BANK POLICY INSTITUTE

August 23, 2022

Via electronic mail

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

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

To Whom It May Concern:

The Bank Policy Institute[1] appreciates the opportunity to submit comments to the California Privacy Protection Agency on proposed regulations implementing the California Consumer Privacy Act, as amended by the California Privacy Rights Act.[2]

I. Executive Summary

BPI members are committed to promoting robust privacy protections for California consumers within the parameters set out by the CCPA. 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.

Drawing on the experience of its members operationalizing privacy and security safeguards for their customers, BPI has carefully considered the Proposed Regulations, which reflect nearly 70-pages of detailed requirements that build on, and in some cases impose new requirements that go beyond, statutory protections.

While we support aspects of the Proposed Regulations, we recommend through this letter certain amendments, including to ensure consistency with the statutory text and other federal and state privacy and consumer protection frameworks. We also have identified several areas of the Proposed Regulations where prescriptive requirements limit flexibility for businesses that are

[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*.

subject to multiple privacy frameworks, which may lead to consumer confusion rather than provide consumers greater clarity, as we presume was intended. The Proposed Regulations should focus on incentivizing businesses to better protect consumers, without detailed technical requirements with no tangible consumer benefit that could serve to distract businesses from focusing on core protections. In addition, we identify proposed requirements that potentially undermine the privacy aims of the statutory framework by requiring businesses to obtain and maintain more information about consumers than they otherwise would or by making it more challenging for businesses to safeguard consumers against identity theft and other data security risks.

For ease, **Appendix A**, which is referenced throughout, contains a set of proposed amendments that BPI urges the Agency to adopt.

II. Key Principles

Our comments on the Proposed Regulations focus on three key principles that we urge the Agency to consider as it undergoes the important process of evaluating and refining the Proposed Regulations.

First, the Proposed Regulations should enhance the consumer experience by protecting consumers' choices about their personal information, promoting practices grounded in data minimization and streamlining disclosures and choices presented to consumers.

The Proposed Regulations are strongest when they set forth clear but flexible standards that embody these principles, such as requirements that disclosures and communications be "easy to read and understandable by consumers."[3] Consumers are not necessarily served by lengthy and technical disclosures or overly prescriptive presentation requirements. Indeed, federal banking regulators spent years developing model notices for financial institutions that embody "succinct" and "streamlined" disclosures intended to promote comprehension and readability.[4] Likewise, the Proposed Regulations best preserve consumer autonomy and choice by avoiding defaults or requirements that constrain or presuppose consumer intent.[5]

Further, the Proposed Regulations should align with principles of data minimization. As discussed in the ISOR, data minimization is an internationally recognized fair information practice principle.[6] It should be a touchstone of the Proposed Regulations, which should avoid requirements that could result in businesses collecting or retaining more personal information than they otherwise would.

Second, the Proposed Regulations must operate within the parameters established by the legislature and California voters, reflecting the judgment captured in relevant statutory language

[3] *See* § 7003(a); *see also* Initial Statement of Reasons ("ISOR"), § 7003.

[4] *See* 74 Fed. Reg. 62890 (Dec. 1, 2009).

[5] *See* Cal. Civ. Code § 1798.185(19).

[6] *See* ISOR, § 7026.

as to the appropriate balance between privacy principles and other considerations. Longstanding principles of administrative law make clear that the Agency does not have the authority to amend the statute.[7] The Agency plays a critical role in ensuring that any new requirements are consistent with both the plain language and statutory design of the CCPA.

Third, the Proposed Regulations should recognize the critical role of other federal and state privacy and consumer protection frameworks in augmenting the protections created under the CCPA. Banks and non-banks alike are subject to a broad suite of other state, federal and international privacy laws. The overall CCPA framework should complement these broader protections and avoid new requirements that do not align with other laws that apply to businesses. Indeed, the Agency's interest in preserving a state framework in addition to any federal privacy standard that emerges would be best served by requirements that afford the flexibility required to achieve consistency and interoperability with other federal and state privacy laws.

This is particularly important for banks, which are subject to extensive regulatory requirements that provide a comprehensive framework to manage privacy and security risks. Even with respect to data that is not governed by the federal Gramm-Leach-Bliley Act ("GLBA") or the Fair Credit Reporting Act ("FCRA"), BPI's members are subject to a constellation of federal banking agency rules and guidance relating to data protection and information security, including with respect to risk management for service providers and other third parties and the management of risks relating to the integrity of data and use of models.[8]

III. Proposed Amendments

a. Highly prescriptive contract requirements do not safeguard consumers and aspects may be inconsistent with statutory text.

The Proposed Regulations call for businesses to implement specific contract terms in agreements with service providers and third parties to whom personal information is sold or shared beyond those terms contemplated by the statute. However, the statute already adopts detailed requirements for written contracts with service providers. Therefore, there should be a high bar before the Agency adopts new requirements, particularly where the new language further deviates from emerging U.S. and global privacy standards. In this case, the bar is not

[7] *See* Cal. Gov't Code § 11342.2 (2022) ("[A] state agency has authority to adopt regulations to implement, interpret, make specific or otherwise carry out the provisions of the statute, [but] no regulation adopted is valid or effective unless consistent and not in conflict with the statute and reasonably necessary to effectuate the purpose of the statute."); *see also San Bernardino City Sch. Dist.*, 294 Cal. Rptr. 3d 348, 352 (Cal. Ct. App. 2022) (noting that a regulation is unenforceable if it "conflicts with the Legislature's intent as manifested in the statute").

[8] *See, e.g.,* Office of the Comptroller of the Currency ("OCC") Bulletin 2021-55, Computer-Security Incident Notification (Nov. 23, 2021); OCC Bulletin 2013-29, Third-Party Relationships: Risk Management Guidance (Oct. 30, 2013); OCC Bulletin 2020-10, Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-19 (Mar. 4, 2020); OCC Bulletin 2011-12, Supervisory Guidance on Model Risk Management (Apr. 4, 2011); Federal Reserve Board, SR 11-7, Supervisory Guidance on Model Risk Management (Apr. 4, 2011).

satisfied, as the additional requirements will confer minimal incremental benefit to consumers while imposing a substantial burden on both businesses and their service providers.

For example, Subsection 7051(a)(2) of the Proposed Regulations states that service provider and contractor contracts must:

> Identify the specific business purpose(s) and service(s) for which the service provider or contractor is processing personal information on behalf of 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 or service shall not be described in *generic terms*, such as referencing the entire contract generally. The description shall be specific (emphasis added).

As an additional example, the Proposed Regulations require contract language specifying a five-day time period for a service provider or contractor to notify a business that it can no longer meet its obligations under the CCPA. These new terms do not have a clear consumer benefit where businesses have imposed contract terms that are consistent with the contract terms contemplated by the statute.[9]

Businesses often retain service providers to support activities that involve the processing of personal information that is subject to multiple privacy frameworks. However, the prohibition on using generic language deviates from, and therefore makes the CCPA framework less interoperable with, other federal, state, and international privacy laws. For example, the prohibition on using "generic terms" to define business purposes or services is not found in other similar privacy laws or even Article 28 of GDPR.[10] Such a prohibition creates particular complexity for banks retaining service providers to support a bank's 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 GLBA's separate requirements for contractual agreements with service providers.[11] Banks are also subject to broader third-party risk management guidance issued by banking regulators.

