
From: Leder, Leslie [REDACTED] on behalf of Daylami, Ronak
[REDACTED]
Sent: Thursday, November 3, 2022 1:24 PM
To: Urban, Jennifer [REDACTED]
Cc: Delatorre, Lydia [REDACTED]; Le, Vinhcent [REDACTED]; Mactaggart, Alastair [REDACTED];
[REDACTED]; Soltani, Ashkan [REDACTED];
[REDACTED]; Kurpiewski, Christian; [REDACTED]
Subject: Coalition Letter - Business Community Concerns re CPRA Regulatory Process
Attachments: 2022 CPPA Letter Nov. 3.pdf
Importance: High

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good afternoon,

Attached please find our coalition letter regarding business communities concerns about the CPRA regulatory process. If you have any questions, please reach out to me or Ashley Hoffman
[REDACTED].

Thank you,

Ronak Daylami
Policy Advocate



California Chamber of Commerce
1215 K Street, 14th Floor
Sacramento, CA 95814
T: [REDACTED]

Visit calchamber.com for the latest California business legislative news plus products and services to help you do business.

This email and any attachments may contain material that is confidential, privileged and for the sole use of the intended recipient. Any review, reliance or distribution by others or forwarding without express permission is strictly prohibited. If you are not the intended recipient or have reason to believe you are not the intended recipient, please reply to advise the sender of the error and delete the message, attachments and all copies.



Jennifer M. Urban
Chairperson, California Privacy Protection Agency Board
2101 Arena Boulevard
Sacramento, CA 95834

SUBJECT: BUSINESS COMMUNITY CONCERNS REGARDING CPRA REGULATORY PROCESS

We write to you on behalf of the California Chamber of Commerce (CalChamber) and the organizations listed below, which represent a significant portion of California's business community. Our members are deeply concerned about the CPRA taking effect on January 1, 2023, prior to the Agency finalizing the necessary and long overdue regulatory guidance.

We believe that it is imperative for the Agency to effectuate the voters' intent to provide for a six-month delay between the adoption of final regulations and the date that companies must begin compliance and a 12-month delay in the adoption of final regulations and enforcement of the CPRA. At the same time, we urge that it is critical to get this done right, rather than to get it done rushed.

We recognize the magnitude of the task that the CPRA charged this new California Privacy Protection Agency ("Agency") with upon its formation: to issue final regulations implementing the CPRA by July 2022, less than 16 months after the first Board members were appointed. The complications that come with building a brand new agency and the challenges of undertaking a formal regulatory process, let alone doing both of those tasks at the same time, are considerable. Nonetheless, that is the timeline approved by the voters and relied upon by our members, who simply want to know how to comply with the law. We ask that you, in turn, consider the significant burden placed on businesses, particularly if they must unwind all of their compliance work if their best and good faith interpretation of the statute does not ultimately align with the final regulations.

Our associations have consistently stood in favor of privacy laws and regulations that can be operationalized without unintended consequences and unnecessary exposure to litigation. To that end, the business community has worked to provide as much feedback as possible using the avenues made available to us since this Agency's inception. However, we have found some of those avenues lacking, particularly with respect to the lack of representation from members of the business community at the Agency's informational sessions. Along these same lines, we were also discouraged to find that the stakeholder sessions (which we participated in) did not receive the same level of Board member attendance and active participation as the informational sessions. While we have done our best to provide as much constructive feedback as possible to the draft regulations, our members' concerns about the overdue regulations are valid and should be given greater consideration as the Agency moves forward with the regulatory process.

To be clear, the fact that we do not have final regulations in time to effectively implement raises significant concerns both practically, and legally. When the voters approved Proposition 24, they approved a system that included a full year of ramp up time between the July 1, 2022 deadline for final regulations and the commencement of enforcement actions beginning July 1, 2023. At best, even if a portion of the mandated regulations were completed and submitted to the Secretary of State by November 30 (which we understand is unlikely), businesses would get half that amount of time. By that same token, businesses would have received six months between the regulations being finalized on July 1, 2022, and the law becoming effective on January 1, 2023 had the Agency adhered to the voter approved deadlines.

Instead, California businesses are being placed in the untenable position of being required to comply with and effectuate the CPRA starting January 1st, without having been provided all of the final regulations necessary to do so. This is hugely problematic, not only as an operational matter, but also as a legal one.

Recent Case Illustrates that Past-Due Regulations are Problematic and Warrant Remedies

The impacts of a failure to timely complete regulations is well-illustrated in a recent lawsuit involving similar circumstances. In 2022, the California Hispanic Chambers of Commerce, Kruse & Son Inc, California Grocers Association, California Restaurants Association, and the California Retailers Association ("Petitioners") successfully petitioned for a prohibitory writ of mandate against the California Department of Food and Agriculture (CDFA) and the Attorney General's Office ("Respondents"). This CDFA suit involved another voter approved law, the Prevention of Cruelty to Farm Animals Act enacted pursuant to Proposition 12 in 2018 regulating the raising and selling of meat products. Proposition 12 provided that CDFA and the California Department of Public Health "shall jointly promulgate rules and regulations for the implementation of this act by September 1, 2019" which was three months before the act's first requirements took effect. Notwithstanding that September 1, 2019, deadline, those departments did not release a Notice of Proposed Act (NOPA) pursuant to the Administrative Procedures Act (APA) until May 2021 and did not issue its revised proposed regulations until December 2021. At the time that the court granted a prohibitory writ of mandate (January 21, 2022), final regulations were not in effect, but the law was to go into effect on January 1, 2022.

In this CDFA lawsuit, the Petitioners sought a judicial declaration that the square-footage requirement affecting pork sales effective January 1, 2022, are unenforceable absent final implementing regulations and further sought to delay enforcement of that same requirement until after the regulations are promulgated, consistent with voter intent. The court ultimately agreed with the Petitioners and issued a declaration that the petitioning organizations and their members owners and operators “are not subject to enforcement of the prohibition on sales of whole pork meat ... [citations omitted] ... until 180 days after final regulations are enacted...” subject to potential adjustments once the final regulations were in effect.

In its decision, the court noted that the Act’s deadline on the promulgation of regulations is mandatory, not permissive, and infers a mandate for pre-enforcement regulations. Further supporting this was that the regulations that the voters intended are regulations “for the implementation of [that] act ...” In other words, Proposition 12 was not self-executing. Accordingly, the court rejected the Respondents’ argument that the Act is clear enough to enforce without additional guidance (as the act’s square footage requirements and many of the Act’s definitions are explicit).

The court also distinguished the CDFA case from two prior cases, *Alfaro v. Terhune* (2002) and *Fisher v. State Personnel Board* (2018). In the first case, the court said that the specification to regulate “as necessary” indicated a discretionary grant limiting regulatory authority, rather than commanding it – which is materially different from Proposition 12’s mandate. In the second case involving incompatible employment, the statutory provisions in question directed the Department of Human Resources to “adopt rules governing the application” of the bar on incompatible employment, but also provided that “existing procedures shall remain in full force and effect” until the department “adopts rules governing the application” of that section. In other words, the court in that case determined that the statute was binding even before CalHR’s implementation of rules governing the statute’s application. In the CDFA suit, Proposition 12 built upon a prior voter approved law, the Prevention of Farm Animal Cruelty Act (Proposition 2 from 2008) but contained no reference to preexisting or alternative rules of implementation; rather, the text described mandatory regulations in effect prior to square footage requirements governing sales.

This situation is nearly identical to that of the CDFA suit. Similar to Proposition 12, Proposition 24 mandates regulations effectuating the CPRA (Civ. Code Section 1798.185 specifically states “shall solicit broad public participation and adopt regulations to further the purposes of this title”). While Proposition 24 also authorizes additional regulations “as necessary” to further the purposes of the CPRA, there are a host of specified areas in which new regulations are explicitly required, such as with respect to the Act’s new audit requirements. While the regulations issued by the Attorney General under the CCPA remain in place absent changes by the Agency’s upcoming regulations, unlike the CalHR case which determined “existing procedures remain in full force and effect, Proposition 24 does not have existing procedures for mandated regulatory topics such as audits, automated decision-making technology-specific opt-out rights, and the like. Here, the Agency’s regulations were due by July 1, 2022, six months prior to Proposition 24’s effective date, whereas the Agency only commenced formal rulemaking on July 8th, when it issued its NOPA in accordance with the APA. Finally, like Proposition 12, the CPPA has not issued a NOPA for some of the categories required in Proposition 24.

Without intervention, Proposition 24 will go into effect without any completed regulations and with some required regulations not even begun.

In Absence of a Delay in the CPRA’s Effective Date, we Request that the Agency, at a Minimum, Delay the July 1, 2023, CPRA Enforcement Date

It is critical that the Agency’s failure to issue regulations be addressed out of fairness to those striving to comply with the CPRA and to mitigate the harm to covered businesses, employees, and consumers. The fairest solution would be to delay CPRA’s effective date until six months after final regulations are completed as originally intended in Proposition 24. However, understanding that the Agency may not possess the authority to do so, at the very least the Agency must delay the July 1, 2023, enforcement date.

CalChamber and others have consistently raised concerns about covered businesses having to comply with the law and potentially having to legally defend themselves for failing to meet the requirements of future regulations. At a legislative budget subcommittee hearing earlier this spring, Agency staff dismissed concerns that the regulations would not be timely adopted, stating that “the California DOJ also did not

meet their deadline but faced no issue, no legal implications, for missing that deadline necessarily". We respectfully disagree.

The consequences to businesses are very real and highly detrimental and should not be minimized. Consider, for example, the new audits that covered businesses will face under the CPRA. Covered businesses are subject to audits starting January 1. Even if an enforcement action cannot be commenced for violations until after July 1, 2023, we must still comply with those audit requirements on January 1, without any idea of how to do so, for lack of final regulations.

Further, the problem created by the past-due CPRA regulations is only exacerbated by the fact that the employee and business to business sunsets (Cal. Civ. Code Sec. 1798.145 (m) and (n)) are set to lapse on January 1, 2023, making the consumer law now applicable in employment contexts. In fact, **none of the regulations drafted thus far take employees or business-to-business transactions into account.** They relate to consumers, not employees or employment communications.

To say that this is overwhelming and highly problematic as a matter of operationalizing the voters' intent is a massive understatement. We fail to see how a law that cannot be implemented by its effective date, let alone implemented properly, protects consumers or takes into consideration impact on businesses. Stated plainly, the problem identified has nothing to do with the intentions and good faith efforts of businesses to comply; it has to do with the delayed regulations of this Agency. Yet, the ones who will feel the consequences of that failure are businesses, their employees and the consumers they serve.

We ask that you seriously consider whether this process serves Californians and their privacy rights, and the businesses struggling to understand what it is they must do to be compliant. As stated at the top of this letter, our organizations represent businesses big and small. We ask that you keep in mind that not all businesses have the resources to pay for compliance attorneys, let alone make operational changes only to find that they did it incorrectly because they did not have the required regulations to do so properly. Without timely regulations, we do not believe that this process has been and will be in furtherance of privacy. We must therefore ask for a six-month delay in implementation and/or 12-month delay of enforcement of the CPRA, after the final regulations are adopted.

Sincerely



Ronak Daylami
Policy Advocate
California Chamber of Commerce
on behalf of

Acclamation Insurance Management Services
Advanced Medical Technology Association
Aerospace and Defense Alliance of California
Alliance for Automotive Innovation
Allied Managed Care
American Association of Advertising Agencies
American Council of Life Insurers
American Property Casualty Insurance
Association
Association of California Life and Health
Insurance companies
Association of National Advertisers
Auto Care Association
Biocom California
Brea Chamber of Commerce
BSA The Software Alliance
Building Owners and Managers Association,
California

California Association of Collectors
California Association of Health Facilities
California Association of Winegrape Growers
California Attractions and Parks Association
California Bankers Association
California Beer and Beverage Distributors
California Business Properties Association
California Chamber of Commerce
California Credit Union League
California Farm Bureau
California Grocers Association
California Hospital Association
California Hotel & Lodging Association
California Land Title Association
California Manufacturers & Technology
Association
California New Car Dealers Association
California Restaurant Association

California Retailers Association
 California Self Storage Association
 California State Council of the Society for Human
 Resource Management (CalSHRM)
 California Travel Association
 California Water Association
 Carlsbad Chamber of Commerce
 CAWA, Representing the Automotive Parts
 Industry
 Chino Valley Chamber of Commerce
 Civil Justice Association of California
 Coalition of Small and Disabled Veteran
 Businesses
 Consumer Data Industry Association
 Costa Mesa Chamber of Commerce
 Escrow Institute of California
 Family Business Association of California
 Fidelity Investments
 Flasher Barricade Association
 Fresno Chamber of Commerce
 Greater Coachella Valley Chamber of Commerce
 Greater High Desert Chamber of Commerce
 Greater Riverside Chamber of Commerce
 Greater San Fernando Valley Chamber of
 Commerce
 Housing Contractors of California
 Insights Association

Laguna Niguel Chamber of Commerce
 Long Beach Area Chamber of Commerce
 Los Angeles Area Chamber of Commerce
 Murrieta/Wildomar Chamber of Commerce
 NAIOP, California
 National Association of Mutual Insurance
 Companies
 Palos Verdes Peninsula Chamber of Commerce
 Personal Insurance Federation of California
 Rancho Cordova Area Chamber of Commerce
 San Gabriel Valley Economic Partnership
 San Marcos Chamber of Commerce
 Santa Barbara South Coast Chamber of
 Commerce
 Santa Clarita Valley Chamber of Commerce
 Santa Maria Valley Chamber of Commerce
 SIIA
 Southwest California Legislative Council
 TechNet
 Torrance Area Chamber of Commerce
 Tri County Chamber Alliance
 United Parcel Service
 Valley Industry & Commerce Association
 West Ventura County Business Alliance
 Western Electrical Contractors Association
 Western Growers Association
 Wine Institute

cc: Board Member Lydia de la Torre, California Privacy Protection Agency
 Board Member Vinhcent Le, California Privacy Protection Agency
 Board Member Alastair MacTaggart, California Privacy Protection Agency
 Board Member Christopher Thompson, California Privacy Protection Agency
 Ashkan Soltani, Executive Director, California Privacy Protection Agency
 Christine Aurre, Office of the Governor
 Darci Sears, Office of Assembly Speaker Anthony Rendon
 Eric Dang, Office of the Senate President Pro Tempore Toni Atkins
 Landon Klein, Assembly Privacy & Consumer Protection Committee
 Christian Kurpiewski, Senate Judiciary Committee
 Anthony Lew, Office of the California Attorney General

RD:ldl

From: [REDACTED]
Sent: Friday, November 4, 2022 10:19 AM
To: Regulations
Subject: Important Comments Concerning The Consumer Privacy Rights Act

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

With regard to the 28 / 29th October Board Meeting and the subsequent Notice of Modification to Proposed Regulations Implementing New Consumer Privacy Law sent by email on 3rd November 2022 , we would like to provide the following comments that we consider are important factors that would both strengthen the Act and close potential loopholes in the text as currently written. They are as follows:

1. With regard to the consumer's opportunity to opt-out of the sale and sharing of personal information and do so conforming with the requirements set forth in section 7025 to have their data protected, the current text states that a Business must place this opt-out signal on the home page of their web site. However, it is largely the case that consumers enter a website at various different places or pages, not just the home page. In other words, the consumer would not see the opt-out signal as their point of entry to the site.

We suggest that the text is amended to have the opt-out signal present on all pages of a Business web site to ensure consumers have that right available to them irrespective of where they first engage with that site. Doing so would also ensure Businesses can't by-pass this important aspect of the regulations .

2. With regard to consumer data, the terms used throughout the text such as "Do not sell" and "Do not share" are clear and obvious in their meaning and regulatory intent. However, the term "Do not use" again seen throughout the text is **confusing and open to interpretation** as to exactly what this entails.

We suggest that "the term "Do not use" is defined clearly throughout the text as to its meaning and activities that are covered by it.

We hope and trust you will find these comments helpful and thank you in anticipation of your consideration.

Sincerely,

Pat Whelan



p: [REDACTED] | e: [REDACTED]
w: [REDACTED]

From: jmunoz [REDACTED]
Sent: Monday, November 7, 2022 9:12 AM
To: Regulations
Subject: CCPA Public Comment
Attachments: CCPA Comment.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: jmunoz [REDACTED]

Please see attached.

November 7, 2022

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

Thank you for the opportunity to comment on the Consumer Privacy Rights Act of 2020 (CPRA).

Privacy for consumers and individuals has evolved to become immensely complicated, and changes rapidly. I want to emphasize that the use of data brokers poses an ever-increasing threat to individual privacy.

As such, I want to point out a potential loophole in this legislation.

As I understand it, the opt-out procedures and sharing restrictions apply to businesses that collect information on California consumers. However, does any of it apply to companies that do not directly collect anything, but instead, utilize data brokers for decision-making?

For example, Quest Diagnostics, a large public company offering lab testing services uses data from Lexis Nexis in an attempt to validate email addresses and identity. This cumbersome process is a threat to privacy on multiple levels. Not the least of which is that a company is often denying access to its service based on information it never collected and cannot verify.

And for those who have opted out of data broker companies, but third-party companies such as Quest buy and use that data, the opt-out for the consumer has now become invalidated.

