential business information and internal business records and communications.

In the meantime, until the Agency is able to provide more specific guidance, the Agency should make clear that the CCPA should not be enforced in respect of employee and business customer data. The statute affords the Agency the discretion to treat employee and business customer data differently. Indeed, the statute makes clear that the privacy interests of employees should 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."[8] The ballot initiative also specifies that the law is not intended to interfere with other laws, such as the National Labor Relations Act ("NLRA").[9] And, more generally, the ballot initiative makes clear that "[b]usinesses and consumers should be provided with clear guidance about their responsibilities and rights."[10] This provides ample basis for the Agency to delay application of the CCPA with respect to employee and business customer data.

Conversely, long-standing principles of administrative law preclude the Agency from adopting rules without such a provision in the absence of full consideration of the implications. At present, the current record fails to reflect consideration of the impact of applying various regulatory requirements to employee and B2B personal information. For example, Section 7027(m) lists "[t]he purposes. . . for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit[.]" However, none of the eight examples seem to contemplate processing activities that would be relevant for employee or business-to-business data.

---

[8] The California Privacy Rights Act of 2020, Cal. Prop. 24 § 3(A)(8) (2020).

[9] *Id.*

[10] *Id.* § 3(C)(2). Unlike the CCPA, the other comprehensive state privacy laws exempt employee and business-to-business data, recognizing that there are fundamentally different considerations at play with respect to this data. *See, e.g.,* Va. Code Ann. § 59.1-571 (definition of "consumer" exempts "a natural person acting in a commercial or employment context"); Colo. Rev. Stat. § 6-1-1303(6) (definition of "consumer" "does not include an individual acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context").

Further, the record also does not reflect any consideration of the potential economic impact of extending various provisions in the employment and business customer context, including as it relates to the economic burden where there is tension between confidentiality obligations owed to a business customer and privacy rights of their personnel. These economic impacts are exacerbated given the context: until the end of its legislative session on August 1, the California legislature was still considering bills that would have extended the exemptions.[11] And the CCPA has emerged as an outlier in the U.S. in terms of its treatment of employee and B2B personal information.[12]

In order to resolve these issues, the Agency should clarify that the CCPA and implementing regulations will not be enforced with respect to employee and B2B personal information until the Agency has a chance to review the final regulations and implement appropriate exceptions. At a minimum, the Agency should ensure that the regulations specify that enforcement must account for the lack of clear guidance with respect to employee and business-to-business personal information. Proposed language can be found in Appendix A to this letter.

IV. BPI's Prior Comments Should Also Be Considered Before Finalizing the Rules.

Finally, we urge the Agency to address recommended changes from BPI's August 23, 2022 comment letter that have not yet been addressed. The changes that the Agency made in response to BPI's prior comment letter are positive in better aligning the Modified Proposed Regulations with business incentives to better protect consumers, including by removing certain detailed technical requirements that lacked any tangible consumer benefit. For example, we commend the change the Agency made to remove the arbitrary five-day requirement for service providers to notify a business in the event a service provider can no longer meet its obligations. However, we urge the Agency to revisit those recommendations it has not yet addressed, particularly as it relates to prescriptive contract requirements and mandatory requirements to honor a global opt-out preference signal.

a. Contract Requirements – Modified Proposed Regulations §§ 7051(a)(2), 7053(a)(1)

The Modified Proposed Regulations retain requirements of Section 7051(a)(2) that requires businesses to identify, in each service provider or contractor agreement, the specific business purpose(s) for which personal information is disclosed, and prohibits use of generic language in doing so. Similar language appears in Section 7053(a)(1). These prescriptive contract requirements go beyond the obligations in the statute. There should be a high bar before the Agency adopts new requirements that are not grounded in the statutory text, particularly given that many businesses have already adapted their contracts multiple times to adhere to the evolving requirements set out in the CCPA and its implementing regulations. This bar is not met here, where the additional requirements will confer minimal incremental benefit to consumers while imposing a substantial burden on both businesses and their service providers.

[11] *See* A.B. 2871, Cal. Assembly (2021–2022); A.B. 2891, Cal. Assembly (2021–2022).

Further, these requirements deviate from, and therefore make the CCPA framework less interoperable with, other federal, state, and international privacy laws. This issue is particularly salient for banks, which retain service providers to support activities that do not just involve the processing of personal information subject to the CCPA—but also involve the processing of nonpublic personal information subject to the Gramm-Leach-Bliley Act's ("GLBA") separate requirements for contractual agreements with service providers.[13] For more information on these concerns, we refer the Agency to our additional analysis on contractual requirements in Section 3(a) of our comments dated August 23, 2022.

