August 23, 2022

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

Via email to regulations@cppa.ca.gov

Subject: Public Comment on Notice of Proposed Rulemaking (July 8, 2022)

Dear California Privacy Protection Agency:

Biocom California and the International Pharmaceutical & Medical Device Privacy Consortium ("IPMPC") welcome the opportunity to provide comments on the Agency's proposed regulations implementing the Consumer Privacy Rights Act of 2020 ("CPRA") and revising the regulations issued previously under the California Consumer Privacy Act of 2018 ("CCPA").

Biocom California is the state's premier life sciences organization representing over 1,700 member companies throughout California. Biocom California is a leading voice in the advocacy efforts of the California life science community whose members include biotechnology, pharmaceutical, medical device, genomics and diagnostics companies of all sizes, research universities and institutes, clinical research organizations, investors and service providers.[1]

The IPMPC is comprised of chief privacy officers and other data privacy and security professionals from a number of research-based, global pharmaceutical and medical-device manufacturers. The IPMPC is the leading voice in the global pharmaceutical and medical device industry to advance innovative privacy solutions to protect patients, enhance healthcare, and support business enablement.[2]

Our specific comments are below, but we would like to make a few general observations. First, we thank the Agency for including examples illustrating key concepts and providing interpretive insight. These examples are critical to structuring effective privacy compliance programs. Second, we would urge the Agency to add even more examples to the draft regulations. Many of the concepts discussed would benefit from a practical, real-world illustration showing how the Agency views the matter at hand.

[1] More information about Biocom California is available at https://www.biocom.org. These comments reflect the position of the Biocom California as an organization and should not be construed as the positions of any individual member.

[2] More information about the IPMPC is available at https://www.ipmpc.org. These comments reflect the position of the IPMPC as an organization and should not be construed as the positions of any individual member.

Finally, we ask the Agency to develop and release sample notices and data subject responses. We appreciate that the CPRA and the Agency have urged businesses to present information to consumers in clear and understandable ways. However, the CPRA and draft regulations also require that this information be comprehensive and detailed. As science-based organizations, we are mindful that detailed and comprehensive descriptions may not always be simple or easy to understand. We work continuously to ensure that our communications can be understood by patients and caregivers, but we would appreciate further guidance from the Agency about its expectations.

§7002(b)(2) Restrictions on the Collection and Use of Personal Information, example involving cloud storage services for consumers.

We request that this example be clarified to avoid implying that deletion of consumer data is required in all cases once a consumer ends its business relationship with a company.

Other sections of the CPRA (including the exceptions to the consumer's right to deletion) acknowledge that data may be retained for permissible purposes or in archive or back-up forms. We encourage the Agency to make it clear that the general requirement that "collection, use, retention or sharing of data be necessary and proportionate to the purposes" for which the information was originally collected does not override more specific language found elsewhere in the CPRA and the draft regulations about specific situations in which data may be permissibly used and retained.

§ 7014(a) Notice of Right to Limit and the "Limit the Use of My Sensitive Personal Information" Link.

This provision states that the "purpose of the 'Limit the Use of my Sensitive Personal Information' link is to immediately effectuate the consumer's right to limit, or in the alternative, direct the consumer to the notice of the right to limit." (emphasis added). We believe the word "immediately" could lead to confusion – elsewhere, the regulations permit a business to implement a request to limit the use of a consumer's sensitive information "as soon as feasibly possible," but always within 15 days. See §7027(g)(1). We encourage the Agency to remove the word "immediately" in §7014(a) to avoid contradiction.

§ 7022(c)(4). Requests to Delete, notification to other parties.

We request that this language be clarified. The use of the word "may" creates ambiguity: "Notifying any other service providers, contractors, or third parties that may have accessed personal information . . . ." We assume the Agency wishes to require notification to anyone who did access personal information, not to anyone who simply could have accessed personal information (including those that, in fact, did not). Omitting "may have" in the quoted language would leave a clearer regulatory requirement.

§ 7022(f)(1). Requests to Delete, denials by a business.

We ask that the Agency provide examples of the kind of information that would satisfy the requirement for a "detailed explanation" of the basis for denial. The regulations currently require that the basis be "described." The change from "described" to "detailed explanation" suggests the Agency anticipates businesses will provide the consumer with more information than they had previously. But the substantive requirement to identify a conflict with federal or state law or an exemption to the CCPA has not changed, so it is not clear what other information the Agency wants businesses to provide.

§ 7025(b). Opt-Out Preference Signals, requirements for valid requests.

The Agency should identify and provide technical examples of formats that are "commonly used and recognized by businesses." We do not believe that there is a common and recognizable format for opt-out signals in the market at this time. We suggest that the Agency identify a particular technology or standard format and provide for an implementation period before any of the related regulations come into effect. This would allow technologists and businesses to develop compliance tools that work as the Agency intends. Regulatory endorsement of a particular approach would speed adoption and improve compliance.

§ 7025(e). Opt-Out Preference Signals, processing choices.

The Agency's statement that 1798.135(b) "does not give the business a choice between posting the above-referenced links or honoring opt-out preference signals" appears contrary to the plain language on 1798.135(b) and other provisions of the CPRA. 1798.135 clearly sets up two approaches for facilitating opt-out requests – a business can either post the links or honor consumer opt-out "signals." Doing both, as the Agency suggests, is not required. 1798.135(b)(3) makes it very clear that "a business may elect whether to comply with subdivision (a) [posting links] or (b) [honoring opt-out signals]."