Further, many businesses have already updated their contracts multiple times to adhere to the evolving requirements set out in the CCPA and its implementing regulations. Indeed, businesses have already been working to update contracts for the CPRA based on the statutory language, but the Proposed Regulations further move the goal posts by adding additional,

[9] *See, e.g.*, Cal Civ. Code § 1798.140(ag)(B), (C). Standard contract provisions requiring compliance with law and indemnification sufficiently incentivize parties to comply with the CCPA.

[10] The Agency should seek to make its rules interoperable with and complementary to other U.S. state and federal privacy laws. As such, the GDPR framework is not necessarily the best reference point. Here, however, this absolute prohibition on generic language doesn't even have a basis in GDPR. Even non-binding guidance from the European Data Protection Board ("EDPB") affords businesses flexibility in the description of processing purposes and recognizes that the comprehensiveness of the description may vary based on the processing activity. *See* EDPB, Guidelines 08/2020 on the concepts of controller and processor in the GDPR, version 2.0 (July 7, 2021).

[11] *See, e.g.*, 12 C.F.R. § 1016.13(a).

idiosyncratic contract language without a clear benefit to consumers or basis in the statute. Incorporating another series of more specific contract requirements could require yet another update and unreasonably limit contracting flexibility. It also distracts businesses from focusing on substantive CPRA requirements in favor of detailed technical requirements with no tangible consumer benefit.

In addition, the new contract terms contemplated in the Proposed Regulations may not serve consumers. With respect to the five-day notification, businesses are best situated to define the appropriate notification timeline on a case-by-case basis that takes account of the risks to the business. For example, a business may want immediate notification of an existing, material compliance issue but may want notification of an expected future compliance issue within a certain proximity to the issue. The prohibition on "generic" language seems potentially inconsistent with language elsewhere in the Proposed Regulations and in the underlying statute, which defines "business purposes" for which service providers may use personal information to include, *inter alia*, "[p]erforming services on behalf of the business[.]"[12] For these reasons, and as proposed in **Appendix A**, we recommend that these provisions be deleted altogether.

Further, the requirements for third parties should not be tantamount to those that the CCPA contemplates for service provider and contractor relationships. The Proposed Regulations should reflect the differences between third parties, on the one hand, and service providers and contractors, on the other hand, that are manifest in the statute. Indeed, the statutory design is clear that businesses operate independently from any third party to which personal information is sold or shared. Under the CCPA, consumers have rights to opt out of the sale and sharing of their personal information with third parties, and those third parties, in turn, are subject to their own obligations under the CCPA to provide consumers with transparency and consumer rights.

As a result, it does not make sense to impose the kind of downstream third-party contract protections—such as restrictions on use of data to "specific" purposes—in agreements with third parties that are appropriate for a service provider relationship. Here too, the Proposed Regulations should defer to the relevant statutory language without adding new requirements that are not consistent with the statutory design.

b. Prescriptive privacy notice requirements should be clarified to avoid creating consumer confusion and to ensure consistency with the statute.

In the interest of crafting more consumer-friendly experiences, the Proposed Regulations should permit businesses to tailor their approach to privacy notices within the parameters of the statute, rather than creating requirements that make developing succinct and streamlined notices more difficult. We support Proposed Regulation Subsection 7003(a), which sets forth a general principle that disclosures should be easy to read and understandable to consumers. However, certain other elements of the proposed requirements relating to privacy notices are overly prescriptive, inconsistent with the statute, or unclear. We discuss examples of each point and propose specific revisions in this section and **Appendix A**.

[12] *See, e.g.,* Cal. Civ. Code § 1798.140(e)(5); Proposed Regulations § 7050(b)(1) ("to process or maintain personal information on behalf of the business").

The goal of providing privacy notices that are both meaningful and transparent to consumers would be undermined if businesses were subject to overly detailed content and format obligations for such notices. Requirements imposed by the Proposed Regulations, however, go beyond the information required under current rules or other U.S. privacy frameworks. For example, Subsection 7011(e)(1)(J) requires "[i]dentification of the specific business or commercial purpose for disclosing the consumer's personal information[,]" while Subsection 7012(e)(6) maintains that a business must include "the names of all the third parties . . . [or] information about the third parties' business practices" in its privacy notice "[i]f a business allows third parties to control the collection of personal information[.]"[13] Other provisions of the Proposed Regulations seem to contemplate cross-references to particular provisions of the Proposed Regulations.[14]

The Proposed Regulations similarly contemplate highly prescriptive expectations for linking to a privacy policy when a business relies on a privacy policy to provide notice at collection.[15] Such a requirement potentially limits the flexibility that businesses have to link to a privacy policy that contains information in different sections, even where that is the clearest presentation for consumers. It also creates significant confusion for non-California consumers. We recommend generalizing the requirements to permit businesses greater latitude to communicate effectively with consumers, both Californians and non-Californians alike.

The level of specificity dictated in the Proposed Regulations risks confusing and overloading consumers, rather than promoting transparency. This is particularly true for customers of financial institutions, as financial institutions must already provide multiple privacy notices to different categories of customers under federal privacy rules. The Proposed Regulations would prevent financial institutions from structuring notices to optimize transparency and clarity for these consumers.

c. Opt-out preference signal requirements do not include needed technical specifications and are inconsistent with the statute.

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.[16] In any event, to the extent some businesses honor opt-out preference signals, the Proposed Regulations should be clear and consistent in terms of the relevant requirements. For example, the Proposed Regulations should be clear that the obligations to

[13] *Compare with* Cal. Civ. Code § 1798.130(a)(5)(B)(iii), (iv) (requiring disclosure of "the business or commercial purpose for collecting or selling or sharing consumers' personal information" and "the categories of third parties to whom the business discloses consumers' personal information").

[14] *See* Subsection 7011(e)(1).

[15] Proposed Regulations § 7012(f) (providing that it is not adequate to direct a consumer to "another section of the privacy policy . . . so that the consumer is required to scroll through other information").

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

provide two or more designated methods for submitting requests to opt-out of sale/sharing[17] do not apply where a business processes an opt-out preference signal in a frictionless manner. This would ensure consistency with the provisions explaining that processing an opt-out preference signal in a frictionless manner obviates the requirement to post a link.[18] It also would better incentivize businesses to adopt opt-out preference signals.

Furthermore, the Proposed Regulations should include adequate technical specifications to afford businesses the guidance necessary to implement the opt-out preference signal. Implementing this solution will be a complex, and in some instances, multi-year effort. Promptly issuing technical specifications would make this development process more efficient and reduce the need for costly re-architectures in the future.