In addition, we recommend deleting both of these sections in full or, in the alternative, deleting the language requiring a "specific" rather than "generic" description of the business purposes. Proposed language can be found in Appendix A to this letter.

b. Opt-Out Preference Signals – Modified Proposed Regulations § 7026(a)

The requirements relating to opt-out preference signals should be consistent with the statutory design, which affords businesses flexibility as to whether to honor such signals or post a link on their home page.[14] In any event, to the extent some businesses honor opt-out preference signals, the Modified Proposed Regulations should be clear and consistent in terms of the relevant requirements, including by addressing the comments we provided in Section 3(c) of our comments dated August 23, 2022.

More broadly, we urge the Agency to further consider BPI's recommendations that were not addressed in full as part of the edits made to the Modified Proposed Regulations on July 8, 2022. For ease of review, we refer the Agency to Appendix A of our comments dated August 23, 2022. This appendix contains a set of proposed amendments that BPI continues to urge the Agency to adopt, together with the additional amendments included as Appendix A to today's comment letter.

*****

The Bank Policy Institute appreciates the opportunity to submit comments on the Agency's Modified Proposed Regulations implementing the CPRA. If you have any questions, please contact the undersigned by phone at (917) 863-5945 or by email at Gregg.Rozansky@BPI.com

Respectfully submitted,

Gregg Rozansky
Senior Vice President

[13] *See, e.g.*, 12 C.F.R. § 1016.13(a). Banks are also subject to broader third-party risk management guidance issued by banking regulators.

[14] Cal. Civ. Code § 1798.135(a)–(b).

Senior Associate General Counsel
Bank Policy Institute

Appendix A

Gray rows provide detail on points made in Parts II, III, and IV. White rows include additional examples and/or points not addressed in Parts II, II, and IV.

Citations	Comment	Proposed Redline to Cited Modified Proposed Regulations Provision
Section II – Technical Corrections and Clarifications		
Modified Proposed Regulations § 7012(f) Cal. Civ. Code § 1798.100(a)(1)	Section 7012(f) requires a business that collects personal information online to provide the notice at collection by providing a "link that takes the consumer directly to the specific section of the business's privacy policy that contains the information required in subsection (e)(1) through (6)." This requirement is overly prescriptive, burdensome, and impracticable, particularly for financial institutions that are managing disclosures to consumers that comply not only with a constellation of general privacy laws, but also federal and state financial privacy laws.	*Delete § 7012(f).* *In the alternative, amend § 7012(f):* "If a business collects personal information from a consumer online, the Notice at Collection may be given to the consumer by providing a link ~~that takes the consumer directly~~ to the ~~specific section of the~~ business's privacy policy that contains the information required in subsection (e)(1) through (6). ~~Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain the required information, so that the consumer is required to scroll through other information in order to determine the categories of personal information to be collected and/or whether the business sells or shares the personal information collected, does not satisfy this standard.~~"
Modified Proposed Regulations § 7052(a) Cal. Civ. Code § 1798.100(d)	The modified Section 7052(a) reads that, "[a] third party that does not have a contract that complies with section 7053, subsection (a), shall not collect, use, process, retain, sell, or share the personal information that the business made available to it. This is unclear in that it could be read to contemplate a contract between businesses and *every* third party—not just those to which personal information	*Amend § 7052:* § 7052. Third Parties "(a) A third party to which personal information is sold or shared that does not have a contract that complies with section 7053 subsection (a) in respect of such personal information, shall not collect, use, process, retain, sell, or share the personal information that the business made available to it. (b) A third party shall ~~comply with the terms of the contract required by the~~