This clear statement is further supported by the text of 1798.135(b)(1), which states that a business is not required to post Do Not Sell or Share links "if the business allows" (emphasis added) consumers to opt-out via an "opt-out preference signal." The use of "if" and "allow" clearly indicate that honoring opt-out preference signals is not required under the CPRA. The use of the word "allows" is repeated in 1798.135(b)(2). In addition, the delegation of rule-making authority to the Agency in 1798.185(a)(20) empowers the Agency to make regulations that govern how "a business that has elected to comply with subdivision (b) of Section 1798.135 responds to the opt-out preference signal" (emphasis added). All of this language indicates that businesses have a choice between posting links or honoring opt-out signals.

The Agency's proposed approach requires businesses to allow consumers to opt-out via a preference signal. This is inconsistent with the text of the CPRA, which clearly gives businesses a choice between posting links or responding to signals. The Agency suggests that the choice is instead between "frictionless" and "non-frictionless" responses to opt-out signals. However, the term "frictionless" does not appear in the CPRA. The CPRA does not contemplate two different kinds of responses to opt-out signals – it just describes two options for receiving such signals.

§ 7027(e). Requests to Limit Use and Disclosure of Sensitive Personal Information, requests to limit.

We ask that the Agency treat requests to limit use of sensitive personal information according to the same time periods as other consumer rights and provide clear guidelines for how businesses should collect additional information. Admittedly, the CPRA does not specifically require verification of the identity of a consumer who seeks to limit the use of their sensitive personal information. However, as the Agency acknowledges, it may be necessary for a company to ask for additional information in order to identify the right consumer. A limitation on the use of a consumer's sensitive personal information has the potential for negative consequences for the consumer (especially if misapplied), and businesses should be allowed time to make sure the right person is impacted and requested the limitation at issue.

Especially in the healthcare context, it may take courage for a consumer to share sensitive information about their racial identity, sexual orientation, and health condition. Mistakenly terminating the use of such information could leave a consumer upset. Companies should be provided with time and a process to make sure limitations are applied to the right person.

§ 7027(l)(7). Requests to Limit Use and Disclosure of Sensitive Personal Information, allowable uses and disclosures not requiring notice of a right to limit, quality and safety of services or devices.

We ask that the Agency adjust the references to "service or device" to "product, service, or device." We think the addition of the word "product" would help clarify that data may be used to ensure consumer safety and product quality across a variety of economic activities.

§ 7028(c). Requests to Opt-In After Opting-Out of the Sale or Sharing of Personal Information or Limiting the Use and Disclosure of Sensitive Personal Information, attempts to use a product or service after exercising the right to limit.

This paragraph is confusing. If a consumer requests a service that requires the use of sensitive personal information, the use of that personal information is already permitted by §7027(l)(1). So, there should not be a situation where a consumer requests a service that requires sensitive personal information for a purpose not covered by §7027(l). Uses of sensitive personal information required to provide a requested service are always permitted. This section should be revised to indicate the consent is required only if the business seeks to use sensitive personal information for a purpose that is not covered by §7027(l).

§ 7050(b)(2). Service Providers and Contractors. Exceptions to prohibition retaining, using, or disclosing personal information. Specific business purposes.

The use of the phrase "business purposes and services" expands the contracting requirements beyond what is found in the CPRA. The CPRA only mentions "business purposes" or "purposes" when describing how a contract should limit a service provider's use of data. To further require the specific services to be identified creates contractual complexity without an off-setting benefit to consumers.

For example, many companies enter into "master service agreements" that generally describe how the companies will relate to their service providers and create a framework for the purchase of a variety of services – some of which may be known at the time of contracting and others which may arise in the future. Often, the addition of new services is done via quasi-contractual documents like Statements of Work, Purchase Orders, or Change Orders. These documents may, in turn, refer out to product descriptions or specifications found elsewhere.

To require all of these service descriptions to be pulled into the master agreement and enshrined at each point in the process would be very burdensome. It would also require amending contracts signed using the "purpose"-based approach adopted in the existing regulations. Statements that data may not be used except in the context of the business relationship between the parties and for the purposes of providing purchased services to the business are more than adequate to put enforceable contractual limits on service provider conduct. Providing more detail does not benefit consumers (who likely will never encounter the full master services agreement).

§ 7051 (Generally). Contract Requirements for Service Providers and Contractors.

We encourage the Agency to adopt a transition period for the execution of new contracts. The Agency's should take note of the recent changes to the European Standard Contractual Clauses, where the European Commission acknowledged that the process of revising and updating contracts (even with very similar substantive provisions) is time-consuming and cannot be done overnight. The Agency should provide a similar transition period, where existing contracts executed in compliance with the current regulations remain valid until a certain point in time. New contracts could be expected to comply with Agency requirements a few months after they go into effect. We propose that businesses be given three months to come into compliance for new contracts, with existing contracts remaining valid for a year before changes are required.

§ 7051(e). Contract Requirements for Service Providers and Contractors. Contractual due diligence.

The Agency's statement that a business which "never enforces the terms of the contract nor exercises its rights to audit" a service provider may not claim it did not know and should not have known of a service provider's violation runs counter to the plain language of the CPRA. The CPRA clearly establishes a misconduct or gross negligence standard for a business's loss of liability protection. The Agency's proposed approach converts this standard to a mere "negligence" standard. This is not what the statute envisions. This statement should be removed.

Conclusion and contact information.

Thank you for considering our comments and recommendations. If you have any questions, you may contact Fielding Greaves at fgreaves@biocom.org or Reed Abrahamson at reed.abrahamson@faegredrinker.com.

Sincerely,

Fielding Greaves
Sr. Director, State Government Affairs
Biocom California

Reed Abrahamson
Secretariat
International Pharmaceutical & Medical Device Privacy Consortium (IPMPC)