For this purpose, the CPRA charged the CPPA with "[i]ssuing regulations to define the requirements and technical specifications for an opt-out preference signal sent by a platform, technology, or mechanism[.]"[19] The Proposed Regulations, however, do not include adequate detail, which is critical to the successful implementation of the signal—particularly at a platform level. At a minimum, the Proposed Regulations should fully address all the categories of technical specifications that are specifically contemplated under Cal. Civ. Code § 1798.185(a)(19), including specifications to ensure that signals clearly represent a consumer's intent and be free of defaults constraining or presupposing such intent,[20] and to enable consumers to selectively consent to one business's processing of their personal information without affecting their preferences for other business.[21] This important language in Cal. Civ. Code Subsection 1798.185(a)(19) serves consumer autonomy.

The technical requirements for opt-out preference signals should be consistent with principles of consumer autonomy and recognize limitations in current technology. For example, notwithstanding language in Cal. Civ. Code § 1798.185(a)(19), Subsection 7025(c)(5) prohibits a business from interpreting the absence of an opt-out preference signal as consent to opt-in to the sale or sharing of personal information. If current technologies do not provide a separate opt-in option, then businesses *should* be able to interpret the absence of an opt-out preference signal as consent to opt-in.

In addition, the technical specifications also should address that universal opt-out preference signals must have sufficient scale to effectively communicate a consumer's opt-out preference signals across a large universe of websites, online platforms, and mobile applications. At this time, there is no universal opt-out preference signal capable of effectively communicating a consumer's opt-out preferences across websites, online platforms, and mobile applications.

[17] Proposed Regulations § 7026(a).

[18] *Id.* § 7025(e).

[19] Cal. Civ. Code § 1798.185(a)(19)(A).

[20] *Id.* § 1798.185(a)(19)(A)(iii).

[21] *Id.* § 1798.185(a)(19)(A)(v).

Finally, we note that Subsections 7026(f)(2) and (f)(3) require a business to notify certain third parties to whom the business has sold, shared, or made available a consumer's personal information of a consumer's request to opt-out of sale/sharing and to forward the consumer's opt-out request to "any other person with whom the person has disclosed or shared the personal information[.]" Both requirements go beyond the requirements of the statute and would be technically challenging, if not impossible, at the device level. The requirement to forward a consumer's request to any person with whom the person has disclosed or shared the information does not account for lawful disclosures to service providers, contractors, law enforcement, government agencies, or disclosures to other businesses or individuals pursuant to an explicit request or direction from the consumers to make the disclosure. We have included specific suggestions on language in **Appendix A**.

d. The Proposed Regulations should not impose new requirements to obtain "explicit consent" in ways that are inconsistent with the statutory design.

Language in the Proposed Regulations Subsection 7002(a) contemplates that a business should obtain "explicit consent" before processing personal information "for any purpose that is unrelated or incompatible with the purpose(s) for which the personal information [was] collected or processed." Such a provision would be inconsistent with the statutory design of the CCPA framework, which creates a number of *opt-out* rights for consumers. It also would be inconsistent with the plain language of Cal. Civ. Code Subsection 1798.100(a)(1), under which businesses must provide a consumer with *additional notice*—not obtain explicit consent—to use personal information in ways that are incompatible with the disclosed purposes for which personal information was collected initially.

To the extent that the Proposed Regulations provide examples of implementing Cal. Civ. Code Subsection 1798.100(c), they should focus on the data minimization principle—that is, to provide guidance about what it means to process personal information in a manner that is "necessary and proportionate" to disclosed processing purposes.

e. The Proposed Regulations should not disrupt the balance struck by the CCPA and CPRA between various privacy principles.

The CCPA and CPRA created clear exemptions reflecting a carefully negotiated balance between the statutory objectives and other important privacy principles, such as data minimization, understandability for consumers, and consumer choice. Key exceptions include, for example, prohibiting the re-identification or linking of consumers' personal information and clarifying that data regulated by sector-specific laws is not within the scope of the statute.[22] These exceptions are critical to helping consumers understand their rights and protections under the CCPA and CPRA.

Certain provisions in the Proposed Regulations, however, muddy these principles by failing to reflect the clear and plain language of the statute. For example, Subsection 7025(c)(1) requires a business, upon receipt of an opt-out preference signal, to "treat the [signal] as a valid

[22] *See, e.g.*, Cal Civ. Code §§ 1798.145(e), (j).

request to opt-out of sale/sharing . . . for that browser or device, and, if known, for the consumer." However, businesses typically do not maintain pseudonymous browser data with a customer's account or other identifiable data. As another example, the definition of "disproportionate effort" suggests that businesses might otherwise have obligations to respond to a consumer request with respect to personal information that is "not [maintained] in a searchable or readily-accessible format[.]"[23]

Consistent with the plain language of the statute and principles of data minimization, the rules should be clarified to avoid implying that businesses must (i) re-identify or link information that, in the ordinary course of business, is not maintained in a manner that would be considered personal information; (ii) maintain information in identifiable, linkable, or associable form; or (iii) collect, obtain, retain, or access any data or technology in order to be capable of linking or associating a verifiable consumer request with personal information. We have proposed specific language for such a clarification in **Appendix A**. Not only does such a clarification conform to the plain language of the statute, but it helps preserve the goals of data minimization that were preserved with nuanced statutory language.

These clarifications are more important in these Proposed Regulations than in past iterations of the statute and regulations, in light of new requirements established under Subsection 7025(a). The revisions would also enhance consumer privacy by encouraging businesses to maintain information in non-identifiable or non-linkable form in the ordinary course of business. For financial institutions, in particular, any requirement to link pseudonymous browsing data with a known customer or applicant could have the unintended effect of making more information subject to the GLBA and therefore exempt from the CCPA.

f. **Obligations to address requests to know or for deletion and correction should permit businesses more flexibility to address data security risks.**

Responding to consumer requests creates security challenges for all businesses, who must balance consumer rights with anti-fraud and security concerns—which, inherently, are in the interest of all consumers. Certain elements of the approach outlined in the Proposed Regulations exacerbate security risks, which is a particular problem for banks, who are frequent targets for fraud and other malicious activities due to the nature of their business. The consequences of such actions against banks, when successful, can be more severe than for other industries. We therefore propose amendments to these provisions to re-establish the balance between consumer rights and security, detailed in **Appendix A**.

For example, requirements relating to the right to know do not incorporate sufficient safeguards for consumer data. Specifically, businesses need latitude to withhold disclosure of "specific pieces of information" to consumers in consideration of security concerns. The Proposed Regulations should reinstate language clarifying that businesses should not provide consumers with specific pieces of personal information if the disclosure creates a substantial,

[23] *See* Proposed Regulations § 7001(h).

articulable and unreasonable risk to the customer or business's security.[24] If such information were to be compromised, malicious actors could use it to facilitate future fraudulent activity (e.g., spear phishing campaigns). Financial institutions are experienced actors in detecting and preventing such activities.