Lastly, I cannot emphasize the danger that the prevalence of data brokers poses to not only identity theft, but to legitimate security issues. Perhaps the most glaring example is that it has become ridiculously easy to buy data on an individual online, and most likely learn their cell phone number. Scammers and criminals then use that number in spoofing and SIM-swapping scams to bypass phone-based two-factor authentication (2FA), and gain control of bank accounts, credit card accounts, and other important accounts and assets of unsuspecting victims.

These scams are hard to investigate, easy to get away with, and while the loss to victims is often very high, and the criminal penalties for the scammers is very low.

Ask any knowledgeable law enforcement fraud investigator about the threat posed by the prevalence of data brokers, cell phones, and two-factor authentication. Most departments and agencies cannot adequately investigate these crimes because of the challenges and necessary resources needed to locate suspects.

In conclusion, I would like to emphasize that no company operating in California should be able to use any third-party data in any way without the consumer's express written consent in advance, and should adhere to all other provisions of this law.

Thank you.

From: Walsh, Kevin [REDACTED] <[REDACTED]>
Sent: Tuesday, November 15, 2022 1:24 PM
To: Regulations
Subject: CCPA Public Comment
Attachments: Spark CCPA November 11 2022 FINAL.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Please find attached The Spark Institute, Inc.'s comments.

Regards,

Kevin Walsh

Notice: This message is intended only for use by the person or entity to which it is addressed. Because it may contain confidential information intended solely for the addressee, you are notified that any disclosing, copying, downloading, distributing, or retaining of this message, and any attached files, is prohibited and may be a violation of state or federal law. If you received this message in error, please notify the sender by reply mail, and delete the message and all attached files.



November 11, 2022

The California Privacy Protection Agency
 Attn: Brian Soublet
 2101 Arena Blvd., Sacramento, CA 95834
 (279) 895-6083

Re: Comments in Response to November 3, 2022 Modifications of Text of Proposed Regulations

Dear Acting General Counsel Soublet:

The SPARK Institute, Inc. writes to encourage you to take into account the continued expectations of employees and retirees as it finalizes the regulations that were most recently proposed on November 3, 2022 (the “Proposed Regulations”). We applaud the CCPA’s goal of providing consumers with strong protections, while still leaving employers and their service providers in a position to help employees receive health care and meet their retirement and other savings goals.

It is important to recognize that while the California Privacy Rights Act of 2020 provided for the sunset of the employer exception and the business-to-business exception, it did not create a mandate that data shared by a non-business with a vendor for purposes of providing employment benefits must be covered by the CCPA.

While we are optimistic that the California legislature will make our position clearer through future amendments to the text of CCPA, we ask that you adopt our interpretation of the current text to avoid disrupting employee access to employment benefits.

The SPARK Institute represents the interests of a broad-based cross section of retirement plan service providers and investment managers, including banks, mutual fund companies, insurance companies, third party administrators, trade clearing firms, and benefits consultants. Collectively, our members serve over 100 million employer-sponsored plan participants. Our comments reflect our unique perspective and our goal of advancing critical issues that affect plan sponsors, participants, service providers, and investment providers.

COMMENTS FROM THE SPARK INSTITUTE

A vital mission of the SPARK Institute is the promotion of employer-sponsored retirement plans, which play a critical role in helping every hardworking American retire with financial security. We worked closely with the Attorney General on the CCPA

We ask specifically that Article 4, § 7050(g) be amended as follows:

“Whether an entity that provides services to a Nonbusiness must comply with a consumer’s CCPA request depends upon whether the entity is a “business,” as defined by Civil Code section 1798.140, subdivision (d) and the entity is using the personal information for any business purpose other than as necessary to provide Employment Benefits.”

This would clarify that when a non-business, such as a retirement plan, contracts with a business to provide Employment Benefits, the requirements of CCPA would not arise. Not only would our proposed change help mitigate some preemption concerns, but it would also make the regulations more consistent with CCPA’s stated mission of providing Californians with strong privacy rights while not interfering with their expectations to continue to enjoy the benefits to which they are accustomed.

Our proposed amendment is tailored to the existing definition of Employment Benefits found in Article 1, § 7001(j):

“‘Employment Benefits’ means retirement, health, and other benefit programs, services, or products to which consumers and their dependents or their beneficiaries receive access through the consumer’s employer.”

Retirement plans and health plans are often structured as stand-alone not-for-profit legal entities. This means that they generally, are not subject to CCPA. However, retirement plans and health plans are unable to operate absent reliance on service providers. Unless § 7050(g) is amended, the proposed language would appear to subject retirement and health plans to the full scope of CCPA as any time a plan contracts for the services it needs to deliver services – like retirement plan recordkeeping – the strictures of CCPA spring into being.

It is important that the regulatory framework surrounding employer-provided benefits not be disrupted. Absent changes, we are concerned not only for the reasons described above but also because benefits are already subject to federal regulation under laws like the Employee Retirement Income Security Act of 1974, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and the Health Information Technology for Economic and Clinical Health Act. Because the Proposed Regulations conflict with the structural frameworks provided by those federal laws, we are hopeful that our proposed amendments will be accepted to help avoid the need for courts to intervene to resolve how these laws and CCPA interact.

* * * * *

The SPARK Institute appreciates the opportunity to provide these comments to the California Privacy Protection Agency. If you have any questions or if you would like^{W106} more information regarding this letter, please contact me or the SPARK Institute's outside counsel, David Levine and Kevin Walsh with Groom Law Group, Chartered ([REDACTED]).

Sincerely,

[REDACTED]

Tim Rouse
Executive Director

From: Blake Edwards <[REDACTED]>
Sent: Wednesday, November 16, 2022 9:26 AM
To: Regulations
Cc: Howard Fienberg; Stuart Pardau
Subject: CPPA Public Comment from the Insights Association
Attachments: IA-CPPA-comments-on-CPRA-11-16-22.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Mr. Soublet

Please see the attached comments, filed on behalf of the Insights Association, regarding the latest CPRA regulations.

We appreciate the opportunity to comment.

--

Blake M. Edwards
Law Offices of Stuart L. Pardau & Associates
11620 Wilshire Blvd Suite #850
Los Angeles, CA 90025
p: [REDACTED]
e: [REDACTED]

This message is sent by a law firm and may contain information that is privileged or confidential. If you received this transmission in error, please notify the sender by reply e-mail and delete the message and any attachments.



California Privacy Protection Agency
 Attn: Brian Soublet
 2101 Arena Blvd.
 Sacramento, CA 95834
regulations@cppa.ca.gov

November 16, 2022

Re: CPPA Public Comment from the Insights Association

Mr. Soublet:

The Insights Association (“Insights”) submits the following comments regarding the proposed regulations relating to the California Privacy Rights Act of 2020 (“CPRA”).

For additional background on Insights and our membership, I refer you to the comments we previously submitted on August 11, 2022,¹ attached hereto as Attachment 1, and on November 8, 2021,² attached hereto as Attachment 2.

In addition to reiterating our previous comments, all of which we continue to feel should be addressed by the Agency, we would like to highlight again the issue of audience measurement, which we prioritized in our most recent comments (item #1 in Attachment 1).

To recap the issue, the current regulations prohibit service providers from combining personal information received from businesses with personal information received from the service provider’s own interactions with consumers unless it has a valid “business purpose” for combining the information. Because audience measurement is not included in the list of business purposes, this effectively amounts to a ban on critical audience measurement activities.

We do not believe the CPRA’s drafters intended to regulate these types of activities. To that point, draft federal legislation and extant state privacy statutes already make an accommodation for audience measurement.

Accordingly, we again strongly urge the Agency to follow the lead of federal and other state legislators and add audience measurement to the express list of business purposes.

¹ Available online at <https://www.insightsassociation.org/Portals/INSIGHTS/xBlog/uploads/2022/8/11/Insights-Association-comments-CPRA-8-11-22.pdf>

² Available online at <https://www.insightsassociation.org/Portals/INSIGHTS/xBlog/uploads/2022/11/16/Insights--CPRAComments11821.pdf>

We hope all of our comments have been useful to you and your team, and we are happy to entertain any questions or concerns you may have about the market research and data analytics industry.

In particular, we are eager to discuss the concept of audience measurement specifically if you believe that would be helpful.

Again, we appreciate the opportunity to comment.

Sincerely,

Howard Fienberg
Senior VP, Advocacy
Insights Association

Stuart Pardau
Counsel to Insights Association

Blake Edwards
Counsel to Insights Association

Attachment A

California Privacy Protection Agency
 Attn: Brian Soublet
 2101 Arena Blvd.
 Sacramento, CA 95834
regulations@coppa.ca.gov

August 11, 2022

Re: CPPA Public Comment of Insights Association

Mr. Soublet:

The Insights Association ("Insights") submits the following comments regarding the proposed regulations relating to the California Privacy Rights Act of 2020 ("CPRA").

Representing more than 750 individuals and companies in California and more than 6,000 across the United States, Insights is the leading nonprofit trade association for the market research¹ and data analytics industry. We are the world's leading producers of intelligence, analytics and insights defining the needs, attitudes and behaviors of consumers, organizations, employees, students and citizens. With that essential understanding, leaders can make intelligent decisions and deploy strategies and tactics to build trust, inspire innovation, realize the full potential of individuals and teams, and successfully create and promote products, services and ideas.

CPRA is going to have a profound impact on the business community, including the market research and data analytics industry. Small and medium-sized research firms in particular will face tremendous costs in updating and expanding on their already-extensive compliance efforts in connection with the California Consumer Privacy Act of 2018 ("CCPA"). Accordingly, and on behalf of our members, we commend your decision to seek input on the proposed regulations and are grateful for the opportunity to comment.

1. Bring CPRA in line with draft federal privacy legislation and other state laws by adding audience measurement to the list of "business purposes"

As you are aware, CPRA requires that contracts with service providers "prohibit[] the person from...[c]ombining the personal information that the service provider receives from, or on behalf of, the business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer," with the exception that the service provider "may combine personal information to perform any business purpose as defined in [the] regulations."

¹ Market research, as defined in model federal privacy legislation from Privacy for America, is "the collection, use, maintenance, or transfer of personal information as reasonably necessary to investigate the market for or marketing of products, services, or ideas, where the information is not: (i) integrated into any product or service; (ii) otherwise used to contact any particular individual or device; or (iii) used to advertise or market to any particular individual or device." See Part I, Section 1, R: <https://www.privacyforamerica.com/overview/principles-for-privacy-legislation-dec-2019/>

This restriction has implications for certain methodologies used in our industry which we believe the Agency may not have intended. Specifically, conducting audience measurement requires de-duplicating the relevant data, which in turn requires combining, at least temporarily, the relevant data from the client business with a research firm's own internal data. We believe such a combination, and audience measurement more generally, is not the type of activity the Agency intended to restrict. Accordingly, we request that audience measurement be added to the CPRA's list of "business purposes."

As you may be aware, this change by the Agency would bring CPRA in line with other privacy legislation. **Draft federal legislation and extant state privacy statutes already make an accommodation for audience measurement.** For example, the American Data Privacy and Protection Act exempts from the definition of targeted advertising "processing covered data solely for measuring or reporting advertising or content, performance, reach, or frequency, including independent measurement."² We urge the Agency to leverage the foregoing definition, which we believe most completely captures audience measurement activities. Extant state laws may also, of course, provide further guidance.³

Finally, if the Agency is amenable to the foregoing suggestion, we would also urge the Agency to clarify that such audience measurement activities do not constitute "cross-contextual advertising," to avoid any ambiguity in the regulations if audience measurement is designated as a business purpose.

2. Limit the opt-out preference signal requirement businesses that meet one of the first two prongs of the CPRA's "business" definition.

As the Agency is aware, there are three different ways for an organization to be defined as a "business" under the CPRA: (1) annual gross revenues in excess of \$25 million; (2) buying, selling, or sharing the personal information of at least 100,000 consumers or households; or (3) deriving 50 percent or more of its annual revenues from selling or sharing personal information.

Because the third prong is not tied in any way to business size or processing volume, it includes a substantial number of small and medium-sized firms in the market research and data analytics industry. Firms who are subject to CPRA solely on the basis of this third prong should be exempt from implementing a solution to respond to opt-out preference signals.

In order to respond to these signals, firms will likely have to hire outside expertise to implement a technological solution, an expense which will be potentially significant for smaller firms. That expense may, moreover, be recurring — i.e., firms will likely have to update or at least review the technology regularly as opt-out signals evolve. Because this method for submitting an opt-out request is in addition to already-existing methods for submitting opt-out requests, we believe limiting the preference signal

² See American Data Privacy and Protection Act (pp. 15-16):

<https://www.insightsassociation.org/Portals/INSIGHTS/xBlog/uploads/2022/8/5/AmendmentsAdoptedbyHouseEnergyANDCommerceCommitteeDuringJuly2022MarkuptoJuly182022AINSPDF.pdf>

³ See UTAH CONSUMER PRIVACY ACT (S.B. 227), available at <https://le.utah.gov/~2022/bills/static/SB0227.html> ("'Targeted advertising' does not include...processing personal data solely to measure or report advertising performance, reach, or frequency"); CONNECTICUT DATA PRIVACY ACT (S.B. 6), available at <https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF> ("'Targeted advertising' does not include...processing personal data solely to measure or report advertising frequency, performance or reach."); COLORADO PRIVACY ACT (SB21-190), available at https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf ("'TARGETED ADVERTISING'...DOES NOT INCLUDE...PROCESSING PERSONAL DATA SOLELY FOR MEASURING OR REPORTING ADVERTISING PERFORMANCE, REACH, OR FREQUENCY").

requirement as we propose would allow the Agency to balance the interests of small businesses without hampering the opt-out right of California consumers.

Alternatively, the Agency could limit the preference signal requirements based on smaller limits than those in the CPRA's "business" definition (e.g., firms that do \$15 million in revenue or deal with at least 50,000 records), to protect the smallest businesses from overly onerous regulatory requirements.

Conclusion

We hope the above comments will be useful to you and your team, and we are happy to entertain any questions or concerns you may have about the market research and data analytics industry.

And we are eager to discuss the concept of audience measurement, specifically, if you believe that would be helpful.

Again, we appreciate the opportunity to comment.

Sincerely,

Howard Fienberg
Senior VP, Advocacy
Insights Association

Stuart Pardau
Counsel to Insights Association

Blake Edwards
Counsel to Insights Association

PROTECT • CONNECT • INFORM • PROMOTE
Insights Association | 1629 K Street NW, Suite 300 Washington, DC 20006 | Phone: 202-800-2545 | www.insightsassociation.org

Attachment 2

1



California Privacy Protection Agency
 Attn: Debra Castanon
 915 Capitol Mall, Suite 350A
 Sacramento, CA 95814
regulations@coppa.ca.gov

November 8, 2021

Re: Comments of the Insights Association on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Proceeding No. 01-21)

Ms. Castanon:

The Insights Association ("Insights") submits the following comments regarding future regulations relating to the California Privacy Rights Act of 2020 ("CPRA").

Representing more than 750 individuals and companies in California and more than 6,000 across the United States, Insights is the leading nonprofit trade association for the market research¹ and data analytics industry. We are the world's leading producers of intelligence, analytics and insights defining the needs, attitudes and behaviors of consumers, organizations, employees, students and citizens. With that essential understanding, leaders can make intelligent decisions and deploy strategies and tactics to build trust, inspire innovation, realize the full potential of individuals and teams, and successfully create and promote products, services and ideas.

The CPRA is going to have a profound impact on the business community, including the market research and data analytics industry. Small and medium-sized research firms in particular will face tremendous costs in updating and expanding on their already-extensive compliance efforts in connection with the California Consumer Privacy Act of 2018 ("CCPA"). Accordingly, and on behalf of our members, we commend your decision to seek input on future regulations and are grateful for the opportunity to comment.

1. Limit processing which presents a "significant risk" to consumers' privacy or security to highly sensitive personal information, such as financial account information

The CPRA directs the Agency to issue regulations "requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy" to perform annual cybersecurity audits and submit regular risk assessments to the Agency. The Agency has specifically requested feedback on this provision.

¹ Market research, as defined in model federal privacy legislation from Privacy for America, is "the collection, use, maintenance, or transfer of personal information as reasonably necessary to investigate the market for or marketing of products, services, or ideas, where the information is not: (i) integrated into any product or service; (ii) otherwise used to contact any particular individual or device; or (iii) used to advertise or market to any particular individual or device." See Part I, Section 1, R: <https://www.privacyforamerica.com/overview/principles-for-privacy-legislation-dec-2019/>

P R O T E C T ◆ C O N N E C T ◆ I N F O R M ◆ P R O M O T E

Insights Association | 1629 K Street NW, Suite 300 Washington, DC 20006 | Phone: 202-800-2545 | www.insightsassociation.org

We respectfully request that processing which presents a “significant risk” be limited to processing of highly sensitive personal information, such as financial account or payment card information, social security numbers, or other personal information which, if breached, could result in immediate financial harm to consumers.

2. Limit processing which presents a “significant risk” to processing which occurs on a regular basis or a minimum number of times per year

In addition to limiting “significant risk” scenarios as described above, the Agency could also clarify that such processing must occur on a regular basis, or at least with some minimal frequency, to trigger the auditing and risk assessment requirements. It does not meaningfully further the spirit of the CPRA, and imposes particularly unnecessary burdens on small businesses, to require an audit and security assessment solely on the basis of one, two, or a handful of isolated instances of processing deemed to present a “significant risk” in a given year.