Citations	Comment	Proposed Redline to Cited Modified Proposed Regulations Provision
	is sold or shared. Such a requirement is not consistent with the statutory design and would limit consumers' control over their personal information.	~~CCPA and these regulations, which include~~ treat~~ing~~ the personal information that the business made available to it in a manner consistent with the ~~business's~~ third party's obligations under the CCPA and these regulations."
Modified Proposed Regulations § 7024(h) Cal. Civ. Code §§ 1798.130(a)(2)(B), 1798.185(a)(9)	The Proposed Regulations do not address the 12-month look-back period for consumer requests in a manner consistent with the statutory text. Consumers should be permitted to request older information from businesses, but the rules should not impose a mandatory requirement that businesses *shall* affirmatively provide the information.	*Amend § 7024(h):* "In response to a request to know, a business shall provide all the personal information it has collected and maintains about the consumer for the 12-month period preceding the business's receipt of the verifiable consumer request. A consumer may request that the business provide all the personal information it has on or after January 1, 2022, including beyond the 12-month period preceding the business's receipt of the request, unless doing so proves impossible or would involve disproportionate effort~~, or the consumer requests data for a specific time period~~. The~~at~~ information to be provided shall include any personal information that the business's service providers or contractors Collected pursuant to their written contract with the business. If a business claims that providing personal information beyond the 12-month period would be impossible or would involve disproportionate effort, the business shall provide the consumer an ~~detailed~~ explanation ~~that includes enough facts to give a consumer a meaningful understanding as to why the business cannot provide personal information beyond the 12-month period~~ for its decision. ~~The business shall not simply state that it is impossible or would require disproportionate effort.~~"
Modified Proposed Regulations §§ 7022(d),	Section 7022(d) states that a business that stores any personal information on archived or back-up systems	*Amend § 7022(d) and 7023(c) either in line with our proposed edits in Appendix A of our letter dated August 23, 2022 or, at a minimum, in line with the below:*

Citations	Comment	Proposed Redline to Cited Modified Proposed Regulations Provision
7022(b)(1), 7023(c) Cal. Civ. Code §§ 1798.105(c), 1798.106(c)	"may delay compliance with the consumer's request" until the archived or back-up system is "restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose." Clarifications are needed to align this provision with 7022(b)(1), which does not require businesses to delete a consumer's personal information from "archived or back-up systems." Section 7023(c) also contains similar contradictions tied to correction rights.	§ 7022. Requests to Delete "(d) If a business, service provider, or contractor stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the relevant data is restored from the archived or backup system ~~relating to that data is restored~~ to an active system or is ~~next accessed or~~ used for a sale, disclosure, or commercial purpose." *Apply corresponding edits to similar language in Section 7023(c).*
Section III – Employee and B2B Data		
Modified Proposed Regulations § 7301 Cal. Civ. Code §§ 1798.155, 1798.199.40(a), 1798.199.45	Applying the CCPA and its regulations to employee and business-to-business personal information will create unintended consequences and compliance problems not easily solved without further guidance and clarity. At a minimum, the agency should ensure that enforcement must account for the lack of clear guidance until it can adopt and clarify appropriate standards.	*Amend § 7301:* § 7301 Investigations. "(c) For personal information that is described in Civil Code section 1798.145, subdivision (m) or subdivision (n), the Agency shall not begin enforcement of possible or alleged violations of the CCPA until the Agency has promulgated additional regulations addressing businesses' obligations with respect to these categories of personal information." *In the alternative, amend § 7301 as follows:* § 7301 Investigations. "(c) For personal information that is described in Civil Code section 1798.145, subdivision (m) or subdivision (n), the interpretation of the CCPA and investigations of possible or alleged violations of the CCPA will take into

Citations	Comment	Proposed Redline to Cited Modified Proposed Regulations Provision
		account good faith efforts to comply and the lack of clear statutory and regulatory requirements and expectations.”
Section IV – BPI’s Prior Comments		
Modified Proposed Regulations §§ 7051(a)(2), 7053(a)(1) Cal. Civ. Code §§ 1798.100(d), 1798.140(e)(5), (j), (ag)	Section 7051(a)(2) requires businesses to identify, in each service provider or contractor agreement, the specific business purpose(s) for which personal information is disclosed, and prohibits use of generic language in doing so. This goes beyond the obligations in the statute and would require an impracticable amount of contract remediation. Section 7053(a)(1) of the draft regulations requires comparable information for third party agreements.	*Delete §§ 7051(a)(2) and 7053(a)(1).* *In the alternative and at a minimum, amend § 7051(a)(2):* “Identify the specific Business Purpose(s) for which the service provider or contractor is processing personal information pursuant to the written contract with the business, and specify that the business is disclosing the personal information to the service provider or contractor only for the limited and specified Business Purpose(s) set forth within the contract. ~~The Business Purpose shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.~~” *Apply corresponding edits to the similar language in Section 7053(a)(1).*
Proposed Regulations §§ 7025, 7026 Cal. Civ. Code §§ 1798.135(b), 1798.185(a)(19)–(20)	The statutory design plainly contemplates that it should be optional, not mandatory, for businesses to honor global opt-out preference signals.	*Amend language in the Proposed Regulations implying that processing the opt-out preference signal is mandatory, including in §§ 7025(b), 7025(c)(1),(3)–(4), 7026(a), etc.* *Further, include technical specifications for opt-out preference signals under §§ 7025 and 7026, as discussed in greater detail in our prior comments.*