Also, with regard to data security, Subsections 7001(c) and 7063(b) of the Proposed Regulations would loosen safeguards pertaining to requests from authorized agents, providing more opportunities for malicious actors to engage in fraudulent activity. We recommend reinstating the requirements that authorized agents be registered California business entities and permitting businesses to require a power of attorney to use an authorized agent, as this may be necessary for consumer or business security in certain instances. We also recommend striking language that suggests that authorized agents may submit an opt-out preference signal without written permission from the consumer. It would not be consistent with the goals of consumer autonomy and control to require businesses to respond to requests from potentially rogue agents—whether they are malicious actors or just interested in interfering with businesses trying to comply with the requirements.

g. **The Proposed Regulations do not permit needed flexibility for businesses to respond to consumer rights requests.**

Aspects of the Proposed Regulations implement overly prescriptive requirements for handling data subject requests, risk confusing customers, and are not necessary to protect consumer interests. For example, Subsection 7022(f) states that where a business denies a customer's request to delete, it must "[p]rovide to the consumer a detailed explanation of the basis for the denial[.]" Even for personal information that is not subject to GLBA, heavily regulated entities, such as banks, have sophisticated mechanisms in place to support the integrity of their data—e.g., requirements to maintain information on historical account opening, historical transactions, and up-to-date credential and notification information. As a consequence of these existing requirements, the basis for denying a request to correct or delete information could result from a combination of factors, including regulatory and legal requirements, business needs, and fraud prevention purposes. Providing a detailed explanation for the basis of the denial in these circumstances would result in minimal corresponding benefit to consumers, while potentially confusing consumers about their rights under different legal frameworks.

Relatedly, Subsection 7023(f) requires a business denying a consumer's request to correct to, upon the consumer's request, "note both internally and to any person with whom it discloses, shares, or sells the personal information that the accuracy of the personal information is contested by the consumer." It is unclear what benefit would result from informing external parties that certain information is contested where the business has already arbitrated and denied the claim, and thus, where external parties would not take any further action.

[24] "A business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks." §999.313(c)(3).

We recognize that it would be challenging for the CPPA to promulgate separate rules tailored to each regulated industry. Instead, we urge the Agency to exempt entities already subject to quality and integrity requirements from these and related provisions. We have included specific suggestions on language in **Appendix A**.

h. Consumer rights are enforced most effectively directly by consumers.

The Proposed Regulations make businesses responsible for notifying third parties of consumer rights requests, even where the business is not the source of the relevant information. This allocation of responsibility is inefficient, and customers would be better served if they were directed to submit the relevant request at the information source.

For example, Subsection 7023(c) pertaining to correction rights requires that, "[a] business that complies with a consumer's request to correct shall correct the personal information at issue on its existing systems and implement measures to ensure that the information *remains corrected*." At the same time, Subsection 7023(i) provides that "[w]here the business is not the source of the information that the consumer contends is inaccurate, in addition to processing the consumer's request, the business shall provide the consumer with the name of the source from which the business received the alleged inaccurate information."

We recommend revising these provisions to clarify that the source of the inaccurate information is primarily responsible for ensuring that personal information is corrected at the source and remains corrected when transmitted to other parties. This could include, for example, amending Subsection 7023(i) to create optionality for businesses in responding to requests to correct.

We also recommend deleting Subsection 7022(b)(3), which requires businesses in receipt of a deletion request to notify "all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort . . . ." The statute affords consumers granular rights to exercise deletion requests of Business A, but not Business B, and vice versa. The Proposed Regulations should not presuppose consumer intent, but rather continue to allow consumers to exercise these choices more granularly with regard to individual businesses.

We have included specific suggestions on language in **Appendix A**. In the alternative, we recommend that entities regulated by broad compliance frameworks, including banks, be permitted greater flexibility in responding to customer rights requests to account for security concerns.

i. Employee and business customer data is distinct from general consumer data, making the application of new restrictions unclear and complex to implement.

Employee and commercial data (the latter referred to herein as "B2B" data) is fundamentally different from consumer data that is processed outside the context of an employment or commercial relationship, particularly as the CCPA is at its core a consumer protection statute. While there may be limitations on the Agency's authority to effectively amend the statute, it is well within the Agency's discretion to issue rules that further the purposes of the statute, which specifically observes that protections for employees and independent contractors should "tak[e] into account the differences in the relationship between employees or independent contractors and businesses, as compared to the relationship between consumers and businesses."[25]

Consistent with this statutory language, general consumer data protection rules should not be applied to employee and B2B contexts without careful consideration of their impact and analysis with other commercial legal frameworks and employment laws. The Agency has not yet done that affirmatively. Indeed, the examples and detail provided throughout the Proposed Regulations exclusively focus on consumer data rather than the employment and commercial contexts. For example, Subsection 7027(l) 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 seven examples seem to contemplate processing activities that would be relevant for employee or B2B data.

Accordingly, we recommend that the CPPA clarify that the Proposed Regulations do not apply in employment or B2B contexts until there is a separate rulemaking. The compressed timeline for implementing the Proposed Regulations will be particularly infeasible for B2B and employment data.

j. **The dates the Proposed Regulations become effective and enforceable should be extended to correspond to the statutory design.**

BPI is committed to supporting the Agency's efforts to expeditiously adopt implementing rules for the protection of consumer data that are pragmatic and consistent with the statute. However, that process takes time and the Agency has already announced that the rules will be finalized well after the July 1, 2022 date required by the statutory schedule. Indeed, the initial comment period was not open by that date.

In light of this delay, we encourage the Agency to extend the effective date of any implementing rules. Extending the date by twelve (12) months—at the earliest, January 1, 2024—would be consistent with the statutory design, which clearly contemplated that businesses should have a year to implement requirements of the law and regulations before enforcement of such rules would begin—and that is particularly important where the final rules create new substantive obligations (e.g., in the employment and B2B contexts).[26]

In the alternative, we recommend extending the effective date of any implementing rules to at least July 1, 2023, which would align with the statutory date for administrative enforcement. The Agency cannot enforce the new requirements in advance of July 1, 2023 in any event, and this would afford businesses that take seriously their legal compliance obligations with at least some lead time before the rules are finalized to adopt appropriate controls. The Proposed

[25] CPRA, § 3.

[26] Cal. Civ. Code § 1798.185(d).

Regulations go well beyond implementing the statute. If the Agency is going to create ambitious new privacy protections, then it should ensure that the rulemaking process is transparent, open-minded, and methodical,[27] and the Agency must also provide businesses with fair and reasonable notice to come into compliance with the new obligations.

*****

As noted above, **Appendix A** includes proposed amendments to address the above concerns. In addition, **Appendix A** sets out some initial clarifying edits that are important for the Agency to consider.

The Bank Policy Institute appreciates the opportunity to submit comments on the CPPA's proposed regulations implementing the CPRA. If you have any questions, please contact the undersigned by phone at 202-589-1935 or by email at Angelena.Bradfield@bpi.com.