3. Limit processing which presents a “significant risk” to processing of at least 100,000 records

Alternatively, we suggest the Agency could incorporate some numerical trigger into what constitutes “significant risk” processing. For example, this number could track the figure in the CPRA’s “business” definition of 100,000 records, or the Agency could select some lower number. In any case, the underlying statutory language of the CPRA counsels in favor of some such numerical limit. The statute contemplates “significant risk to consumers’ privacy or security,” language which connotes larger concerns of aggregate risk, not every isolated presentation of risk to any individual consumer or small group of consumers.

4. Limit the audit and risk assessment requirement to businesses who meet one of the first two prongs of the CPRA’s “business” definition

As the Agency is aware, there are three different ways for an organization to be defined as a “business” under the CPRA: (1) annual gross revenues in excess of \$25 million; (2) buying, selling, or sharing the personal information of at least 100,000 consumers or households; or (3) deriving 50 percent or more of its annual revenues from selling or sharing personal information.

Because the third prong is not tied in any way to business size or processing volume, it includes a substantial number of small and medium-sized firms in the market research and data analytics industry. Firms who are subject to CPRA solely on the basis of this third prong should be exempt from any annual audit and risk assessment requirements. These audits and risk assessments will be time consuming and expensive, and could in fact cripple small businesses who are just trying to do legitimate marketing research and data analytics work which benefits larger businesses, nonprofit and educational organizations, government entities, and individual consumers.

Alternatively, the Agency could limit the audit and assessment requirements based on smaller limits than those in the CPRA’s “business” definition (e.g., firms that do \$15 million in revenue or deal with at least 50,000 records), to protect the smallest businesses from overly onerous regulatory requirements.

5. Clarify that use in research results and reports of “sensitive personal information” is a “reasonably expected” use of information provided in connection with corresponding surveys and research studies

Under the CPRA, consumers have the right to request that a business “limit its use of the consumer’s sensitive personal information to that use which is necessary to perform the services or provide the goods

P R O T E C T  C O N N E C T  I N F O R M  P R O M O T E

Insights Association | 1629 K Street NW, Suite 300 Washington, DC 20006 | Phone: 202-800-2545 | www.insightsassociation.org

reasonably expected by an average consumer who requests such goods or services.” The Agency has specifically requested comment on “what use or disclosure of a consumer’s sensitive personal information by businesses should be permissible notwithstanding the consumer’s direction to limit the use or disclosure of the consumer’s sensitive personal information.”

Insights is concerned that if research subjects who have provided sensitive personal information in connection with a survey or study (for example, in connection with a poll about an important political issue) submit such a request, this may compromise research results and leave market research firms in a legally unclear relationship with the research subject. Accordingly, the regulations should stipulate that use of sensitive personal information in research results, and the continued use of those results to draw insights about consumers, is a “reasonably expected” use of sensitive personal information which was freely provided in connection with a survey or research study.

6. Define “disproportionate effort” as those efforts which “do not, in the reasonable discretion of the business, meaningfully add to the consumer’s understanding of the business’s historical practices”

The CPRA preserves a consumer’s right to “know” what personal information is being collected and what personal information is sold or shared and to whom. Previously, under CCPA, these rights were limited to a 12-month “look-back” period. Under the CPRA, if a consumer requests to know how information has been collected, sold, or shared, no matter how far back that request might reach, the only limitation on the request is whether it would be “impossible, or involve a disproportionate effort” on the part of the business.

The Agency has specifically requested input on what standard should govern a business’s determination that providing information beyond the 12-month window is “impossible” or “would involve a disproportionate effort.” In the market research and data analytics industry, information relating to a particular research subject (especially if that research subject participates in a research panel, for example) may appear in multiple studies across a long period of time. A research firm could spend theoretically limitless time and resources to reconstruct all the times a research subject was involved in a study, what information that study collected, and with whom the results were shared. Reconstructing every such instance would not meaningfully advance the consumer’s rights under CPRA, and it is not clear how much of this “reconstruction” would constitute “disproportionate effort.”

Accordingly, the Agency should clarify that “disproportionate efforts” beyond the 12-month window are “those additional efforts which require time and expense on the part of the business, but do not, in the reasonable discretion of the business, meaningfully add to the consumer’s understanding of the business’s historical practices.” In the above-referenced panel participant scenario, for example, rather than reconstructing the facts around every past study, the business would only be required to make the requested disclosures beyond the 12-month window as necessary to ensure the research subject has a complete (if not completely granular) view of how the research subject’s information is being processed.

7. Exempt market research from notices of financial incentives

For our members’ research to be effective, they must ensure robust participation. This is frequently done through offering financial incentives. For example, a doctor may be offered an honorarium to answer a survey about various pharmaceuticals, or an individual may be offered a gift card to participate in a half-day focus group about the latest television shows.

Our industry has worked hard to comply with the financial incentive notice requirement under CCPA, but the notice of financial incentives requirements were not written with market research in mind; they inhibit research in an unintended way. Accordingly, we resubmit our request, made previously in connection

P R O T E C T  C O N N E C T  I N F O R M  P R O M O T E

Insights Association | 1629 K Street NW, Suite 300 Washington, DC 20006 | Phone: 202-800-2545 | www.insightsassociation.org

with the CCPA regulations, that market research incentives and similar rewards to research subjects be exempt from notices of financial incentives requirements under the CPRA. Most significant of all, appropriate notices of financial incentives are already provided in every legitimate market research execution. Adding parallel and/or potentially conflicting requirements will only confuse the issue for Insights members, their clients and the public at-large that participates in this research.

8. Limit the “authorized agent” concept to minors, and elderly or incapacitated individuals

Under the CPRA, a consumer may designate an authorized agent to submit opt-out requests, and requests to know and delete. There is currently no limitation on this procedure. Anyone can submit a request through an authorized agent. Increasingly, our members are receiving requests from purported authorized agents and are caught between, on one hand, wanting to honor legitimate requests and, on the other, the pervasive concern that the authorized agent mechanism invites fraud. Of course, our members take steps to verify such requests, as required by law, but those verification efforts are sometimes difficult to complete without requesting additional information, and tend to frustrate agents and/or consumers as much as they frustrate the business.

The registered agent option is unnecessary in the vast majority of cases, increases paperwork associated with the verification process, and opens the door for fraudulent requests designed to harm consumers. Except in cases where the consumer is a minor, or someone who genuinely needs an authorized agent to submit a request (such as an elderly or incapacitated individual), the purpose of the law is better served by requiring requests to be submitted by consumers themselves.

We hope the above comments will be useful to you and your team, and we are happy to entertain any questions or concerns you may have about the market research and data analytics industry.

Sincerely,

Howard Fienberg
Senior VP, Advocacy
Insights Association

Stuart Pardau
Counsel to Insights Association

Blake Edwards
Counsel to Insights Association

P R O T E C T ◆ C O N N E C T ◆ I N F O R M ◆ P R O M O T E

Insights Association | 1629 K Street NW, Suite 300 Washington, DC 20006 | Phone: 202-800-2545 | www.insightsassociation.org

From: Lisa Quaranta [REDACTED]
Sent: Wednesday, November 16, 2022 2:37 PM
To: Regulations
Subject: CPPA Public Comment - California Credit Union League Comment Letter re Modified Proposed Regulations
Attachments: CNCUL Ltr RE Public Comment on CPPA-Mod Prop Regs - SIGNED 111522.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello:

Attached please find the California Credit Union League's comment letter re: CPPA Public Comment – Modified Proposed Regulations to Implement Changes to the California Consumer Privacy Act of 2018 (CCPA), as Amended by the Consumer Privacy Rights Act of 2020 (CPRA).

We appreciate the opportunity to comment on this matter and for considering our views.

Thank you,

Lisa Quaranta

Vice President, Regulatory Advocacy & Compliance
California & Nevada Credit Union Leagues
D: [REDACTED] | www.ccul.org



We Are Committed To Helping Credit Unions Change People's Lives

The information contained in this email message and any attachments to this message are intended only for the person or entity to which it is addressed, and may be proprietary, confidential, and/or privileged. If you are not the intended recipient, please: (1) notify the sender immediately by replying to this message; (2) do not use, disseminate, distribute, or reproduce any part of the message or any attachment; and (3) destroy all copies of this message and attachments. Please let us know if you have any questions.



November 15, 2022

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Boulevard
Sacramento, CA 95834
Via Email: (regulations@coppa.ca.gov)

Re: **CCPA Public Comment**
Modified Proposed Regulations to Implement Changes to the California Consumer Privacy Act of 2018 (CCPA), as Amended by the Consumer Privacy Rights Act of 2020 (CPRA)

Dear Mr. Soublet:

I am writing on behalf of the California Credit Union League (League), one of the largest state trade associations for credit unions in the United States, representing the interests of approximately 230 California credit unions and their more than 11.6 million members.

On July 8, 2022, the California Privacy Protection Agency (CPPA) began its formal rulemaking activities in connection with the administration and enforcement of the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA) (collectively, CCPA/CPRA) (Original Proposed Regulations). On November 3, 2022, the CPPA proposed further amendments to the Original Proposed regulations based on initial comments received (Modified Proposed Regulations).

The League has previously provided comments regarding the CCPA/CPRA and respectfully offers the following comments and feedback on the Modified Proposed Regulations for your further consideration.

➤ **Investigations and Enforcements**

The Modified Proposed Regulations add the following provision (b) to Section 7301:

“[A]s part of the Agency’s decision to pursue investigations of possible or alleged violations of the CCPA, the Agency may consider all facts it determines to be relevant, including the amount of time between the effective date of the statutory or regulatory requirement(s) and the possible or alleged violation(s) of those requirements, and good faith efforts to comply with those requirements.”

CCPA Public Comment on Modified Proposed Regulations to Implement Changes to the California Consumer Privacy Act of 2018 (CCPA), as Amended by the Consumer Privacy Rights Act of 2020 (CPRA)

November 15, 2022 – Page 2

The above Modified Proposed Regulation language states that the CPPA may take the delay in promulgating regulations and good faith efforts to comply into consideration instead of that it shall take them into consideration.

Given that covered businesses are likely to have six or seven less months to prepare for the July 1, 2023, enforcement start date than initially intended, the League is concerned that the Modified Proposed language is too permissive, leaving businesses at risk of possible enforcement actions despite their best efforts to comply. We believe that the considerations identified in §7301(b) are reasonable and fair and should always be taken into consideration.

➤ **Burden of Potential Agency Audits to Highly Regulated Businesses**

Calif. Civil Code §1798.199.65 gives the CPPA the authority to audit businesses' compliance with the law. The proposed regulations (§7304) would allow the CPPA to perform audits in three situations: (1) to investigate possible violations of the CCPA/CPRA; (2) if the subject's collections or processing activities present significant risk to consumer privacy or security; or (3) if the subject has a history of noncompliance with the CCPA/CPRA or any other privacy protection laws. Moreover, these audits ~~maybe~~ announced or unannounced, and a business's failure to cooperate with an audit could lead to enforcement action against that business.

The League previously provided comments on August 22, 2022, in response to the Original Proposed Rules wherein the League expressed concerns regarding the proposed Section 7304, which concerns persist.

As indicated in our prior comment letter, pending further clarification regarding the definition of a "business" as discussed in below, credit unions may be subject to the CCPA/CPRA and therefore to audits performed by the CPPA. Moreover, the CPPA's enforcement authority could extend to both state and federally chartered credit unions.

As financial institutions, credit unions are already among one of the most highly regulated industries. California's state-chartered credit unions are licensed and regulated by the California Department of Financial Protection and Innovation (DFPI), and the National Credit Union Administration (NCUA) regulates federal credit unions as well as federally insured state credit unions. Additionally, credit unions are subject to federal Consumer Financial Protection Bureau (CFPB) oversight, among other agencies. Credit unions currently undergo robust examinations by their regulatory agencies, which includes their compliance with applicable state and federal privacy and data security laws and regulations. We strongly reiterate our position that potential audits conducted by CPPA would be not only duplicative of existing examination requirements, but unjustifiably intrusive, burdensome, and overreaching for credit unions. The burden of these additional audits on smaller financial institutions could be especially significant in terms of disruption to staffing and operations. Therefore, we believe that a clear exemption is warranted and appropriate.

CCPA Public Comment on Modified Proposed Regulations to Implement Changes to the California Consumer Privacy Act of 2018 (CCPA), as Amended by the Consumer Privacy Rights Act of 2020 (CPRA)

November 15, 2022 – Page 3

However, if the CPPA is unwilling to provide such an exemption for credit unions, then it must provide guidance as to how credit unions can comply without unnecessarily burdening the credit union industry. At a minimum, coordination with state and federal primary regulators would be warranted.

➤ **Enforcement Date**

The CCPA/CPRA provides that the CPPA can bring enforcement action six months after publication of the final regulations or July 1, 2023, whichever is sooner. That means the CPPA could literally adopt final regulations on June 30, 2023 and enforce the law and the regulations the next day, on July 1, 2023.

While we understand that this is not the most likely scenario, it is still a serious concern. Despite the language of §7301(b) of the Modified Proposed Regulations regarding possible enforcement considerations, covered businesses should have adequate time to understand the requirements of the statute and the final regulations, and sufficient time to design and implement comprehensive compliance solutions before being subjected to enforcement actions, or the threat of enforcement actions. This is particularly true in light of the fact that the temporary exemptions extended to employee and certain business-to-business (B2B) data under Cal. Civil Code §1798.145 (m) and (n) sunsets as of January 1, 2023. The Modified Proposed Regulations remain silent on these specific compliance challenges that covered businesses are currently facing.

Due to the complexities of the CCPA/CPRA, the fact that the Modified Proposed Regulations are missing key guidance on all topics for which regulations are still necessary pursuant to §1798.185 of the CCPA/CPRA, as well as sunseting of the exemption for employee and B2B transactions, we urge the CPPA to delay enforcement until no less than six months after publication of final regulations. It is essential for effective compliance that the Agency take the time needed to ensure that any regulatory language adopted is comprehensive and complete, and based upon underlying CCPA/CPRA statutes that are fixed and not in a state of impending amendments.

➤ **GLBA and CFIPA Exemptions**

The CPRA revised the CCPA’s financial information exception to apply to “personal information collected, processed, sold, or disclosed **subject** to the federal Gramm-Leach-Bliley Act . . . , or the California Financial Information Privacy Act...” (emphasis and revision added).

Regardless of this change, there is still significant confusion regarding the exemption for personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (GLBA) or the California Financial Information Privacy Act (CFIPA). We are disappointed that neither the Original Proposed Regulations nor the Modified Proposed Regulations clarify this exemption.

CCPA Public Comment on Modified Proposed Regulations to Implement Changes to the California Consumer Privacy Act of 2018 (CCPA), as Amended by the Consumer Privacy Rights Act of 2020 (CPRA)

November 15, 2022 – Page 4

The confusion arises because the CCPA/CPRA uses terms that are inconsistent with the GLBA and CFIPA.

- The GLBA and CFIPA both use the terms “nonpublic personal information” and define that term to mean “personally identifiable financial information.”
- The CCPA/CPRA uses the term “personal information,” which is defined in Calif. Civil Code §1798.140(o) and is much broader than the GLBA/CFIPA’s definition of “nonpublic personal information.”
- In addition, the GLBA pertains to “personally identifiable financial information” collected in the course of a transaction or providing a financial product or service, etc. The CCPA/CPRA pertains to personal information collected in basically any manner, including when there is no transaction.

Because of the inconsistent terminology, the exemption provided in Calif. Civil Code §1798.145(e) is vague and unclear and can be interpreted several ways. It is essential that the CCPA provide clarification in the regulations.

Moreover, for financial institutions that are only subject to the CCPA/CPRA notice requirements to the extent not covered by an exemption, guidance with regard to the appropriate response to a consumer’s verifiable request that recognizes this exemption would be especially useful, given that consumers are unlikely to be familiar with the nature of the exemption or the extent to which it applies.

➤ **Model Notices Needed**

The CCPA and its regulations created several notice requirements for businesses, including:

- Notice at or Before Collection,
- Right to Opt-Out,
- Notice of Financial Incentives, and
- Updated Privacy Notices.

Further, the regulations require specific responses to certain verifiable consumer requests, for which model forms for both the request and the response would be beneficial:

- Verifiable Consumer Request to Know,
- Response to Verifiable Consumer Request to Know,

CCPA Public Comment on Modified Proposed Regulations to Implement Changes to the California Consumer Privacy Act of 2018 (CCPA), as Amended by the Consumer Privacy Rights Act of 2020 (CPRA)

November 15, 2022 – Page 5

- Verifiable Consumer Request to Delete,
- Response to Verifiable Consumer Request to Delete,
- Verifiable Consumer Request to Limit the Use of Sensitive Personal Information, and
- Response to Verifiable Consumer Request to Limit the Use of Sensitive Personal Information.

As noted above, the CPRA added the new Right to Request Correction of Inaccurate Personal Information, which would require a specific response to another form of verifiable consumer request. Useful Model forms would include:

- Verifiable Consumer Request to Correct Inaccurate Personal Information, and
- Response to Verifiable Consumer Request to Correct Inaccurate Personal Information.

Additionally, businesses must provide notice of the following consumer requests to third party service providers and contractors:

- Notice to Third Party Service Provider/Contractor that Consumer Contests the Accuracy of Certain Personal Information,
- Notice to Third Party Service Provider/Contractor of Consumer Opt-Out Request,
- Notice to Third Party Service Provider/Contractor of Consumer Deletion Request, and
- Notice to Third Party Service Provider/Contractor of Consumer Request to Limit the Use of Sensitive Personal Information.