Respectfully submitted,

Angelena Bradfield

Angelena Bradfield
Senior Vice President
AML/BSA, Sanctions & Privacy
Bank Policy Institute

[27] Likewise, the economic analysis that the Agency performs as part of its rulemaking process should reflect the magnitude of investment that businesses are and will continue to make to comply with the CPRA, including analysis of the level of investment that multinational companies undertook to comply with GDPR and, in 2020, the CCPA. Further, to the extent the Agency retains the most prescriptive elements of the Proposed Regulations, it should consider the economic impact that will result if businesses operate separate online services and customer interfaces with California residents to avoid confusing non-Californians.

IV. Appendix A

Gray rows provide detail on points made in Part III. White rows include additional examples and/or points not addressed in Part III.

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
Section III.a – Contract Requirements		
Proposed Regulations §§ 7051, 7053 Cal. Civ. Code §§ 1798.100(d), 1798.140(e)(5), (j), (ag)	Service provider and third party contract requirements have been sufficiently defined in the statutory text and previous regulations. The proposed requirements do not serve to align the CCPA's contract requirements more closely with other statutory frameworks, such as the GDPR, but instead impose stricter requirements on third party contracting. Accordingly, additional prescriptive requirements should be deleted.	*Delete contract requirements in Proposed Regulations Subsections 7051 and 7053.*
Proposed Regulations §§ 7050(b)(2), 7051(a), 7053(a) Cal. Civ. Code § 1798.140(e)(5)	The prohibition against describing business purposes "in generic terms" is inconsistent with the statute and other sections of the Proposed Regulations.	*In the alternative to deleting § 7051 altogether, amend § 7051:* "The contract required by the CCPA for service providers and contractors shall . . . Identify the specific business purpose(s) and service(s) for which the service provider or contractor is processing personal information on behalf of 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 or service shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.~~" *Apply corresponding edits to similar language in Subsection 7053(a).*

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
Proposed Regulations § 7051(a)(8) Cal. Civ. Code § 1798.100(d)(4)	The requirement that service providers and contractors notify the business within five days after determining that it cannot fulfill its CCPA obligations deviates from the statute and is overly prescriptive. Businesses are best situated to define the appropriate notification timeline on a case-by-case basis, based on the nature of the information and parties' relationship. Furthermore, standard contract provisions (e.g., those requiring compliance with applicable law) sufficiently incentivize parties to comply with the CCPA / CPRA.	*In the alternative to deleting § 7051 altogether, amend § 7051(a)(8):* “Require the service provider or contractor to notify the business ~~no later than five business days~~ within a reasonable time frame specified by the business after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.”
Section III.b – Privacy Notices		
Proposed Regulations § 7011(b) Cal. Civ. Code § 1798.130(5)(B)(iii)	Prescriptive requirements pertaining to the form and content of privacy notices exceed the statutory text and risk confusing consumers. The Proposed Regulations should include an alternative provision clarifying that businesses may forego the prescriptive requirements where they demonstrate a more consumer-friendly and privacy-protective approach.	*Amend § 7011(b):* “The privacy policy shall comply with section 7003, subsections (a) and (b), including as to the interpretation and implementation of the requirements of this section 7011.” *Conforming edits should be made to §§7012(b), 7013(b), 7014(b), & 7016(b).*
Proposed Regulations § 7012(e)(6); *see also* § 7012(g)(2) Cal. Civ. Code § 1798.130(5)(B)(iv)	Prescriptive requirements pertaining to the form and content of privacy notices exceed the statutory text and risk confusing consumers.	*Amend § 7012(e)(6):* “If a business allows third parties to control the collection of personal information, the ~~names~~ categories of all the third parties; or, in the alternative, general information about the third parties' business practices.”
Proposed Regulations § 7011(e)(3)(J) Cal. Civ. Code § 1798.130(a)(1)	Designating particular contact methods in privacy notices inhibits businesses from adopting the simplest and most efficient means for addressing consumers' questions and requests. Many	*Amend § 7011(e)(3)(J):* “A contact for questions or concerns about the business's privacy policies and practices ~~using a method reflecting the manner in which the~~, which take account the manner in which

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
	financial institutions use a combination of in-person, telephone, and online means to interact with customers, making the identification of a primary method of interaction difficult.	the business ~~primarily~~ interacts with ~~the~~ consumers.”
Proposed Regulations § 7012(f) Cal. Civ. Code § 1798.100(a)(1)	The requirement that notice at collection must direct the consumer to a specific section of the privacy policy will complicate business’s efforts to provide transparent disclosures to consumers, particularly where a business is subject to additional privacy frameworks. This approach limits business’s ability to prioritize providing consumers easy-to-find information that is most relevant to them in light of the constellation of required privacy notices and disclosures.	*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.~~”
Proposed Regulations §§ 7010(b); *see* 7012(a) Cal. Civ. Code § 1798.100	In explaining obligations to provide notice at collection, the Proposed Regulations remove the reference to collecting personal information “from a consumer,” suggesting that the online notice must cover personal information obtained from third parties as well as directly from consumers. The existing regulations’ language should be restored to ensure consistency with Subsection 7012(a) (“…to be collected from *them*” (emphasis added)).	*Amend § 7010(b):* “A business that controls the collection of a consumer’s personal information from a consumer shall provide a notice at collection in accordance with the CCPA and section 7012.”
Section III.c – Opt-Out Preference Signal & Statutory Consistency		

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
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), (c)(1),(3)–(4), 7026(a), etc.*
Proposed Regulations §§ 7025(b), (c)(5) Cal. Civ. Code §§ 1798.135(b), 1798.185(a)(19)–(20)	According to requirements set out in the CPRA, the Agency should provide technical specifications for the opt-out preference signal, particularly at the platform level. For example, designing a useable opt-out preference signal that most accurately reflects consumers' preferences with regard to the use of their data requires symmetry and sufficient granularity of choice. The Proposed Regulations should attempt to capture consumers' choices as accurately as possible, rather than skewing their selections towards opt-out. Taking into account the requirements built into Subsection 7025(b), businesses should be able to rely on the absence of a signal to determine that a consumer has consented to the sharing of their personal information.	*Include technical specifications for opt-out preference signals under §§ 7025 and 7026.* *For example, amend § 7025(b):* "To the extent that a business processes ~~A business shall process~~ ~~any~~ opt-out preference signals, those signals that meet~~s~~ the following requirements shall be considered valid ~~as a valid~~ requests to opt-out of sale/sharing: (1) The signal shall be in a format commonly used and recognized by ~~businesses~~ websites, online platforms, and mobile applications. ~~An example would be an HTTP header field.~~ (2) The signal shall be widely recognized by websites, online platforms, and mobile applications. (3) The platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, whether in its configuration or in disclosures to the public, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information. The configuration or disclosure