For all these required notices and responses, the regulations require the notices be easy to read and understandable by the average consumer and provide some standards to achieve that. This direction is subjective and does not contemplate a method or metric to assess the readability.

Since all covered businesses need to provide the required notices and responses, uniform model notices would help to ensure a consumer's understanding of the information being provided, simplify the requirements for businesses, and create an objective standard of review to determine whether a business' notices comply with the required standards.

We are disappointed that neither the Original Proposed Regulations nor the Modified Proposed Regulations included model notices. The League strongly recommends that the CCPA create

CCPA Public Comment on Modified Proposed Regulations to Implement Changes to the California Consumer Privacy Act of 2018 (CCPA), as Amended by the Consumer Privacy Rights Act of 2020 (CPRA)

November 15, 2022 – Page 6

proposed model notices for public comment and then include a safe harbor in the final regulations for the use of notices substantially similar to the model notices.

The provision of model notices by the CCPA will also help to alleviate some of the initial compliance burden associated with meeting the fast-approaching Effective Date and Enforcement Date.

➤ **Other Considerations**

A. The Credit Union Difference

The League supports the spirit of the law; however, it is important that the CCPA understand the credit union difference. Credit unions, while highly regulated financial institutions, are first and foremost member-owned, democratically governed, not-for-profit financial cooperatives whose purpose is to promote thrift and improve access to credit for their member-owners, particularly those of modest means. As not-for-profit entities, credit union earnings are passed on to their member-owners in the forms of reduced fees, higher savings rates, and lower loan rates. Credit unions exist for the financial benefit of their member-owners, but they are ultimately driven by the philosophy of people-helping-people.

The credit union structure is vastly different than for-profit entities. “Owners” are not proprietors or shareholders in a business whose only goal is that the business maximize individual shareholder profits. Instead, credit union shareholders are members of a not-for-profit cooperative with a volunteer board of directors democratically elected by and from among its members. Each member has one vote, regardless of the number of shares (amount of funds) held in the credit union. Consumer personal information collected by credit unions is the personal information of its member-owner consumers in order to provide them with the products and services they desire.

Credit unions are the original consumer financial protection advocates. In addition, as highly regulated insured depository institutions, credit unions already comply with a plethora of data privacy and security requirements, including GLBA, CFIPA, and NCUA’s data security regulations.

B. Definition of a Business

We continue to call on the CCPA to clarify the definition of a business. The Modified Proposed Regulations do not define or further clarify the CCPA/CPRA definition of a business. We strongly recommend the final regulations clarify both the threshold criteria and the phrase “doing business in California.”

CCPA Public Comment on Modified Proposed Regulations to Implement Changes to the California Consumer Privacy Act of 2018 (CCPA), as Amended by the Consumer Privacy Rights Act of 2020 (CPRA)

November 15, 2022 – Page 7

- Thresholds

The CPRA changed the scope of covered businesses. Part of the definition of a business is that it satisfies one or more of the following thresholds:

(A) As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars (\$25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys or sells, or shares the personal information of 100,000 or more consumers or households.

(C) Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.

The application of threshold (B) to the personal information of 100,000 or more “consumers or households” is confusing. A consumer, as defined in the CCPA/CPRA is a natural person California resident. Is the rest of the threshold then related to households of natural person California residents? Additionally, further clarification is needed to determine the method for counting the number of consumers or households toward the 100,000 threshold. For example, if one household has five individual residents/consumers, would they be counted as one (household), five (consumers) or six (five consumers plus one household) toward the 100,000 threshold? For smaller credit unions, these distinctions are essential to the determination of whether they are subject to the requirements of the CCPA/CPRA.

- Doing Business in California

Another part of the definition of a business is that the entity “does business in the State of California.” There is no clear definition under the CCPA/CPRA or the regulations of what it means to “do business” in the State of California. Clarification is needed.

For credit unions based outside of California, members may live in or relocate to California while maintaining a relationship with their out of state credit union through ATMs or a shared branching network. (A shared branching network allows a member of one credit union to walk into the local branch of another credit union of which they are not a member and perform a range of transactions.)

At what point does the non-California credit union become subject to the CCPA/CPRA despite the lack of a physical presence? “Doing business” in a state should mean something more than isolated or incidental transactions. There should be a clearly defined standard that contemplates intentional repeated and successive transactions that clearly indicates a pattern or practice of choosing to do business with California consumers, and not one-time or occasional transactions.

CCPA Public Comment on Modified Proposed Regulations to Implement Changes to the California Consumer Privacy Act of 2018 (CCPA), as Amended by the Consumer Privacy Rights Act of 2020 (CPRA)

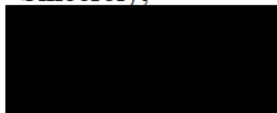
November 15, 2022 – Page 8

Final Comments

Ultimately, the League supports the spirit of the law and the need to protect the personal information of its members, but we continue to have significant concerns with the practicality and implementation of the Modified Proposed Regulations.

We thank you for the opportunity to comment. We trust you will carefully consider our views and recommendations. If you have any questions regarding our comments, please contact me.

Sincerely,



Diana R. Dykstra
President/CEO
California Credit Union League

From: Dave Kasten <[REDACTED]>
Sent: Thursday, November 17, 2022 7:59 AM
To: Regulations
Subject: CPPA Public Comment
Attachments: Block Party CPPA Comment Letter.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good morning,
Attached please find the public comments of Block Party Studio Company.

If you have any questions, please do not hesitate to reach out to me at [REDACTED].

Sincerely,
David Kasten
Chief of Staff
Block Party Studio Company



November 18, 2022

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

RE: CCPA Public Comment

Dear California Privacy Protection Agency Board Members,

We appreciate the opportunity to provide comments in response to the California Consumer Privacy Act Regulations modifications.

I am founder and CEO of Block Party, a company that builds online safety and anti-harassment products to give users more control of their online experience (currently on Twitter). Because the intent of the proposed regulations is to return control to consumers over their data, we have identified further opportunities that will allow consumers greater access to and control of their social media data with respect to the algorithms that currently dictate their online experience without the consumer's input or knowledge.

We believe that there are ambiguities in the proposed regulations that, if clarified, will further the purposes of the CCPA. Further, these ambiguities suggest other areas, not addressed in the proposed regulations, that remain necessary to address. We understand that the current notice for public comment is focused on minor modifications to the proposed text, but we seek to recognize these additional points for consideration for future rulemaking to further protect consumers and their rights to data.

1. 7001(i) "Disproportionate Effort". We recognize the important role that the concept of "disproportionate effort" has for businesses to weigh the cost to providers with the risks to consumers. However, we wish to suggest that the definition, as currently drafted, creates a false dichotomy. The balancing proposed in the current definition places all effort on the side of the provider, while assuming that consumers can't provide resources on behalf of data requests.

However, with the support of third-party advocates and tools, consumers may have the ability, for example, to process data that is not in a readily accessible format.

This is not merely an academic distinction. It would arguably be a “disproportionate effort” under the proposed rules for providers to allow consumers to modify the algorithms that are collecting and using their data or to perform tasks within a platform that relies upon their data, because these tasks would require significant time and resources to address the valid concerns of an individual user. However, allowing access to an API for tools developed by a third party would allow all users the rights to this level of control and protection, such as enabling millions of users to use tools to selectively mute or block users who engage in harassment, spam, or other unwanted behavior, without creating significant additional effort by the platform.

Proposed Change: We recommend the following change to the final line of the definition: “A business, service provider, contractor, or third party that has failed to put in place adequate processes and procedures to receive and process comply with ~~consumer~~ requests of consumers or their agents in accordance with the CCPA and these regulations cannot claim that responding to a consumer’s request by a consumer or their agent requires disproportionate effort.”

2. 7001 (ff) “Right to Know.” Under the “right to know” component of the regulations, the consumer has a right to request that a business disclose personal information that it has collected, sold or shared about the consumer. We believe that these categories are important, but insufficient. Under Civil Code section 1798.110(a)(3), CCPA grants to consumers the right to know the business purposes for which consumer data is being collected. This right includes allowing consumers to understand the manner in which a business uses algorithms to serve a consumer based on data collected from the consumer.

We recommend adding to the definition of “right to know” the rights already provided in section (a)(3) about the business purposes for which consumer data is used by the business, to wit what algorithms are being used and how they are being used with users’ personal information. Users should have the right to know how their data is being used by social media platforms and have the right to that information. This access will enable consumers (and their authorized agents) to understand what personal information is used by algorithms and how those algorithms are using their personal information. Users cannot make meaningful choices about how to use privacy and anti-harassment features on a social media platform without this information; even if they could, it often is difficult or slow to use those features manually. It’s crucial to open up access to third-party developers so that consumers can take back control of their information, instead of relying on the social media platform to have sole control over their data or how it is manipulated or displayed.

Proposed Change: “Right to know” means the consumer’s right to request that a business disclose personal information that it has collected (including the purposes and use for collection), sold, or shared about the consumer as set forth in Civil Code sections 1798.110 and 1798.115.

3. § 7002. Restrictions on the Collection and Use of Personal Information. Section 7002 states that, “the purposes for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer whose personal information is collected or processed.” However, this provision leaves ambiguous whether the reasonable expectations of the consumer relate only to the transfer or sale of collected or processed data to third parties or the collection, processing, and use of consumer data by the business for its own purposes in ways that may be hidden from the consumer/user of the business.

The definition of consumers’ reasonable expectations should include their reasonable expectations around a business’s own use of collected data, and consumers should have the opportunity to become aware of the algorithms that businesses apply to their personal information and have the ability to access their personal data via open APIs. We recommend that future rulemaking should specifically address the issue of consumer’s reasonable expectations to be able to understand the use of algorithms powered by their own personal information. To facilitate this rulemaking, we recommend a further change to the proposed rules as described below.

Proposed Change: Amend Section 7002 to address the issue of business use of collected data as follows: “specificity, explicitness, prominence and clarity of disclosures to the consumer about the purpose for collecting, ~~or~~ processing, or using their personal information.”

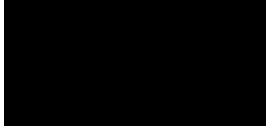
4. § 7012. Notice at Collection of Personal Information. Section 7012 states that, “the purposes of the Notice at Collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them, the purposes for which the personal information is collected or used and whether that information is sold or shared, so that consumers to have a tool to exercise meaningful control over the business’s use of their personal information.” The algorithms that impact the consumers personal information should be disclosed in the Notice at Collection so that users can exercise the aforementioned control around their personal information.

Proposed Change: The addition of “algorithms” in the Notice at Collection as an item to be included as (e)(6).

We would strongly encourage the California Privacy Protection Agency to consider future rulemaking that addresses current ambiguities in the proposed rules. Specifically, by expanding consumer control of data through requiring social media platforms to offer open APIs, which will allow users to choose tools (whether developed by third-party developers or by the users themselves) to better manage the algorithms for materials provided to users and set the terms of their online experience. We believe that consumers deserve real solutions for user control, protection and safety.

I would welcome the opportunity to continue this conversation with the Board. Thank you for your consideration.

Sincerely,



Tracy Chou
CEO and Founder
Block Party

From: Otaku Nation <[REDACTED]>
Sent: Thursday, November 17, 2022 3:27 PM
To: Regulations
Subject: CCPA Public Comment
Attachments: Public comment on proposed regulation.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hi All,

Please see the attached pdf document of our public comment for the proposed regulation on consumer privacy.

Kind Regards.

November 17, 2022

INTRODUCTION

Hi there we are simple consumers who work in IT backgrounds, after reading the proposed bill we have suggestions when it comes to retention of personal information under **Article 1 Section 7002 "Restriction On The Use And Collection Of Personal Information"** We are mentioning regarding social communication business that provides private messaging support.

It would be really amazing if the proposed bill would clearly mention regarding private communication with regards to data retention, as you might know this has been a really essential topic recently in keeping users private communications safe and secure as possible. We would like it if the following could be considered in the rulemaking process.

Contents of private communication (Direct message) should not be retained by business on their systems/servers if all users of that particular conversation have deleted their accounts with that service. Private messages do not need to be removed immediately if there is at least one active user with the service in that private communication.

REASONS

A lot of companies retain private communications between users who are no longer with the platform and keep their private communication indefinitely, these services mention in their privacy policies that users' messages are anonymized once they request to delete their accounts but in reality it is not. You can still tell who Jack Wilson (not a real person) is from the contents of the messages and still be able to get all sorts of information about him like addresses, health, pictures etc and successfully re-identified him. This is very wrong from a privacy standard point. There is literally no reason why a company should hold such sensitive information of users who have left the service, especially if it's not end-to-end encrypted. Only some social media companies delete both sides of the conversations from their servers/systems if both users delete their accounts or by temporary retaining messages and providing the active users with copy of the deleted users messages and then they remove all contents if the active user deletes their account later down the line, whereas a big chunk of companies still keep private communications as plain text on their servers and never deletes them. This makes it really uneasy for consumers to know that their private communication still exists and could be used to dox them in case of future data breaches.

Hence why we highly recommend if the bill could mention more regarding private messages. The bill does not mention enough to protect consumers' private messages even after mentioning it is considered as sensitive personal information, only mentions that companies can

moderate the reported messages in good faith that it contains illegal or hateful content reported by their users which is valid. Consumers share very private information between family and friends and must not be read by anyone else, not even businesses unless reported. Some consumers do not even know what end-to-end encryption is and assume that their messages are secure when it is clearly not. It's high time business protects our private communication while keeping them safe. Many people in the privacy community and government bodies have requested better handling of users' private communication.

WHAT COULD BE DONE TO IMPROVE THE PROPOSED BILL

If any or all of the following could be added to the proposed bill would give consumers more control over their content when it comes to their private messages please feel free to improve/modify them before considering adding them to the rulemaking process.

1. As mentioned above in the **reason** section, social media companies that provide messaging services need to delete users' private messages from their servers/systems if all users of that particular conversation have deleted their accounts with the service. This does not apply to messages sent in public spaces as the consumer decided to make these messages publicly available. businesses may retain such messages in public spaces as it expresses the freedom of speech.
2. If social media services makes it hard for active users to access private communication with other users who are no longer with the service, retains the private messages of both those users on their system/servers and the active user is not able to see any of the messages sent by the deleted user, the business must delete the private communication from their system/servers, as no messages are accessible by any of the users who were apart of that communication.
3. Social media services should enable end to end encryption by default for at least user private communication. This is an excellent opportunity to introduce this and make it a standard to protect consumers' private communication. So many consumers have requested for business to add encryption but they never listen. Some big social media companies are slowly adding end-to-end encryption to their platforms for users' private messages but there are still a few stubborn businesses who will refuse to add such encryption.

CONCLUSION

This bill needs to be strong when it comes to consumers' private communication and prevent bad actors from accessing such sensitive information. Text messages being the biggest data that businesses have on their users.

Since this comment might be submitted publicly we believe multiple consumers would agree with our statements mentioned above.

Our main purpose for this comment is for proposed bill to clearly mention that communication businesses cannot retain sensitive information (private messages) on their system/servers if all users of that private conversation are no longer with that service, messages cannot be anonymized or de-identified they must be deleted immediately or eventually however personal information that does not fall under the category of sensitive information can be anonymized, de-identified or deleted.

Thank you for taking your time to read this, hope this comment helps in making the proposed bill stronger. All information provided is from different privacy groups, new trends in how businesses are protecting users' private communication, users complaints from public posts about users retaining their private conversation.

From: [REDACTED]
Sent: Thursday, November 17, 2022 7:07 PM
To: Regulations
Subject: CPPA Public Comment
Attachments: Exception to CCPA.docx

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

See Attached

Status of the Proposal: This rulemaking is undergoing a 15-day public comment period. Any interested person or their authorized representative may submit written comments regarding the proposed regulatory action. The written comment period opens on **Thursday, November 3, 2022** and closes at **8:00 am on Monday, November 21, 2022**. Comments may be submitted by:

- E-mail to: regulations@cppa.ca.gov. Please include "CPPA Public Comment" in the subject line and include your comments as an attachment to the email. This will help ensure that personal information is not posted to the Agency's website.

Theresa Rodriguez Fritz, Attorney
FRITZ LAW OFFICES
950 College Avenue
Santa Rosa CA 95404
Website: www.fritzlawoffices.com
For Court & Attny Correspondence:

General: [REDACTED]

Fax : [REDACTED]

Phone: [REDACTED]



This electronic communication, including attachments, is intended for the named recipient(s) only. It may contain information protected by attorney-client privilege, confidentiality and applicable privacy laws. If you have received

this email in error, please notify the sender immediately by replying to this email or by telephone at [REDACTED], and then delete the email and any attachments immediately. If you are not the intended recipient, any use, copying, disclosure, dissemination or distribution is strictly prohibited. Please do not disclose the contents to anyone. Thank you.

There should be a clear exception for certain information that an employer is required to collect and report to a government or other institutions such as Banks and Insurance Companies.

If the law broadly states that employers will be prohibited from collecting personal information on their employees, how can the employer comply with other obligations without being in violation? Government agencies such as Employment Development Department (EDD) and Homeland Security require employers to collect and/or report Social Security numbers, other identification information on EDD tax forms and the Form I-9. In addition, Banks and Insurance Companies require reporting of certain employee personal information.