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		does not need to be tailored only to California or to refer to California. (4) The platform, technology, or mechanism that sends the opt-out preference signal shall provide symmetry of choice, clearly represent a consumer's intent, and be free of defaults constraining or presupposing that intent. (5) The platform, technology, or mechanism that sends the opt-out preference signal shall provide a mechanism for the consumer to selectively consent to a business' sale of the consumer's personal information, or the use or disclosure of the consumer's without affecting the consumer's preferences with respect to other businesses or disabling the opt-out preference signal globally." *Amend § 7025(c)(5):* "When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b) . . . ~~A business shall not interpret the absence of an opt-out preference signal after the consumer previously sent an opt-out preference signal as consent to opt-in to the sale or sharing of personal information.~~"

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
Proposed Regulations §§ 7025(e), 7026(a) Cal. Civ. Code §§ 1798.135(a)–(b), 1798.185(a)(19), (20)	The Agency should reconcile more stringent requirements for processing opt-out preferences under the Proposed Regulations with the alternative processes established under the CPRA. It should also clarify that posting links is not required where a business uses a frictionless opt-out preference signal applicable to the full scope of shared data.	*Amend 7025(e):* "Civil Code section 1798.135, subdivisions (b)(1) and (3), provides a business the choice between (1) processing opt-out preference signals and providing the "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links or the alternative opt-out link; or (2) processing opt-out preference signals in a frictionless manner in accordance with these regulations and not having to provide the "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links or the alternative opt-out link. ~~It does not give the business the choice between posting the above-referenced links or honoring opt-out preference signals. Even if the business posts the above-referenced links, the business must still process opt-out preference signals, though it may do so in a non-frictionless manner.~~ If a business processes opt-out preference signals in a frictionless manner in accordance with subsections (f) and (g) of this regulation, then it may, but is not required to, provide the above-referenced links." *Amend § 7026(a):* "A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing, unless the business honors the opt-out-preference signal in a frictionless manner for all relevant shared data.. . . . A business that

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		collects personal information from consumers online shall~~, at a minimum,~~ allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal in a frictionless manner in accordance with subsections (f) and (g) of section 7025 of this regulation ~~and~~or through an interactive form accessible via the “Do Not Sell My Personal Information” link, the alternative opt-out link, or the business’s privacy policy.”
Section III.d – Explicit Consent		
Proposed Regulations § 7002(a) Cal. Civ. Code § 1798.100(a)(1)	Requirements under the Proposed Regulations suggesting that explicit consent is required in circumstances that are not compatible with an average consumer’s expectations are inconsistent with the statute. The statute requires the provision of notice prior to collecting new categories of personal information or using collected data for new purposes not initially disclosed. Further, the notion of explicit consent is at odds with the overall statutory design, which contemplates that consumers will be provided notice and choice with regard to a business’s processing activities.	*Amend § 7002(a):* “A business’s collection, use, retention, and/or sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purpose(s) for which the personal information was collected or processed. ~~To be reasonably necessary and proportionate, the business’s collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected.~~ A business’s collection, use, retention, and/or sharing of a consumer’s personal information may also be for other disclosed purpose(s) if they are compatible with what is reasonably expected by the average consumer. A business shall ~~obtain the consumer’s explicit consent in accordance with section 7004~~ provide additional notice to the consumer before collecting, using, retaining, and/or sharing the consumer’s personal information

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		for any purpose that is unrelated or incompatible with the purpose(s) for which the personal information collected or processed.”
Section III.e – Balance of Privacy Principles		
Proposed Regulations § 7025(c)(1) Cal. Civ. Code § 1798.145(j)	Opt-out preference signal requirements in the Proposed Regulations should avoid the implication that a business must re-identify or link data not otherwise maintained in that state to comply with the signal.	*Amend § 7025(c)(1):* “When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b): . . . The business shall treat the opt-out preference signal as a valid request to opt-out of sale/sharing submitted pursuant to Civil Code section 1798.120 for that browser or device~~, and, if known, for the consumer~~.”
Proposed Regulations §§ 7001(h), 7022(b)(3) (*and similar provisions*) Cal. Civ. Code § 1798.145(j)	The Proposed Regulations should clarify that its requirements never necessitate re-identifying or linking data with a customer where it is not already maintained in that format. We recommend clarifying this approach across the Proposed Regulations by adding a new § 7000(c).	*Add a new § 7000(c):* “(c) No provision of these regulations (1) shall require a business to maintain information in identifiable, linkable, or associable form, or collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating the consumer's request with personal information or (2) otherwise be construed to regulate any activity or data or impose any obligations in a manner that is inconsistent with the CCPA.”
Proposed Regulations §§ 7026(f)(4) and 7027(g)(5) Cal. Civ. Code §§ 1798.120, 1798.121	The Proposed Regulations contemplate that businesses have obligations to provide consumers with the means to confirm that their request to opt-out of sale/sharing and/or a request to limit has been processed. Maintaining this information for noncustomers is contrary to principles of data minimization, and thus, it should be sufficient that the business responds	*Delete § 7026(f)(4):* “~~Providing a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business. For example, the business may display on its website “Consumer Opted Out of Sale/Sharing” or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.~~”

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
	affirmatively to the consumer's request.	*Delete § 7027(g)(5):* "~~Providing a means by which the consumer can confirm that their request to limit has been processed by the business. For example, the business may display through a toggle or radio button that the consumer has limited the business's use and sale of their sensitive personal information.~~"
Sections III.f – Data Security		
Proposed Regulations § 7024(c) Cal. Civ. Code §§ 1798.110, 1798.145	The Proposed Regulations should make clear that specific pieces of information need not be provided in response to a request to know where the disclosure would create a security risk for customers or the business, consistent with a previous draft of the AG regulations. §999.313(c)(3).	*Amend § 7024(c):* "A business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks. Neither shall the business provide such information if the consumer's request is intended to or has the effect of circumventing rules of discovery pertaining to an ongoing litigation. In responding to a request to know, a business is not required to search for . . ."
Proposed Regulations § 7001(c), 7063(b) Cal. Civ. Code §§ 1798.130(a)(3), 1798.185(a)(7)	The Proposed Regulations should permit businesses to impose more stringent security safeguards on requests from authorized agents in the interest of consumer and business security.	*Amend § 7001(c):* "'Authorized agent' means a natural person or a business entity registered with the Secretary of State to conduct business in California that a consumer has authorized to act on their behalf subject to the requirements set forth in section 7063." *Amend 7063(b):* "Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		Probate Code sections 4121 to 4130. ~~A business shall not require a power of attorney in order for a consumer to use an authorized agent to act on their behalf.~~"
Proposed Regulations § 7026(i)	The Proposed Regulations should strike language suggesting that authorized agents may submit an opt-out preference signal without written permission from the consumer. It would not be consistent with the goals of consumer autonomy and control to require businesses to respond to requests from potentially rogue agents—whether they are malicious actors or just interested in interfering with businesses trying to comply with the requirements.	*Amend § 7026(i):* "A consumer may use an authorized agent to submit a request to opt-out of sale/sharing on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. ~~The requirement to obtain and provide written permission from the consumer does not apply to requests made by an opt-out preference signal.~~"
Section III.g – Rights to Correct and Delete		
Proposed Regulation §§ 7022(f), 7023(f)	Entities regulated under other legal privacy frameworks should be exempt from certain prescriptive requirements relating to the rights to correction and deletion.	*Amend § 7022(f):* "In cases where a business denies a consumer's request to delete in whole or in part, the business shall . . . Provide to the consumer a detailed explanation of the basis for the denial, including any conflict with federal or state law, or exception to the CCPA, or factual basis for contending that compliance would be impossible or involve disproportionate effort, unless prohibited from doing so by law[.] This requirement shall not apply to businesses that are subject to federal laws or regulations governing the quality and integrity of personal information maintained by the business."