From: Divya Sridhar <[REDACTED]>
Sent: Friday, November 18, 2022 10:03 AM
To: Regulations
Subject: CPPA Public Comment (SIIA - 111822)
Attachments: SIIA Comments_ CPRA _111822.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear Mr. Soublet and the CPPA:

Thank you very much for the opportunity to comment on the modified text of the CCPA/CPRA draft regulations.

Attached we share our comments on behalf of SIIA. Please do not hesitate to reach out if you have further questions.

Best,
Divya



Divya Sridhar, Ph.D.
Senior Director, Data Protection

[REDACTED]
[REDACTED]

Siia.net



November 18, 2022

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd.
Sacramento, CA 95834
Via email to regulations@ccpa.ca.gov

RE: Modified Text of the California Consumer Privacy Act Proposed Regulations

Dear Mr. Soublet and the California Privacy Protection Agency:

On behalf of the Software & Information Industry Association (SIIA), we write in response to the California Privacy Protection Agency's draft modified rules to implement the California Privacy Rights Act (CPRA) and update existing regulations under the California Consumer Privacy Act (CCPA).

SIIA is the principal trade association for the software and digital information industries worldwide. Our members include over 450 companies and associations reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide and companies specializing in data analytics and information services.

SIIA supports privacy as a fundamental value, one essential to individual autonomy and a functioning democracy. We believe that data privacy standards that harmonize meaningful consumer safeguards with appropriate business compliance will ensure smooth implementation of uniform data privacy practices. We have previously provided stakeholder input on CCPA and CPRA, as the law sets an important milestone for companies engaging in interstate commerce both within and outside of California.

We commend the CPPA on taking SIIA's (and other stakeholders') constructive feedback into consideration. For example, we were pleased to see the CPPA's decision to: streamline notice at collection for first and third parties, as well as streamlined practices for the information shared with consumers in the privacy policy (§ 7012); expand the types of entities that can claim "disproportionate effort" to fulfill consumer requests (§ 7023 and § 7001); allow businesses the option to display whether the company processed an opt out preference signal (§ 7025); and the decision to add clarity with regard to the business purposes for which service providers can use data (including when the business purpose is not specified in the written

contract required by the CCPA). The substantive changes in the modified regulations will greatly reduce consent fatigue and support harmonized business processes.

We provide recommendations intended to better align the CPRA regulations with the letter and spirit of the statute. Our suggested edits to the proposed regulations are reflected in **purple, bolded** text. We do so to avoid confusion across earlier drafts of the proposed regulations.

The following are outstanding recommendations that require additional consideration:

- Issue 1: Clarify the considerations for businesses to meet the expectations of the “average consumer”, to streamline business compliance. (§ 7002)
- Issue 2: Remove the example that implies businesses are prohibited from leveraging advertising based on email addresses, which diverges from statute. (§ 7050)

Issue 1: Clarify considerations for businesses to meet the expectations of the “average consumer”, to streamline business compliance. (§ 7002)

We appreciate that the CPPA incorporates our recommendation to modify language in § 7002 in an effort to clarify the reasonable expectations of the average consumer that the business should consider as it determines whether to process the consumer’s personal information without consent. The CPPA Statement of Reasons further clarifies the section, explaining that the “purpose for which the personal information was collected or processed must be consistent with the reasonable expectations of the consumer and enumerates factors that establish the reasonable expectations of the consumer.”¹

We recommend clarifying the section to ensure practical, streamlined business compliance, as follows.

Therefore, SIIA recommends the following edits:

[§ 7002. Restrictions on the Collection and Use of Personal Information.](#)

- (b) The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed. The consumer’s reasonable expectations concerning the purpose for which their personal information will be collected or processed shall be based on the following:
- (1) The relationship between the consumer(s) and the business. For example, if the consumer is intentionally interacting with the business on its website to purchase a good or service, the consumer likely expects that the purpose for collecting or processing the personal information is to provide that good or service or another related product or service within the same industry. By

¹CPPA. Page 3. [Explanation of Modified Text of Proposed Regulations.](#)

contrast, for example, the consumer of a business's mobile flashlight application would not expect the business to collect the consumer's geolocation information to provide the flashlight service.

[...]

- (3) The source of the personal information and the business's method for collecting or processing it. For example, if the consumer is providing their personal information directly to the business while using the business's product or service, the consumer likely expects that the business will use the personal information to provide that product or service **or another related product or service within the same industry. However, the consumer may not expect that the business will use that same personal information for a different product or service offered by the business or the business's subsidiary.**
- (5) ~~The degree to which the involvement of service providers, contractors, third parties, or other entities in the collecting or processing of personal information is apparent to the consumer(s). For example, the consumer likely expects an online retailer's disclosure of the consumer's name and address to a delivery service provider in order for that service provider to deliver a purchased product, because that service provider's involvement is apparent to the consumer. By contrast, the consumer may not expect the disclosure of personal information to a service provider if the consumer is not directly interacting with the service provider or the service provider's role in the processing is not apparent to the consumer.~~

(c) ~~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. Whether another disclosed purpose is compatible with the context in which the personal information was collected shall be based on the following:~~

- (1) At the time of collection of the personal information, the reasonable expectations of the consumer(s) whose personal information is collected or processed concerning the purpose for which their personal information will be collected or processed, based on the factors set forth in subsection (b).
- (2) The other disclosed purpose for which the business seeks to further collect or process the consumer's personal information, including whether it is a Business Purpose listed in Civil Code section 1798.140, subdivisions (e)(1) through (e)(8).

(3) The strength of the link between subsection (c)(1) and subsection (c)(2). For example, a strong link exists between the consumer's expectations that the personal information will be used to provide them with a requested service at the time of collection, and the use of the information to repair errors that impair the intended functionality of that requested service **or another related product or service within the same industry**. This would weigh in favor of compatibility. By contrast, for example, a weak link exists between the consumer's reasonable expectations that the personal information will be collected to provide a requested cloud storage service at the time of collection, and the use of the information to research and develop an unrelated facial recognition service.

(d) For each purpose identified in subsection (a)(1) or (a)(2), the collection, use, retention, and/or sharing of a consumer's personal information to achieve that purpose shall be reasonably necessary and proportionate. The business's collection, use, retention, and/or sharing of a consumer's personal information shall also be reasonably necessary and proportionate to achieve any purpose for which the business obtains the consumer's consent in compliance with subsection (e). Whether a business's collection, use, retention, and/or sharing of a consumer's personal information is reasonably necessary and proportionate to achieve the purpose identified in subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent, shall be based on the following:

- (1) The minimum personal information that is necessary to achieve the purpose identified in subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent. For example, to complete an online purchase and send an email confirmation of the purchase to the consumer, an online retailer may need the consumer's order information, payment and shipping information, and email address.
- (2) The possible **negative** impacts on consumers posed by the **unauthorized disclosure of the** business's collection or processing of the personal information. For example, a possible negative impact of collecting precise geolocation information is that it may reveal other sensitive personal information about the consumer, such as health information based on visits to healthcare providers.
- (3) The existence of additional safeguards for the personal information ~~to~~ **specifically address the possible negative impacts on consumers considered by the business in subsection (d)(2)**. For example, a business may consider encryption or automatic deletion of personal information within a specific window of time as potential safeguards.

IIA Comments:

Section 7002 (b)(1) would not permit the processing of personal information for multiple products or services, within the same industry, by one business. Businesses engage in data analytics, product development and testing on a variety of related products and services within a related industry/vertical on a fairly routine basis, so this section would hamstring and curtail innovation. We want to underscore the importance of information collection to support product development within the same industry.

We also recommend revising § 7002 (b)(3) by clarifying the expectation and deleting the example in the last sentence. The section focuses on how a business can determine whether processing a consumer's personal information is in line with the reasonable expectations of the consumer. The expectation and example in § 7002 (b)(3) states that a business would not be able to "use personal information for a different product or service offered by the business or the business's subsidiary." This is a critical restriction that places burdensome limitations on a fairly routine part of the business life cycle, used to support product development, market research, and basic data security practices – without a meaningful benefit to consumers. By restricting the use of consumer data for companies and their supporting entities (conglomerates and their service providers and contractors) for an overly specific purpose, restricted to only one specific product or service, businesses are subject to obtaining consent for every individual update or analytical test they run on similar products within the same vertical or industry (including preliminary/ early stage design tests), which will likely result in consent fatigue. As well-established research² suggests, overly restrictive practices reminiscent of the data minimization and purpose limitation principles in GDPR may hamstring the potential of an innovative digital marketplace.

Section 7002 (b)(1), (b)(3), and the example in § 7002 (c)(3) conflict with the new language that supports and streamlines business compliance under § 7050(a)(3)³. Section 7050(a)(3) was intentionally added to the regulations to ensure that businesses *can* use consumer personal information for internal use "to build or improve the quality of services." As noted previously, and in line with § 7050(a)(3), businesses, service providers and contractors should be able to use consumer personal information for the purposes of product development, security compliance and investigations, and a range of other purposes that would be beneficial for multiple products in the product life cycle that support research and development. Thus, revising § 7002 (b)(1), deleting the section in § 7002 (b)(3), and revising the example in § 7002 (c)(3) would align with the intent of § 7050(a)(3).

In addition, we recommend striking § 7002 (b)(5). Section § 7002 (b)(5) places the expectation on businesses to base the reasonable consumer standard on the consumer's

² Tal Z. Zarsky, "[Incompatible: The GDPR in the Age of Big Data](#)," Seton Hall Law Review 47 no. 995 (2017).

³ In the Statement of Reasons, CCPA notes: "7050(a)(3): Revised this subsection to clarify that the service provider or contractor may use personal information collected pursuant to the contract with the business to build or improve the quality of the services that the service provider or contractor is providing, even if this business purpose is not specified in the written contract required by the CCPA and these regulations, provided that they are not using the personal information to perform services on behalf of another person."

understanding of the vast number of service providers or other downstream providers that the business works with. It seems impractical to expect the business to align the expectations to a standard that rationalizes the consumers' understanding of the potentially vast and excessive range of entities working with the business, including all service providers and third parties. From a compliance perspective, it would be better to remove this language and instead, rely on the expectations of the business to share the information about all downstream providers that is already included in the privacy policy (in line with § 7011).

Next, we are concerned with unwieldy and concerning requirements in § 7002 (d)(2) and § 7002 (d)(3). Section § 7002 (d) notes that “whether a business’s collection, use, retention, and/or sharing of a consumer’s personal information is reasonably necessary and proportionate to achieve the purpose identified in subsection (a)(1) or (a)(2)” and other valid methods to obtain consent is to be based on specific data minimization principles that the business must apply before processing the data. As written, the expectation is overbroad, and would require businesses to gauge *all* the possible negative impacts of processing personal information, for potentially *all* consumers. This burdensome requirement places an expectation on businesses to gauge all possible harms to a consumer, whether they include a lack of technical safeguards, or much broader consumer harms that are not based on injury-in-fact. The lack of clarity regarding the “possible negative impacts on consumers” was also noted by CPPA Board Member de la Torre at the recent board meetings⁴ in October. We believe that modifications will bring the language in line with reasonable business compliance.

To clarify § 7002 (d)(2) and § 7002 (d)(3), we recommend the business be expected to gauge the *unauthorized disclosure* of the business’s collection or processing of the personal information and its impact on the consumer. This would place an inherent expectation on the business to implement and maintain technical safeguards for consumers’ personal information, which is part of § 7002 (d)(3).

Issue 2: Remove the example that implies businesses are prohibited from leveraging advertising based on email addresses, which diverges from statute. (§ 7050)

Section § 7050, which focuses on service provider restrictions, includes an example that restricts service providers from fulfilling their obligations to their respective businesses and, in doing so, diverges from statute. The example conflates the role of service providers and third parties. The example suggests that the service provider should not fulfill its duty to the business to use email addresses granted by the business to serve the business’s customers with ads – even if the email addresses are directly obtained by the business and strictly used on the business’s own customers.

Therefore, we suggest the following edits:

⁴ CPPA. Discussion from [October 28 and 29th Board Meeting](#).

§ 7050. ~~§ 7051.~~ Service Providers and Contractors.

(b) ~~(e)~~ A service provider or contractor cannot contract with a business to provide cross- contextual behavioral advertising. Per Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but the service provider or contractor ~~these services~~ shall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or collects from its own interaction with consumers. A person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor with respect to cross-contextual behavioral advertising services.
Illustrative examples follow.

- (1) Business S, a clothing company, hires a social media company as a service provider for the purpose of providing Business S's advertisements on the social media company's platform. The social media company can serve Business S by providing non-personalized advertising services on its platform based on aggregated or demographic information (e.g., advertisements to women, 18-30 years old, that live in Los Angeles). However, it cannot use a list of customer email addresses provided by Business S to identify users on the social media company's platform to serve advertisements to them. The social media company can also use a customer list provided by Business S to serve Business S's advertisements to Business S's customers. However, it cannot use a list of customer email addresses provided by Business S to then target those customers with advertisements based on information obtained from other third party businesses's websites, applications, or services.

IIIA Comments:

We suggest clarifying the example with the suggested sentence (noted above) that authorizes the service provider to fulfill its fiduciary duty in using the list of customer email addresses provided by its business (Business S) to serve Business S's customers with ads. We also recommend adding a sentence to further clarify the prohibition on cross-contextual advertising, which would prevent the service provider from using the same email addresses to target Business S's customers with ads that are grounded in third party sources of information (i.e., information obtained from other third party business websites, applications, or services). This clarification would align the example to how it reads in the statute⁵.

⁵ California Privacy Rights Act. § 1798.140 (k) "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

Conclusion

As noted, after reviewing the most recent draft of the modified regulations, we have identified additional areas where the regulations significantly diverge from the statute. We believe that the draft regulations should be further clarified and aligned to the statute, so that companies are not left with additional outstanding questions, onerous requirements that result in negligible privacy protective benefits to consumers, and high costs to comply, on the heels of the CPRA compliance date: January 1, 2023.

Furthermore, we make two recommendations that require procedural changes. First, we recommend that additional guidance be provided to a) exempt employee and business to business (B2B) data from compliance with CCPA and CPRA, as well as the modified regulations; and b) ensure businesses are provided further support on the appropriate treatment of employee and B2B data with regard to CPRA, including how to mitigate the uncertainty and conflicting requirements imposed on treating employee data and B2B data in the same breath as consumer data.

The CPRA draft rules were required to be finalized by July 1, 2022 and become enforceable on July 1, 2023. To ensure consistency with the intent of the statute, which provides for one year between the date when the rules are finalized and the enforcement date, we recommend the enforcement date be shifted to one year from the date of when the rules are finalized. Providing sufficient time for compliance with the regulations will help to mitigate confusion across the business and consumer community.

* * *

Thank you for considering our suggested revisions to the proposed regulations to the CPRA. We are happy to discuss in further detail, as appropriate. For further information, please contact Divya Sridhar, at [REDACTED].

Respectfully submitted,

Divya Sridhar, Ph.D.,
Senior Director, Data Policy
Software and Information Industry Association (SIIA)

From: Edwin A. Lombard III [REDACTED]
Sent: Friday, November 18, 2022 1:07 PM
To: Regulations
Subject: Re: CPPA 15 Day Comment Period Nov 2022
Attachments: CPPA 15 Day Comment Period Nov 2022 FINAL.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Here is the PDF attachment. Please let me know if you received it.



Edwin A. Lombard III
President/CEO
ELM Strategies
1079 Sunrise Avenue, Suite B315
Roseville, CA 95661
[REDACTED]

On Fri, Nov 18, 2022 at 12:59 PM Regulations <Regulations@coppa.ca.gov> wrote:

Mr. Lombard

Thank you for your comment.

The Google document you linked to in your submission is inaccessible.

If you'd like to submit a comment, please send it as a PDF attachment.

Thank You

From: Edwin A. Lombard III [REDACTED]
Date: Friday, November 18, 2022 at 11:54 AM
To: Regulations <Regulations@coppa.ca.gov>
Subject: CPPA 15 Day Comment Period Nov 2022

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Attached please find our CCPA 15 day public comment for the November hearing.

Thank you,

 [CCPA 15 Day Comment Period Nov 2022 FINAL.pdf](#)



Edwin A. Lombard III

President/CEO

ELM Strategies

1079 Sunrise Avenue, Suite B315

Roseville, CA 95661





November 16, 2022

California Privacy Protection Agency
 Attn: Brian Soublet
 2101 Arena Boulevard
 Sacramento, CA 95834
 Submitted via email: regulations@coppa.ca.gov.

Re: California Privacy Protection Agency (CPPA) Public 15-Day Comment Period

Mr. Soublet:

On behalf of our respective organizations and the California businesses we represent, we are submitting our collective comments on the CPPA's proposed California Consumer Privacy Act Regulations ("regulations") and the amendments made available to the public on November 3, 2022, for a 15-day public comment period. We appreciate the opportunity to provide comments on a significant body of law that will have consequential impacts on the many small, diverse businesses we represent.

We reiterate our commitment to upholding Proposition 24 to provide strong privacy protections for consumers, supporting the CPPA in fulfilling its statutory obligations to develop reasonable privacy regulations (e.g., our legislative budget testimonies in support of the CPPA's budget request for 34 additional positions and for extending the CPPA's July 1, 2022, deadline), and working with the CPPA to

achieve the necessary balance to avoid unintended consequential impacts on the many small, diverse California businesses we represent. This balance was sought in Proposition 24, section 3 (C) 1:

- The rights of consumers and the responsibilities of businesses should be implemented with the goal of strengthening consumer privacy while giving attention to the impact on business and innovation. (Emphasis Added)

Much to our continued dismay, however, the perspectives of California small businesses have been ignored. While standing up a new agency and drafting arguably one of the most complex bodies of law presents foreseeable challenges, it is perplexing that the CPPA acknowledged the need to work with the California Legislature (“Legislature”) to have more time to do its work but did not follow through to avoid missing critical deadlines. *In other words, why does the CPPA continue to go down the irresponsible path of jamming Californians with regulations that lack authority and clarity and are likely to change within months of enforcement when it has a more responsible option?*

There is no shame in missing a deadline due to the many challenges that come with a new agency and the lingering workforce impacts of the pandemic. However, there is disgrace in knowing and acknowledging that deadlines will be missed but continuing to rush the job anyway and ignoring the known consequences that lie ahead.

Below is a chronicle of CPPA actions and inactions, the significant potential consequences, and the suggested course of action for the CPPA to ensure that the regulations are equitable for stakeholders. This includes working with the Legislature to extend the approaching July 1, 2023, enforcement date to January 1, 2024, which is consistent with the 1-year compliance period in Proposition 24.

The CPPA Continues to Miss Critical Deadlines

The CPPA violated Proposition 24 by missing the July 1, 2022, deadline to adopt final regulations and will continue to violate the proposition by tabling cybersecurity audits (Section 1798.185 (a)(15)(A)), risk assessments (Section 1798.185 (a)(15)(B)) and automated decision-making technology (Section 1798.185 (a)(16) (See page 6 of Notice of Proposed Rulemaking)). When the CPPA discussed the issue, “informally missing the deadline” was the nonchalant

description used, which is appalling considering the legal background many of the agency's members and staff possess. "Informally missing the deadline" of July 1, 2022, is not legally permissible in Proposition 24.

According to the Office of Administrative Law (OAL), for a regulation to be effective on January 1, 2023, the final regulations must be filed with the Secretary of State (SOS) between September 1 and November 30, 2022. Before the regulations are filed with the SOS, the CPPA must submit the proposed framework to the OAL, which then has 30 working days to approve or disapprove regulations.

(https://oal.ca.gov/rulemaking_participation/)

As it currently stands, the CPPA will not finish the privacy regulations before the November 30, 2022, deadline, which now means that the privacy regulations will likely be effective no sooner than April 1, 2023, just three months before the CPPA enforcement date commences on July 1, 2023. This is unequivocally unacceptable. Under the current CPPA timeline, the businesses we represent will only have three months to comply when all California businesses were provided a one-year compliance period under Proposition 24.

The CPPA Refuses to Extend Critical Deadlines

The CPPA had and continues to have the option to avert many of the potential consequences that it now faces, but it has chosen not to do so. The public record clearly shows that the CPPA had a legislative option before the 2022 legislative session began, as reiterated below:

CPPA Meeting on September 7, 2021

- "If we do the math, we can't meet the May [submission] deadline to submit [to the Office of Administrative Law]."
- "Once we hire the Executive Director, we need to find a legislative champion to push back the deadline." (Emphasis Added)
- "Hate to rush them." "Rather get good set of rules." "Lots of countries and states [are watching this] ..., get it right"

CPPA Meeting on October 18, 2021

- The CPPA discussed “informally missing” the July 1, 2022, deadline.

CPPA Meeting on February 17, 2022

- When asked about the July 1, 2022, deadline, the agency’s executive director acknowledged that the rulemaking process is likely to continue past the July 1, 2022, deadline.

Proposition 24 can be amended by the Legislature. The issue here is that the CPPA was on notice and acknowledged last fall that it did not have enough time to meet the July 1, 2022, regulatory adoption deadline, yet the agency chose to do nothing about it.

In the spring of 2022, our organizations voiced support in legislative budget hearings to extend the July 1, 2022, regulatory adoption deadline to January 1, 2023, and the enforcement date of July 1, 2023, to January 1, 2024. The CPPA ignored our suggestion.

In our previous comment letter, prior to legislative adjournment, our organizations requested that the CPPA “work with the Legislature to extend the July 1, 2022, deadline, and July 1, 2023, enforcement date before the legislative session end[ed] on August 31, 2022, to remedy issues in the draft regulations and rulemaking process.” *It begs the question, why did the CPPA not work with the Legislature to extend critical deadlines when it knew it cannot meet them?*

The CPPA’s Deficient Regulatory Content and Process

There is no real consensus or direction on how the CPPA will develop the privacy regulations. Further, the consequences to California businesses are viewed as secondary, if considered at all at this point.

It is difficult to reconcile board members who voiced support for “building a plane while flying it” (an unfortunate analogy given the magnitude of Proposition 24) with “I am uncomfortable doing legal analysis on the fly.” *What is the agency’s approach, and how is it considering those impacted by the regulations?*

It is even more troubling when a board member provides a thoughtful analysis, requests a certain provision be tabled, given such issues may be outdated or

incomplete, and requests to speak with staff to confer but is summarily rejected by the chair and staff. Further, we are unaware of any provision in Proposition 24 that authorizes board members to defer to staff on regulatory content and process. Consider the adopted board's motion, in part, on October 29, 2022:

- The Board directs Staff to take all steps necessary to prepare and notice modifications to the text of the proposed regulatory amendments for an additional 15-day comment period. The modifications shall reflect the changes proposed by Staff in the written meeting materials, except staff shall further modify the text to: Use the Staff's discretion to consider and include the following items if feasible at this time (Emphasis Added).

After the CPPA board meeting on October 29, 2022, our understanding was that the CPPA was going to meet and vote on the proposed changes in its scheduled meeting on November 4, 2022. From what we heard, on October 29, 2022, the CPPA Chair mentioned that the November 4, 2022, meeting was a placeholder because staff may need more time to draft the proposed changes.

Instead, on November 1, 2022, the CPPA cancelled its November 4, 2022, scheduled meeting, and on November 3, 2022, issued an announcement of the beginning of a 15-day comment period for the proposed changes. At this point, there is nothing on the record about whether these proposed changes have been adopted by the board, or whether the board is going to adopt them.

Nonetheless, we would appreciate the board's thoughts on how its October 29, 2022, motion is consistent or inconsistent with Section 24.6, 1798.199.35, in Proposition 24:

- The agency board may delegate authority to the chairperson or the executive director to act in the name of the agency between meetings of the agency, except with respect to resolution of enforcement actions and rulemaking authority (Emphasis Added).

The CPPA Regulations' Significant Potential Consequences

We resubmit that the small businesses we represent are the backbone of our local communities and a major part of California's economic engine. Further, our state's small, diverse businesses cannot be expected to survive yet another layer of

economic burden on top of continuing inflation, supply chain challenges, workforce challenges and the ongoing pandemic they have already been forced to grapple with.

We understand that the CPPA takes the position that the regulations only apply to larger companies. This is not so, and anyone who takes that position truly does not understand that there is always economic impact on the small businesses we represent, especially those reliant on online platforms and technology. *We will say it again: when large businesses catch a cold, our small businesses catch pneumonia.*

Here is a practical application of the CPPA regulations and the potential impact on our businesses. In the current time frame, the CPPA regulation goes into effect on April 1, 2023. Many of the businesses we represent may or may not be aware of many aspects of the regulations at this point, and they may hear about it sometime in May 2023 and need additional information and time to process what is required of them.

At that point, they may hire an individual or company to help them understand what they need to do (assuming they have the financial resources), and that entity may charge a significant amount of money to help them comply by July 1, 2023. If these businesses have the money to determine how to comply with the regulations, then they may survive, but will face ongoing compliance costs because, as noted by the CPPA during its October 29, 2022, meeting, the regulations may be amended within six to eight months after they become effective.

Conversely, if these businesses do not have the financial means to determine how to comply with regulations, then these businesses may just shut down, a significant consequence we have raised numerous times. These consequences are avoidable, and we urge the CPPA to take responsible action to prevent such outcomes.

Another potential consequence is a lawsuit challenging the regulations for failing to meet statutory deadlines. If a lawsuit should ensue, then privacy protections for consumers under Proposition 24 could be further delayed.

Recommended CPPA Actions Moving Forward

The enforcement date of July 1, 2023, is critical for businesses, particularly now that the regulations could be effective on April 1, 2023. The most practical and reasonable approach is for the CPPA to work with the Legislature to extend the July 1, 2023, enforcement date to January 1, 2024.

We appreciate the CPPA's effort to add Section 7301 (b) with the intent of addressing compliance and enforcement issues:

- As part of the Agency's decision to pursue investigations of possible or alleged violations of the CCPA, the Agency may consider all facts it determines to be relevant, including the amount of time between the effective date of the statutory or regulatory requirement(s) and the possible or alleged violation(s) of those requirements, and good faith efforts to comply with those requirements.

However, the proposed addition of Section 7301 (b) is insufficient. It is important to keep in mind that many, perhaps thousands of businesses, will be unaware of the regulations, and will need time to understand what is required before they can implement changes. That is, if they can even afford to make the required updates on their end.

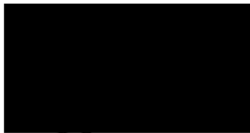
Furthermore, the term "good faith efforts" is ambiguous and arbitrary. On a more practical matter, does the CPPA even have the resources necessary to handle thousands of businesses asking for some kind of relief if they cannot comply with the regulations? Does the CPPA want to be in a position of adjudicating such matters when many are likely to point out the CPPA gave itself a pass when failing to meet its own statutory deadlines – on top of placing the burden of compliance on businesses by July 1, 2023?

In closing, we commend board member de la Torre for providing a thoughtful approach to the regulation by calling out either incomplete or outdated provisions in the regulations and the willingness to iron out important details that may inevitably have larger consequences for consumers and businesses. We also commend board members Le and Thompson for raising the potential consequences that may arise for the businesses we represent in light of the upcoming July 1, 2023, enforcement date.

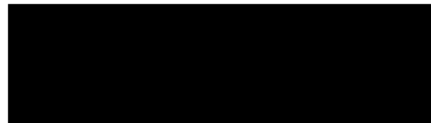
We ask Chair Urban and board member Mactaggart to provide the strong leadership that the board needs and work with the Legislature to extend the July 1, 2023, enforcement date to January 1, 2024. This request is fair and reasonable given that Proposition 24 requires a 1-year compliance period, and that period is likely to be truncated into three months based on the anticipated effective date of the regulations (April 1, 2023).

We appreciate the opportunity to provide comments on a significant body of law that will have consequential impacts on the small, diverse businesses we represent, and our collective organizations are prepared to work with the CPPA in addressing the concerns discussed above.

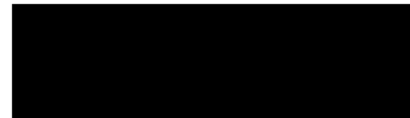
Sincerely,



JULIAN CAÑETE
President & CEO
California Hispanic
Chambers of Commerce
1510 J Street, Suite 110
Sacramento, CA 95814



EDWIN A. LOMBARD III
President/CEO
ELM Strategies
1079 Sunrise Avenue, Suite B315
Roseville, CA 95661



PAT FONG KUSHIDA
President & CEO
California Asian Pacific
Chamber of Commerce
1610 R Street, Suite 300
Sacramento, CA 95811

cc: Members of the Legislature
Dana Williamson, Executive Secretary
Ann Patterson, Cabinet Secretary; Office of Governor Gavin Newsom
Christy Bouma, Legislative Affairs Secretary; Office of Governor Gavin Newsom
Dee Dee Myers, Senior Advisor & Director; Governor's Office of Business & Economic Development
Tara Gray, Director; California Office of Small Business Advocate

From: Aaron Harburg [REDACTED]
Sent: Friday, November 18, 2022 1:07 PM
To: Regulations
Subject: CCPA Public Comment
Attachments: Proposed Amendments to the CCPA.docx

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello,

Please see the attached comments.

Sincerely,

-Aaron

J.D. CIPP-US | [REDACTED] | www.aaronharburg.com



-Notice-

Although I am an employee of SuperRare Labs, these suggestions are made independent of my involvement in the company and are wholly and entirely my own suggestions as a privacy professional and blockchain enthusiast. While the adoption of these suggestions will benefit SuperRare Labs and the RareDAO Foundation I am not submitting these as part of my duties to the company or as a member of the DAO.

Summary

The bulk of these comments are designed to recognize the unique data privacy challenges associated with blockchain technology. It is an error to believe technologies such as Bitcoin and Ethereum are anonymous when they are at best pseudo-anonymous.¹ If you know the identity associated with a public address you can trace that person's transactions.² In this respect it is more transparent than traditional banking transactions which requires heightened privacy for financial information.³

Furthermore, with the advent of NFTs, primarily in the art market, there are places where metadata which would normally be classified as personal information and subject to data deletion requests makes those requests impossible because the information is permanently stored and published. If it could be altered, that would defeat the purpose of the technology.⁴ As NFTs begin to carry more significant data, such as a record of real property deeds and car titles, some methods of controlling sensitive information will be virtually impossible.

¹ Satoshi Nakamoto states that the only way to maintain anonymity is to keep the persons associated with the public wallets private, but that the transactions themselves must be broadcast to maintain the security, stability, and transparency of the system. See Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 6 2009.

² Etherscan provides an easy interface to search and scan Ethereum transactions. <https://etherscan.io/aboutus>. Similarly, Blockchain explorer allows you to search through Bitcoin, and other digital assets <https://www.blockchain.com/explorer>.

³ As the FTC outlines, the Gramm-Leach-Bliley Act (12 U.S.C. and 15 U.S.C.) there are a number of obligations of "financial institutions" to protect financial information. See FTC, *How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, <https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act> (last accessed Nov. 10, 2022). See also the "Financial Privacy Rule" 16 CFR Part 313.

⁴ See *supra* note 1.

Finally, the definition of “sale”⁵ also comes into play when someone sells an NFT with personal information embedded in the metadata or executes a smart contract where the parties are known. Thus, it seems nonsensical, because it is impossible, to comply with requests and requirements not to “sell” that information or to otherwise attempt to conceal those transactions.

The most effective and sensible way to address these privacy concerns is to recognize the unique role that blockchain technology works and within these regulations (1) to introduce industry standard definitions and (2) to provide adequate carve-outs and safe harbors for good faith blockchain organizations. To that end none of the definitions suggested are wholly original and are reflective of the existing legal discussions, rules, regulations, and statutes both domestically and globally. California is home to many major blockchain technology firms,⁶ and it would be tragic to stifle such a promising technology due to imposing misguided regulations.

§ 7001. Definitions.

~~...~~ (e)⁷

(e) “Blockchain Technology” means shared, or distributed data structures or digital ledgers used in peer-to-peer networks using computer software, hardware, or collections of computer software or hardware, and networks that utilize or enable parties to:

- (1) Store digital transactions;
- (2) Verify and secure transactions cryptographically; and
- (3) Allow automated self-execution of smart contracts;⁸
- (4) Storage of Metadata including data stored in Interplanetary File Storage Systems;

(f) “Blockchain Transaction” refers to any transaction using Blockchain Technology, including, but not limited to the execution of Smart Contracts, airdrops, transfers of non-fungible tokens (NFTs), or other digital assets, royalties, node mining activity, verification of ledgers, gas or other fees, or publication of blocks.

⁵ CA Civ. Code § 1798.140 (t) (1)

⁶ Crunchbase reports 1,020 Organizations in California with over \$13 Billion in funding, <https://www.crunchbase.com/hub/california-blockchain-companies>, (last accessed Nov. 10, 2022).

⁷ This number is going to reflect the changes of this commentary based on Modified Text of Proposed Regulations see https://cppa.ca.gov/regulations/pdf/20221102_mod_text.pdf (retrieved Nov. 10, 2022).

⁸ Ky. Rev. Stat. § 42.747; Vt. Stat. tit. 12 § 1913

§ 7003. Requirements for Disclosures and Communications to Consumers.

...

(e) For all Businesses using Blockchain Technology or facilitating Blockchain Transactions, a plain language notice within their Privacy Policy or Privacy Notice disclosing the permanent public nature of all information and associated Metadata contained in Blockchain Transactions shall suffice to provide adequate Disclosure under these regulations.

§ 7011. Privacy Policy.

...

(f) All Businesses using Blockchain Technology shall provide a plain language notice to consumers of the permanent, irrevocable, and public nature of all information or associated Metadata involved in Blockchain Transactions and distinguish how categories of information contained in the Blockchain differ from information collected or contained in standard computer databases.

§ 7028. Requests to Opt-In After Opting Out of the Sale or Sharing of Personal Information.

...

(c) All information or Metadata contained, placed into, transacted with or through Blockchain Technology or in Blockchain Transactions whether actually embedded shall be considered “publicly available” information pursuant to CA Civ. Code § 1798.140(o)(2). So long as there is an adequate Disclosure, no information using or contained in any Blockchain Technology or Blockchain Transaction shall be categorized as a sale and shall be per se consumer direction to a business or organization to intentionally disclose personal information pursuant to CA Civ. Code § 1798.140 (t) (2) (A).⁹

§ 7050. Service Providers and Contractors.

...

(h) No intermediary such as a node involved in verifying Blockchain Transactions shall be construed to be a Service Provider or Contractor of a Business using Blockchain Technology.

⁹ PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 72-76 (2018).

§ 7052. Third Parties.

...