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		Amend § 7023(f): "In responding to a request to correct, a business shall inform the consumer whether or not it has complied with the consumer's request. If the business denies a consumer's request to correct in whole or in part, the business shall . . . Inform the consumer that, upon the consumer's request, it will note both internally and to any person with whom it discloses, shares, or sells the personal information that the accuracy of the personal information is contested by the consumer. The business does not have to provide this option for requests that are fraudulent or abusive. This requirement shall not apply to businesses that are subject to federal laws or regulations governing the quality and integrity of personal information maintained by the business."
Proposed Regulations § 7023(b) Cal. Civ. Code § 1798.106	The "totality of the circumstances" standard proposed for arbitrating requests to correct is ambiguous. In those same circumstances where businesses do not have obligations to delete data, it should be clear that businesses do not have obligations to correct data.	*Amend § 7023(b):* "In determining the accuracy of the personal information that is the subject of a consumer's request to correct, the business shall consider the totality of the circumstances relating to the contested personal information. A business may deny a consumer's request to correct if it is reasonably necessary to maintain the consumer's personal information without correction for any of the activities set forth in Cal. Civ. Code § 1798.105(d) or the business ~~it~~ determines that the contested personal information is more likely than not accurate based on the totality of the circumstances.

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		(1) Considering the totality of the circumstances includes, but is not limited to, considering: (A) The nature of the personal information (e.g., whether it is objective, subjective, unstructured, sensitive, etc.). (B) How the business obtained the contested information. (C) Documentation relating to the accuracy of the information whether provided by the consumer, the business, or another source. Requirements regarding documentation are set forth in subsection (d). (2) If the business is not the source of the personal information and has no documentation to support of the accuracy of the information, the consumer's assertion of inaccuracy may be sufficient to establish that the personal information is inaccurate. (3) In no event shall the business be held liable under this title for its decision as to the accuracy of the personal information under section 7023(b) unless the business is shown to have acted in bad faith in applying the totality of the circumstances standard or failed to apply the standard."
Proposed Regulations § 7023(d) Cal. Civ. Code § 1798.106	Documentation provisions associated with requests to correct hinder businesses from implementing more efficient and less resource-intensive processes for arbitrating consumer requests. Additionally, consumer interests would be better served by requiring more documentation for high impact issues, not less. These issues have the potential to carry the	*Amend § 7023(d)(1):* "A business shall accept, review, and consider any documentation that the consumer provides in connection with their right to correct whether provided voluntarily or as required by the business, unless the business has reason to believe that the documentation provided is irrelevant, excessive, or fraudulent. If the business does not review

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
	heaviest consequences for consumers and should be subject to a more stringent assessment.	documentation submitted by a customer, it must document its reasoning.” *Amend § 7023(d)(2)(D):* “A business may require the consumer to provide documentation if necessary to rebut its own documentation that the personal information is accurate. In determining the necessity of the documentation requested, the business shall consider the following: . . . The impact on the consumer. For example, if the personal information has a high impact on the consumer, the business may require ~~less~~ more documentation.”
Proposed Regulations § 7023(j) Cal. Civ. Code § 1798.130(b)	Consistent with the plain language of the statute, consumers should not be permitted more than two opportunities to make requests to know per year. Subsection 7023(j) effectively operates as a right to know, and thus arguably contradicts the statutory text, which limits a consumer to two disclosure requests per year.	*Amend § 7023(j):* “Upon request, a business shall disclose all the specific pieces of personal information that the business maintains and has collected about the consumer to allow the consumer to confirm that the business has corrected the inaccurate information that was the subject of the consumer’s request to correct. This disclosure shall ~~not~~ be considered a response to a request to know that is counted towards the limitation of two requests within a 12-month period as set forth in Civil Code section 1798.130, subdivision (b).”
Proposed Regulations § 7022(b)(1), (d) Cal. Civ. Code § 1798.105	With regard to requests to delete, business’s obligations for archived and back-up systems are ambiguous. The Proposed Regulations state that these systems are exempt from deletion requests, but also allow compliance with a deletion request affecting them to	*§ 7022(b)(1) for reference:* “A business shall comply with a consumer’s request to delete their personal information by . . . [p]ermanently and completely erasing the personal information from its existing systems except archived or back-up systems,

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
	be "delayed" in certain circumstances.	deidentifying the personal information, or aggregating the consumer information[.]" *Amend § 7022(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 is not required for those systems~~, with respect to data stored on the archived or backup system,~~ unless and until 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. For the purposes of this provision, 'access' does not include de minimis or transient access for the purposes of maintenance, information security, fraud prevention, or system improvement."
Section III.h – Allocation of Responsibility with Service Providers, Contractors, and Third Parties		
Proposed Regulations §§ 7023(c), (c)(1), (i) Cal. Civ. Code § 1798.106	In response to requests to correct, the Proposed Regulations should clarify that the responsibility for correcting inaccurate information rests with the third party source of the information, rather than the business by default. This approach places responsibility for the correction with the entity most able to remedy the problem.	*Amend § 7023(i):* "Where the business is not the source of the information that the consumer contends is inaccurate, in addition to processing the consumer's request, the business shall either provide the consumer with the name of the source from which the business received the alleged inaccurate information or communicate the consumer's request to the source to make the necessary corrections in its systems." *Amend § 7023(c):* "A business that complies with a consumer's request

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		to correct shall correct the personal information at issue on its existing systems and, where the business is not the source of the information that the consumer contends is inaccurate, then ~~implement measures to~~ help the consumer ensure that the information remains corrected by complying with subsection 7023(i). The business shall also instruct all service providers and contractors that maintain the personal information at issue in the course of providing services to the business to make the necessary corrections in their respective systems.” *Amend § 7023(c)(1):* “Business L maintains personal information about consumers that it receives from data brokers on a regular basis. Business L generally refreshes the personal information it maintains about consumers whenever it receives an update from a data broker. Business L receives a request to correct from a consumer and determines that the information is inaccurate. To comply with the consumer’s request, Business L corrects the inaccurate information in its system and ~~ensures that the corrected personal information is not overridden by inaccurate personal information subsequently received from the data broker~~informs the consumer of the data broker from which the business received the alleged inaccurate information or informs the data broker of the consumer’s request and instructs the data broker to make the