(c) No intermediary such as a node involved in verifying Blockchain Transactions shall be construed to be a Third Party of a Business using Blockchain Technology.

§ 7305. Safe Harbor for Blockchain Technology Businesses.

- (a) All Businesses that principally rely on or operate using Blockchain Technology and Blockchain Transactions shall not be held liable for any failing to adequately protect any and all information contained in the Blockchain, or the attendant Metadata so long as said Business provides adequate notice to consumers as described in § 7003 (e) of these regulations.
- (b) None of the rights consumer's rights pursuant to CA Civ. Code Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125 shall apply for any information contained in Blockchain Transactions or the attendant Metadata.
- (c) No right of action against Businesses providing adequate Disclosure shall be available to any consumer who knowingly and intentionally interacts with Blockchain Technology to perform Blockchain Transactions for a Businesses failure to delete, modify, or conceal information published to the Blockchain regardless of how sensitive that information may be or the age of the subject.

Sincerely,
Aaron Harburg, CIPP-US
Cyberlaw Expert at SuperRare® Labs
J.D. 2022 California Western School of Law

From: Brooke Armour [REDACTED]
Sent: Friday, November 18, 2022 3:13 PM
To: Regulations
Subject: CPPA Public Comments from California Business Roundtable
Attachments: the California Privacy Protection Agency Comments CBRT November 18.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Mr. Soublet:

Attached please find public comment from the California Business Roundtable on the rulemaking process under the California Consumer Privacy Act.

Please do not hesitate to reach out if you have any questions or we can help expand on any of the arguments made in this letter.

Thank you,
Brooke



**California
Business
Roundtable**

Brooke Armour Spiegel
Executive Vice President
1301 I Street | Sacramento | 95814
[REDACTED] | [REDACTED]

Leadership for Jobs and a Strong Economy

November 18, 2022

Via Email to regulations@coppa.ca.gov

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

Re: CCPA Public Comment

Dear Mr. Soublet:

The California Business Roundtable appreciates the opportunity to submit comments to the California Privacy Protection Agency (“CCPA”) as part of the CCPA’s rulemaking process under the California Consumer Privacy Act (“CCPA”). The Business Roundtable is a statewide business association made up of CEO’s and senior leadership of California’s major employers.

We have reviewed the modifications that the CCPA has proposed to the regulations proposed pursuant to the CCPA (the “Modified Proposed Regulations”) and we appreciate the consideration that the CCPA has given to our comments to the original draft regulations published on July 8, 2022. But we respectfully submit that the Modified Proposed Regulations should be clarified further to recognize the status of package transportation providers as “businesses” given that carriers, and not their retailer customers, determine the purposes and means of the processing of package-related information and addressing details.

As we explained in our comments to the original draft regulations, the package transportation industry is unique in that a significant portion of the personal information processed in core, day-to-day operations is received not directly from consumers, but instead from retailers and other corporate customers. This information takes the form of addressing details and package-related information, such as package dimensions and weight (collectively, “Shipping Information”).

When a consumer buys a product online, the online merchant provides a package to a carrier along with associated Shipping Information. Transportation providers use this information to fulfill the requested service of delivering the product, but they also process this data inherently for purposes and via means that they, and not the online merchant, determine. This is why transportation providers are considered “controllers” under the EU General Data Protection Regulation (“GDPR”) and UK GDPR, and why they should be deemed “businesses,” not service providers, under the CCPA. Further, this sharing of Shipping Information with transportation providers should be deemed not to constitute a “sale” of personal information because the sharing is performed at the direction of the consumer who has instructed the retailer to ship the goods to the consumer’s designated address.

1. Transportation Providers Are “Businesses” as to Shipping Information, not “Service Providers.”

a. Package Transportation Providers Determine the Purposes and Means of the Processing of Shipping Information and Therefore Constitute “Businesses” as to Shipping Information Within the Meaning of the CCPA.

Transportation providers use Shipping Information by necessity for more than simply to deliver individual packages to each individual address. Shipping Information is inherently embedded into the operations of transportation providers, similar to how an organization might consume and integrate fuel or other supplies into its operations. As a result, transportation companies, not their retailer and other corporate customers, “determine the purposes and means of the processing of [this] information” and therefore constitute businesses, not service providers, under the CCPA.¹ For example:

- Carriers use Shipping Information continuously and on an automated basis for package routing within their networks; transportation and delivery planning and optimization; and to make decisions about package network optimization (including locations of facilities, retail outlets, staffing, “drop boxes” where consumers can pick up and leave packages, and capital investment). They do not simply use the information to deliver a specific package and then forget it.
- Shipping Information constitutes a combination of information received from customers, information carriers append from their own historical information and operations (including very specific details of package handling, status, and routing within a package network), and information they receive from third parties. The individual elements received from customers are integrated into this data and are not reasonably capable of being pulled back out.
 - Carriers continuously and automatically update Shipping Information about individual packages with additional information concerning individual shipment attributes, and operational details and requirements for shipments meeting such attributes (e.g., handling of a particular package due to its dimensions and weight (“DimWeight”) or service level (e.g., standard vs. priority)) in order to fulfill deliveries and operate and improve the carrier’s package transportation network. Carriers do this in order to route large numbers of deliveries to the right place at the right time, to manage the transportation network, and to improve the shipping network for future deliveries.
 - One of the more prominent examples of this is addresses: annually, carriers correct tens or hundreds of millions of addresses that customers have submitted to them using information carriers collect while delivering packages, or from data acquired from, e.g., the US Postal Service. Once an address is corrected, it enables future shipments from any other corporate customer to reach that same address as desired by the consumer(s) resident at that address.

These processing activities and the means of effecting them are all determined by the transportation provider, not the retailer or other corporate customer. The transportation provider therefore clearly constitutes a “business” within the meaning of the CCPA.²

¹ Cal. Civ. Code § 1798.140(d).

² Id.

It is important to note also that carriers also have the corresponding obligations of a business under the CCPA, such as to accept and fulfill requests to know and requests to delete. But if carriers are deemed to constitute service providers, and not businesses, when the shipper happens to be a corporate customer, then the carrier's obligation will be to direct a consumer submitting a request back to the corporate customer. This would be an inefficient result which would create a risk of consumer confusion. Indeed, our members' experience is that consumers continue to see themselves as having direct relationships with the individual carriers delivering shipments to them, whether in connection with tracking shipment status, submitting claims, or requesting privacy-related information.

b. A "Service Provider" Designation under the CCPA Will also Create Fundamental Operational Issues for the Package Transportation Industry.

In addition to being legally incorrect, the designation of transportation providers as "service providers" would create a fundamental operational problem for the transportation industry. Section 7050(a) permits service providers to use personal information for several purposes beyond delivering the requested service back to the business. One such use is "[f]or internal use by the service provider or contractor to build or improve the quality of its services uses of personal information." The regulations provide two examples, one of which references transportation companies:

(B) A shipping service provider that delivers businesses' products to their customers may use the addresses received from their business clients and their experience delivering to those addresses to identify faulty or incomplete addresses, and thus, improve their delivery services. However, the shipping service provider cannot compile the addresses received from one business to send advertisements on behalf of another business, or compile addresses received from businesses to sell to data brokers.

But this fails to acknowledge that carriers use shipping data in the form of package level detail or "PLD" for other operational purposes beyond service improvement, such as to perform advanced route optimization and network planning. These uses are essential to improve the efficiency of the flow of goods in the economy and to the ability of carriers to compete, but would be prohibited by the Modified Proposed Regulations if shipping companies are deemed service providers. Even if this interpretation is incorrect – which the Business Roundtable believes to be the case – we anticipate corporate customers may take a different position as a risk management measure because of concerns about other potential constructions of the law.

c. Even Data Protection Authorities in the European Union Recognize that Package Transportation Providers Are Controllers, not Processors.

The European Union General Data Protection Regulation (the GDPR) is arguably the most comprehensive and protective privacy law in the world. Even in the EU, under the GDPR, and under the UK's version of the GDPR, package transportation providers are deemed controllers for the very reason that carriers determine the purposes and means of the processing of Shipping Information.

- As an example, the United Kingdom's Information Commissioner's Office issued guidance in 2014 stating that a delivery service "will be a data controller in its own right in respect of any data it holds to arrange delivery or tracking ... such as individual senders' and recipients' names and addresses."³
- The Bavarian Office for Data Protection Supervision issued 2018 guidance stating that "postal services for letter or package transportation" are generally "not data processing," but instead "specialized services" offered by "an independent controller."⁴

d. The Sharing of Data by Retailers and Other Corporate Customers with Package Transportation Companies to Ship Packages Should Not be Deemed a "Sale" of Personal Information.

When a retailer provides Shipping Information to a carrier, it discloses the information as a business, as defined in the CCPA, to another business. But this disclosure does not constitute a sale of personal information, because (a) consumers are "direct[ing the retailer] to . . . intentionally disclose personal information."⁵

- Subsection 1798.140(ad)(2)(A) provides that a business does not "sell" personal information when "a consumer uses or directs the business to . . . intentionally disclose personal information." This is precisely what happens when consumers order goods from carriers' corporate customers that need to be shipped.
- Specifically, when consumers buy products, they are directing retailers and other corporate customers to disclose Shipping Information to a transportation provider, instead of making their own separate arrangements with a transportation provider directly or, when applicable, retrieving the merchandise from the corporate customer's facility. In fact, consumers generally pay a separate and extra charge for shipping, arguably affirmatively obligating the corporate customer to share information with a transportation provider for shipping purposes.
- To exempt consumer-directed data disclosures from being a "sale," the CCPA does not require that the consumer specify precisely who should receive their personal information. Instead, the § 1798.140(ad)(2)(A) requires only that the consumer "direct" a retailer or manufacturer to "intentionally disclose" their information. Consumers who purchase merchandise from retailers or manufacturers have exactly this in mind – that their data will be provided to a carrier that will deliver the merchandise to them.

Shipping Information remains protected under the CCPA in the hands of the carrier. This information is also protected by a longstanding federal law that regulates its handling and disclosure.⁶

³ See Information Commissioner's Officer, *Data Controllers and Data Processors: What the Difference Is and What the Governance Implications Are* at 12 (June 5, 2014), available at <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf>.

⁴ See Bayerisches Landesamt für Datenschutzaufsicht [Bavarian Office for Data Protection Supervision], *FAQ zur DS-GVO: Auftragsverarbeitung, Abgrenzung* [GDPR FAQs: Data Processing, Distinguishing [between Controllers and Processors]] at 2 (July 20, 2018), available (in German) at https://www.lida.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf.

⁵ Cal. Civ. Code § 1798.140(ad)(2)(A).

⁶ See 49 U.S.C. § 14908.

The Business Roundtable believes the plain meaning of the CCPA establishes that retailers and other corporate customers transfer Shipping Information to transportation providers outside the definition of a “sale” pursuant to the direction of the consumer purchasing the product. But our members are seeing certain corporate customers interpret the law differently, positioning carriers as “service providers” as defined in the CCPA, out of a concern that disclosing data to a separate “business” carries a “sale” risk. This designation would be inconsistent with the facts. Delivery providers determine the purposes and means of the processing of Shipping Information. But such a finding would also prevent package transportation providers from being able to use Shipping Information for any purpose beyond delivering each individual package – a result that will impair operations across the industry with no corresponding consumer benefit. On behalf of our members, we therefore respectfully request the CPPA to clarify the application of Section 1798.140(ad)(2)(A) to Shipping Information that transportation providers receive from businesses, pursuant to the CPPA’s rulemaking authority under Cal. Civ. Code § 1798.185(b).

* * * * *

We appreciate the California Privacy Protection Agency’s review and consideration of our comments in this letter, and look forward to the CPPA’s continued efforts through the rulemaking process. For any questions or feedback, please contact Brooke Armour, Executive Vice President, at [REDACTED] or [REDACTED]. We thank the California Privacy Protection Agency for the opportunity to provide our views for consideration, and look forward to working with you to address the matters outlined above.

Thank you again,

[REDACTED]

ROBERT C. LAPSLEY
President

From: Leyva, Britteny L. <[REDACTED]>
Sent: Friday, November 18, 2022 5:51 PM
To: Regulations
Cc: Shelton Leipzig, Dominique; Kourinian, Arsen; Von Borstel, Megan; Keck, Sasha L.; Daylami, Ronak
Subject: CPPA Public Comment [MB-AME.FID10098200]
Attachments: 11-18-22 - CalChamber November Comment.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Greetings—

On behalf of the California Chamber of Commerce ("CalChamber"), please find attached CalChamber's comments regarding the proposed California Privacy Rights Act regulations.

Best,

Britteny

Britteny L. Leyva

Associate

Pronouns: she/they

Mayer Brown LLP

350 South Grand Avenue 25th Floor

Los Angeles, CA 90071-1503 United States of America

T [REDACTED]

mayerbrown.com

Please consider the environment before printing this e-mail. If you need to print it, consider printing it double-sided.



Mayer Brown LLP
 350 South Grand Avenue
 25th Floor
 Los Angeles, CA 90071-1503
 United States of America

T: [REDACTED]
 F: [REDACTED]

mayerbrown.com

Dominique Shelton Leipzig
 Partner
 [REDACTED]

November 18, 2022

California Chamber of Commerce Comments to Draft California Privacy Rights Act Regulations

EXECUTIVE SUMMARY	1
COMMENTS	3
1. CalChamber Requests That the Agency Delay Enforcement and Require Consideration of the Delay in Finalizing the Regulations When Conducting Agency Investigations of Alleged Violations. (Section 7301).	3
A. Reasons for Proposed Modifications: CPRA's Operational Hurdles Are Complicated by the Delay in Issuance of Final Regulations.....	3
B. Proposed Language for Requested Modifications.....	3
2. The Agency Should Conform the Purpose Limitation Regulation to a Disclosed Purpose Standard That Is Consistent With the CPRA Statute Rather Than a Factors-Like Analysis That Replaces Consumer Expectations With the Agency's Own Judgment (Section 7002).....	4
A. Reasons for Proposed Modifications: The Current Regulations Deviate from the CPRA's Purpose	4
B. Proposed Language for the Requested Modifications.....	5
3. The Agency Should Clarify That Consent Is Not Required Under the CPRA, That a Business Should Take Reasonable Efforts to Avoid Dark Patterns, and That Maintaining Procedures to Avoid Dark Patterns Should Be a Factor Considered for Assessing Violations (Section 7004).	5
A. Reasons for Proposed Modifications: The Current Regulations Should Delete Requirements for Consent and Clarify the Definition of Dark Patterns	5
B. Proposed Language for Requested Modifications.....	6

4.	The Agency Should Modify the Right to Correct to Avoid Requiring Businesses to Disclose Their Authentication and Fraud Prevention Processes, and Apply a “Reasonable Efforts” Standard for Maintaining Personal Information Corrected Within Their Systems (Section 7023).....	6
A.	Reasons for Proposed Modifications: Current Regulations Create Additional Risks for Businesses that Were Not Contemplated in the CPRA.....	6
B.	Proposed Modifications	7
5.	The Agency Should Clarify That the Opt-Out Icon is Optional, Not Mandatory Under the CPRA (Section 7015).....	7
A.	Reasons for Proposed Modifications: The Current Regulations Improperly Mandate Use of the Opt-Out Icon When the CPRA Makes It Optional	7
B.	Proposed Language for Requested Modifications.....	7
6.	CalChamber Requests Minor Modifications to the Service Provider and Contractor Terms to Align With the Statute, and Correct Verbiage and Create Flexibility With Contract Terms (Sections 7050-7053).	7
A.	Reasons for Proposed Modifications: The Current Regulations Impose Additional Requirements Not Contemplated in the CPRA.....	7
B.	Proposed Language for Requested Modifications.....	9
7.	CalChamber Requests that the Agency Modify Section 7011(e) to Give Businesses More Flexibility in Drafting Privacy Policies (Section 7011).....	9
A.	Reasons for Proposed Modifications: Section 7011 Contains Requirements for Privacy Policies that Exceed the Scope of CPRA and are Not Helpful for Consumers	9
B.	Proposed Language for Requested Modifications.....	9
8.	CalChamber Requests the Agency Reconsider Its August 22, 2022 Written Comments Requesting Revisions to the Draft CPRA Regulations.....	9
APPENDIX A		i
APPENDIX B		ii
APPENDIX C		v
APPENDIX D		vii
APPENDIX E		viii
APPENDIX F.....		ix
APPENDIX G		xi

EXECUTIVE SUMMARY

The California Chamber of Commerce (“CalChamber”) respectfully submits these comments to the California Privacy Protection Agency’s (“the Agency”) November 3, 2022, [Notice of Modifications to Text of Proposed Regulations](#) regarding the [modified draft California Privacy Rights Act \(“CPRA”\) regulations](#). For the Comments below, CalChamber attaches Appendices A through G which accept the Agency’s latest text in black font and proposes changes in red font. Additionally, CalChamber appreciates the Agency incorporating some of CalChamber’s prior comments from our [August 22, 2022, comment letter](#). CalChamber, however, requests that the Agency consider the other issues CalChamber raised that were not addressed in the current draft CPRA regulations, which we note in Section 8 of this letter.