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		necessary corrections in its respective systems.”
Proposed Regulations § 7022(b)	The Proposed Regulations should provide greater flexibility for businesses to address deletion requests where information shared with or sold to third parties is implicated to improve efficiency for consumers and reduce the administrative burden on businesses.	*Delete Proposed Regulation § 7022(b)(3).*
Proposed Regulations §§ 7026(f)(2)–(3)	The Proposed Regulations should be conformed with the statute which provides businesses with 15 days to honor opt out requests. Further, the rules should not impose requirements that would be infeasible, if not technically impossible, at the device level without businesses collecting much more information about consumers and their devices.	*Strike Proposed Regulations § 7026(f)(2) and (f)(3).*
Section III.i – B2B and Employee Data		
Proposed Regulations § 7000 Cal. Civ. Code § 3(A)(8), § 1798.145(m), (n)	The Proposed Regulations insufficiently account for use cases particular to the employee and B2B data. The Agency should carve out these categories from the existing regulations to consider the implications of the rules to these categories of data in more detail.	*Add a new § 7000(d):* “(d) To provide the Agency with time to adopt appropriate requirements, these regulations and the California Consumer Privacy Act shall not, without amendment to these regulations, apply to personal information that is subject to Cal. Civ. Code § 1798.145(m) or § 1798.145(n), irrespective of whether those subdivisions are operative.”
Section III.j – Effective and Enforcement Dates		
Proposed Regulations § 7000 Cal. Civ. Code § 1798.185(d)	To adhere to the statutory timeline, dates the Proposed Regulations are effective and enforceable should be extended by twelve months.	*Add new § 7000(e):* “These regulations shall become operative not less than one year after the date on which these regulations are finalized.”

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
Other Comments – Audit Rights and Complainant Notice		
Proposed Regulations § 7304(b) Cal. Civ. Code §§ 1798.185(a)(18), 1798.199.50–55, 1798.199.65	The audit authority conferred on the Agency is overbroad and lacking reasonable limits for the initiation of an audit.	*Amend § 7304(b):* "Criteria for Selection. The Agency may conduct an audit to investigate possible violations of the CCPA if it determines that it has Probable Cause with regard to a particular subject. ~~Alternatively, the Agency may conduct an audit 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 CCPA or any other privacy protection law.~~"
Proposed Regulations § 7300(b) Cal. Civ. Code § 1798.199.45	Complainant notice requirements should be limited to avoid publicizing Agency investigatory actions prematurely, which has the potential to cause severe reputational impact on businesses before evidence of a violation has been uncovered.	*Amend § 7300(b):* "After Notice (as defined in Cal. Civ. Code § 1798.199.50) has been made, ~~T~~the Enforcement Division ~~will~~ may notify the complainant in writing of the action, if any, the Agency has taken or plans to take on the complaint, together with the reasons for that action or nonaction. Duplicate complaints submitted by the same complainant may be rejected without notice."
Other Comments – Ambiguous Standards and Statutory Inconsistencies		
Proposed Regulations § 7004(c) Cal. Civ. Code § 1798.140(l)	The proposed intent provision relating to dark patterns would effectively impose a strict liability standard for user interfaces. It is common for businesses of all sizes to experience problems with their websites and other features, caused by no negligence or malicious intent. The Proposed Regulations should not hold businesses responsible for issues that they could not have prevented.	*Amend § 7004(c):* "A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice~~, regardless of a business's intent~~, and if the business responsible for the user interface offered it to customers knowing that it was likely to have that effect."

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
Proposed Regulations § 7010(e), 7016 Cal. Civ. Code § 1798.125(b)	The Proposed Regulations create disclosure and other obligations for the collection of personal information in exchange for a financial incentive or price / service difference. Consistent with the plain language of the statute, the Proposed Regulations should not regulate as financial incentives or price/service differences any incentives or differences that are not directly related to a consumer's exercise of her rights under the CCPA.	*An additional example of what is not a financial incentive should be provided to make this more clear.*
Proposed Regulations § 7004 Cal. Civ. Code § 1798.185(a)(7)	Although BPI supports the principle of usability with regard to consumer request submission methods, specifying that broken links could indicate legal noncompliance is excessive. We recommend removing such specific examples in favor of emphasizing the overarching principle.	*Amend § 7004(a)(5)*: "Easy to execute. The business shall not add unnecessary burden or friction to the process by which the consumer submits a CCPA request. Methods should be tested to ensure that they are functional and do not undermine the consumer's choice to submit the request. ~~Illustrative examples follow. . . . Circular or broken links, and nonfunctional email addresses, such as inboxes that are not monitored or have aggressive filters that screen emails from the public, may be in violation of this regulation.~~" *We recommend deleting similarly specific illustrative examples under this subsection.*
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	*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

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
	businesses *shall* affirmatively provide the information.	collected and maintains about the consumer 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. That information shall include any personal information that the business’s service providers or contractors obtained as a result of providing services to 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.~~”
Proposed Regulations § 7052(a) Cal. Civ. Code § 1798.105(c)(1), 1798.140(ah)	The Proposed Regulations imply that a third party that receives a request to delete or to opt-out of sale/sharing of a consumer’s personal information from a business must comply with the request in the same way that the business must. To ensure consistency with the statutory text, the CPPA should clarify that this requirement is limited to third parties that received the personal information for the purposes of behavioral advertising or pursuant to a sale of the relevant information.	*Amend § 7052(a):* “A third party to whom a business has sold or shared a consumer’s personal information shall comply with a consumer’s request to delete or request to opt-out of sale/sharing forwarded to them from a business that provided, made available, or authorized the collection of the consumer’s personal information. The third party shall comply with the request in the same way a business is required to comply with the request under sections 7022, subsection (b), and 7026, subsection (f). The third party shall no longer retain, use, or disclose the personal information

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		unless the third party becomes a service provider or contractor that complies with the CCPA and these regulations."
Other Comments – Sensitive Personal Information		
Proposed Regulations § 7027 Cal. Civ. Code § 1798.121(d)	The Proposed Regulations should be mindful that the right to limit does not apply to "[s]ensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer."	*Amend § 7027(a):* "The unauthorized use or disclosure of sensitive personal information creates a heightened risk of harm for the consumer. The purpose of the request to limit is to give consumers meaningful control over how their sensitive personal information is collected, used, and disclosed. It gives the consumer the ability to limit the business's use of sensitive personal information to that which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, with some narrowly tailored exceptions, which are set forth in subsection (l) and Cal. Civ. Code § 1798.121(d)."
Proposed Regulations § 7027(l) Cal. Civ. Code §§ 1798.121(a)–(b), 1798.140, 1798.185(19)(C)	The list of permissible uses for Sensitive Personal Information captured in § 7027(l) are too narrow and fail to capture important use cases for which Sensitive Personal Data is likely to be necessary.	*Add § 7027(l)(8):* "The purposes for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit are as follows. A business that only uses or discloses sensitive personal information for these purposes is not required to post a notice of right to limit. . . . For compliance and reporting purposes, such as completing regulatory reporting, creating Suspicious Activity Reports (SARs), responding to judicial, administrative, regulatory, or law enforcement inquires, and executing investigations, orders, warrants, and subpoenas."