In sum, CalChamber requests the following modifications to the proposed draft CPRA regulations, which are described in greater detail below in the Comments section:

1. **CalChamber Requests That the Agency Delay Enforcement and Require Consideration of the Delay in Finalizing the Regulations When Conducting Agency Investigations of Alleged Violations (Section 7301).** Under the CPRA, the statutory mandated date for finalizing the regulations was July 1, 2022, and by statute, enforcement is to begin on July 1, 2023. This provided a one-year compliance window. The CPRA regulations still remain in draft form. Because the Agency has not met the deadline to finalize the regulations, enforcement must be postponed to one year after the CPRA regulations are finalized.
2. **The Agency Should Conform the Purpose Limitation Regulation to a Disclosed Purpose Standard That Is Consistent With the CPRA Statute Rather Than a Factors-Like Analysis That Replaces Consumer Expectations With the Agency’s Own Judgment (Section 7002).** We propose modifications to the new complex multi-prong replacement for the “average consumer” standard to a straightforward standard based on disclosures to consumers and compatibility. As currently written, the Agency’s factors-like test for determining whether a business may collect, use, retain, and/or share a consumer’s personal information deviates from the CPRA statute and replaces consumer expectations with the Agency’s judgment.
3. **The Agency Should Clarify that Consent Is Not Required Under the CPRA, That a Business Should Take Reasonable Efforts to Avoid Dark Patterns, and That Maintaining Procedures to Avoid Dark Patterns Should Be a Factor Considered for Determining Violations (Section 7004).** We propose three changes to Section 7004. First, the Agency should clarify any reference to “consent” in Section 7004 because the CPRA is a notice and opt-out statute, with limited exceptions. Second, we propose modifying Section 7004(c) to closely align with the CPRA’s definition of “dark pattern.” Third, we request that the Agency modify Section 7004 to allow businesses to undertake “reasonable efforts” to avoid dark patterns, and consider such “reasonable efforts” as a factor in the dark patterns analysis.
4. **The Agency Should Modify the Right to Correct to Avoid Requiring Businesses to Disclose Their Authentication and Fraud Prevention Processes, and Apply a “Reasonable Efforts” Standard for Maintaining Personal Information Corrected Within Their Systems (Section 7023).** We propose two changes to Section 7023. First, the Agency should clarify Section 7023(h) to ensure that businesses are

not required to disclose authentication or fraud prevention methodologies, trade secrets, and confidential processes. Second, the Agency should modify Section 7023(k) to avoid holding businesses liable for incorrect data that enters their systems after a right to correct has been honored if reasonable efforts have been utilized.

5. The Agency Should Clarify That the Opt-Out Icon Is Optional, Not Mandatory Under the CPRA (Section 7015). We propose that the Agency render the opt-out icon in Section 7015 optional because it could confuse consumers, may not align with a business' design layout, and is contrary to the CPRA's text.

6. CalChamber Requests Minor Modifications to the Service Provider and Contractor Terms to Align With the Statute, and Correct Verbiage and Create Flexibility With Contract Terms (Sections 7050-7053). We propose five changes to sections 7050 and 7051. First, we propose that the Agency change any references to "collected" to "processed" because the CPRA's definition of "collected" is more limited in scope. Second, we request the Agency revert back to its original draft CPRA language and allow service providers and contractors to use consumer personal information to improve overall internal business functions. As currently written, Section 7053(a)(3) precludes such use. Third, we request that the Agency modify Section 7051(a)(5) to allow service providers and contractors to combine or update personal information if it is necessary to carry out a business purpose. Fourth, we request that the Agency remove the following language in Section 7051(a)(7): "Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months" as a contractual requirement for Section 7051(a) compliance because the CPRA does not mandate such terms in service provider or contractor agreements.

7. CalChamber Requests that the Agency Modify Section 7011(e) to Give Businesses More Flexibility in Drafting Privacy Policies (Section 7011). We propose one modification to Section 7011. As currently written, Section 7011 contains numerous requirements for the content of privacy policies that may confuse consumers. The Agency should give businesses flexibility on how to address these issues, instead of making them mandatory elements. This will allow businesses to draft privacy policies in a manner that is easier for consumers to understand and harmonized for other applicable laws.

8. CalChamber Asks the Agency to Reconsider Its August 22, 2022, Written Comments Requesting Revisions to the Draft CPRA Regulations. We appreciate the opportunity for additional comment on the Agency's changes to the proposed CPRA regulations. In addition, we highlight our prior comments addressing concerns that remain in the current draft of the regulations.

COMMENTS

1. **CalChamber Requests That the Agency Delay Enforcement and Require Consideration of the Delay in Finalizing the Regulations When Conducting Agency Investigations of Alleged Violations (Section 7301).**

A. **Reasons for Proposed Modifications: The CPRA's Operational Hurdles Are Complicated by the Delay in Issuance of Final Regulations**

Under the CPRA, the dates set for finalizing the regulations (July 1, 2022) and start of enforcement (July 1, 2023) provided a one-year compliance window. The CPRA regulations remain not finalized and are not expected to finalize until after the effective date of the statute. We appreciate the difficulties the Agency has faced in meeting the statutory deadline. Nevertheless, evolving regulatory standards that will not finalize until after the effective date unnecessarily and unfairly complicates compliance. The burden is further exacerbated by the unexpected development that the CPRA will apply to employee and B2B data on January 1.

As the Chamber has pointed out in a recent letter to the Agency's Board, past-due regulations like these are problematic and warrant remedies to delay enforcement. Indeed, in a recent and nearly identical case against the California Department of Food and Agriculture and the Attorney General's Office, a California court ruled that a statutory deadline to promulgate regulations is mandatory and issued a declaration delaying enforcement on statutory provisions subject to delayed rulemaking. Based on this and the significant operational hurdles for businesses to comply with new requirements in a compressed time period, the Agency should add a provision delaying enforcement until one year after there are final regulations.

As the finalization of the regulations is critical to businesses' compliance, not only should businesses be given additional time to comply, but investigations and enforcement of alleged violations should be prospective from the date of the finalization of the regulations and not retroactive back to the statute's effective date.

B. **Proposed Language for Requested Modifications**

CalChamber proposed revisions in [Appendix A](#) to require the Agency to consider the delay in finalizing the regulations for investigations of alleged violations.

2. **The Agency Should Conform the Purpose Limitation Regulation to a Disclosed Purpose Standard That Is Consistent With the CPRA Statute Rather Than a Factors-Like Analysis That Replaces Consumer Expectations With the Agency’s Own Judgment (Section 7002).**

A. **Reasons for Proposed Modifications: The Current Regulations Deviate from the CPRA’s Purpose**

CalChamber appreciates the Agency striking the “average consumer” standard from Section 7002. However, Section 7002’s factors-like test for determining whether a business may collect, use, retain, and/or share a consumer’s personal information exceeds the Agency’s authority, and still deviates from the CPRA statute, which permits collecting, using, retaining, and/or sharing personal information so long as the business gives a notice at collection. *See* Cal. Civ. Code § 1798.100(a). We therefore request that this test be struck from Section 7002.

The Agency’s proposed modifications create ambiguity by applying a standard that gives the Agency too much discretion and the ability to substitute its own judgment about what is an appropriate use of consumer’s personal information. While we agree that a consumers’ expectations are important to data collection and use practices, the standard must be tied to disclosures made to the consumer, not the Agency’s opinion. This issue is compounded in the proposed modifications, which are mandating an extensive analysis regarding the purpose of processing that gives unequal weight to factors other than the business’s disclosures to the consumers. For example, even though the CPRA statute allows businesses to use personal information if it provides a notice at collection to the consumer, the Agency’s proposed modifications subvert this standard by making the notice at collection only *one of five factors*, which is not what was envisioned when Californians voted the CPRA into law. Moreover, the Agency adds to the confusion by establishing separate multi-prong standards for assessing whether a disclosed purpose is compatible with the context in which the personal information was collected, and whether the collection, use, retention and sharing of personal information is reasonably necessary and proportionate.

The Agency’s focus on various factors, other than a business’s disclosures and compatibility for further processing, risks transforming California’s statutory standard of implied consent (based on notice) to an opt-in standard. The new proposed modifications only amplify this risk and still have no basis in law. To properly assess whether a business’s use is permissible under the CPRA, the regulations should focus on compatible uses and adopt the statutory, and widely accepted, standard that looks at the notice provided to the consumer and whether the use is compatible with that notice. If a use is incompatible with a disclosed purpose, then the business cannot use the personal information without providing an additional notice at collection. This appropriately focuses on the context at the time of collection, which is the statutory standard under the CPRA. It also aligns with other privacy frameworks. *See* [August 22, 2022 CalChamber Comment Letter](#), at p. 7.

Alternatively, if the Agency maintains the factors-like test, CalChamber requests modifications to refocus the analysis to assess compatibility (with the reasonable expectations of the consumer as one factor to balance). This would provide appropriate weight to disclosures, align with the CPRA statutory standard, and also ensure better interoperability with other global frameworks and the developing regulations in Colorado. As set forth in Appendix B, this can be achieved by requiring consistency with the notice at the

time of disclosure, limiting further processing to compatible uses as balanced by the reasonable expectations of the consumer, other factors currently in Section 7002(d)(2)-(3), and modifications to current Section 7002(b)(3)-(5).

Additionally, some modifications to current Section 7002(b)(3)-(5) are warranted as follows:

1. First, for Section 7002(b)(3), the Agency should remove the “unexpected” use limitation language from the consumers’ expected use of their personal information by the business. How a business uses a consumer’s personal information across its products and services should not be unduly limited where the privacy notice expressly discloses those potential uses and that the use might occur across products or services. This is because the consumer obtains substantial benefit from sharing data across products and services, such as using data from a reading app to personalize book recommendations in an online store (when the same business offers both services). To the extent the Agency retains this factor, it should focus on whether the use of different products or services is “unexpected” and “unrelated.”
2. Finally, CalChamber requests that the Agency strike Section 7002(b)(5), which considers “the involvement of service providers, contractors, third parties, or other entities” when deciding whether the business’s disclosure of the consumer’s personal information was appropriate. This factor runs counter to the CPRA and the draft CPRA regulations themselves, which permit a business to disclose the consumers’ personal information to service providers, contractors and third parties if the business enters into an appropriate contract. *See* Cal. Civ. Code §§ 1798.100(d), 1798.140(j)&(ag); Draft CPRA Regulations Sections 7051 and 7053.

B. Proposed Language for the Requested Modifications

We have offered (1) a preferred and (2) an alternative proposal for modification of Section 7002 in [Appendix B](#).

3. **The Agency Should Clarify That Consent Is Not Required Under the CPRA, That a Business Should Take Reasonable Efforts to Avoid Dark Patterns, and That Maintaining Procedures to Avoid Dark Patterns Should Be a Factor Considered for Assessing Violations (Section 7004).**

A. Reasons for Proposed Modifications: The Current Regulations Should Delete Requirements for Consent and Clarify the Definition of Dark Patterns

CalChamber requests that the Agency clarify in Section 7004 that the references to “consent” refer to the limited instances in which the statute mandates consent because the CPRA is largely a notice at collection statute (not opt-in), and therefore does not require consent for the collection and processing of personal information in most instances. The Agency’s overbroad reference to requirements for consent throughout Section 7004 of the draft CPRA regulations only adds confusion to this clear statutory standard. For example, in Section 7004(a)(4)(B), the Agency’s insertion of “because consent must be freely given, specific, informed, and unambiguous” appears to mandate opt-in consent under the CPRA, when that is not

required under the statute for personal information collection, except in instances of selling/sharing children's personal information, or opting back into sale/sharing for adults, both of which are separately addressed under the CPRA. *See* Cal. Civ. Code §§ 1798.120 & 1798.135.

In addition, CalChamber requests that the Agency modify Section 7004(c) to closely align with the definition of “dark pattern” in the CPRA, which requires a “substantial effect of subverting or impairing user autonomy, decision making or choice” before a user interface is considered a dark pattern. *See* Cal. Civ. Code § 1798.140(l). We also request inclusion of the word “may” under Section 7004(a) to clarify that the factors listed are not on their own determinative if there is a dark pattern, but rather, issues a business should consider when designing a user interface.

Further, CalChamber requests a modification to Section 7004(a) and (c) to reflect that a business should make “reasonable efforts” to avoid dark patterns, and that such reasonable efforts are a factor in deciding whether there was a dark pattern. Whether a practice constitutes a dark pattern is not an exact science. Instead, it requires a business to consider its own user interface and analyze what reasonable steps it should take to avoid dark pattern choices. If a business has methodically considered and documented its dark pattern analysis, the Agency should consider this as a factor in the analysis.

Lastly, CalChamber requests modifications to Section 7004(a)(2) clarifying that lack of symmetry is a dark pattern only when it results in impairing or interfering with the ability to make a choice. The textual revisions we propose clarify this point, which we understand may have been the Agency's intent in the last revisions. *See* [Explanation of Modified Text of Proposed Regulations](#) at p. 4.

B. Proposed Language for Requested Modifications

CalChamber has included in [Appendix C](#) specific proposed language for the requested modification of Section 7004 to come within the ambit of the CPRA.

4. **The Agency Should Modify the Right to Correct to Avoid Requiring Businesses to Disclose Their Authentication and Fraud Prevention Processes, and Apply a “Reasonable Efforts” Standard for Maintaining Personal Information Corrected Within Their Systems (Section 7023).**

A. Reasons for Proposed Modifications: Current Regulations Create Additional Risks for Businesses that Were Not Contemplated in the CPRA

CalChamber requests the Agency to make minor modifications to Section 7023(h) to ensure that the draft CPRA regulations would not require a business to disclose its authentication or fraud prevention mechanisms, trade secrets, and confidential processes. As currently written, Section 7023(h) is ambiguous as to the level of detail a business must share with the consumer, only requiring a business to disclose “why [it] believes the request is fraudulent or abusive.” CalChamber requests the modification outlined in Appendix C to avoid having businesses disclose closely-held secrets related to how they guard against bad actors attempting to compromise their systems. This modification is both beneficial for consumers so that they are not subject to identity theft, and for businesses so that they can protect their systems.

Next, CalChamber requests a minor modification to Section 7023(k) so that businesses are not automatically held in violation of the CPRA if incorrect data enters their systems and inadvertently renders corrected information back to an incorrect state. To avoid such a strict-liability approach, CalChamber proposes adding a “reasonable efforts” standard for businesses. This will ensure that businesses have reasonable procedures in place to avoid inadvertent error, while also avoiding imposing liability when issues related to correct and incorrect data are sometimes subjective and subject to change when new data sets enter the business’s systems.

B. Proposed Modifications

CalChamber proposes in [Appendix D](#) specific proposed language for the requested modifications to Section 7023.

5. **The Agency Should Clarify That the Opt-Out Icon is Optional, Not Mandatory Under the CPRA (Section 7015).**

A. Reasons for Proposed Modifications: The Current Regulations Improperly Mandate Use of the Opt-Out Icon When the CPRA Makes It Optional

CalChamber requests that the Agency modify Section 7015(b) to make the use of the opt-out icon optional because it is not mandated under Cal. Civ. Code § 1798.135(a)(3). In addition to being contrary to the CPRA’s text, this icon could confuse consumers because the static image looks like a toggle that a consumer can activate. Lastly, Section 7015(b) also prescribes graphic features that may not align with a business’s design layout, putting unnecessary burden on a business without countervailing consumer benefit.

B. Proposed Language for Requested Modifications

CalChamber proposes in [Appendix E](#) specific language for the requested modification to Section 7015(b).

6. **CalChamber Requests Minor Modifications to the Service Provider and Contractor Terms to Align With the Statute, and Correct Verbiage and Create Flexibility With Contract Terms (Sections 7050-7053).**

A. Reasons for Proposed Modifications: The Current Regulations Impose Additional Requirements Not Contemplated in the CPRA

The CalChamber requests five change to Sections 7050-7053 as follows:

1. First, CalChamber requests that the Agency change references to “Collected” to “processed,” which is a broader and more universally-accepted data privacy term that refers to all personal information handling practices. Further, since the current definition of “Collected” under the CPRA statute is more limited in scope, the broader term of “processed” would capture all potential data handling circumstances.

2. Second, CalChamber requests the Agency revert Section 7050(a)(3) back to its original draft CPRA language, and delete current restrictions on using personal information to only build or improve the quality of the services to a business and limits on such improvements when performing services for other businesses. Service providers and contractors often contract with multiple businesses, and any personal information collected from all of these businesses is then used to improve the service provider and contractor's overall internal functions; these same internal functions are then used to service other businesses. To the extent the Agency has concerns that a service provider or contractor will use personal information from one business to service another business, the remaining provisions in Section 7050(a)(3) already preclude them from doing so.
3. Third, CalChamber requests that the Agency modify Section 7051(a)(5) to allow service providers and contractors to combine or update personal information if it is necessary to carry out a business purpose. There may be instances where service providers and contractors will need to combine or update the personal information of multiple businesses for the business purpose of servicing businesses, such as for fraud prevention. By including this provision, the Agency creates a conflict with Section 7050(a)(4), which allows service providers and contractors to retain, use or disclose personal information to prevent, detect or investigate security incidents or protect against fraud and other activities.
4. Fourth, CalChamber requests that the Agency remove from Section 7051(a)(7) "reasonable and appropriate steps include . . . ongoing manual reviews and automated scans of the service provider's system and regular internal or third-party assessments, audits, or other technical and operational" as a required contractual term because the CPRA does not require such language in service provider and contractor contracts. Instead, the statute states that the parties may include it if they desire to do so. *See* Cal. Civ. Code § 1798.140(ag)(1)(D) ("The contract *may, subject to agreement with the service provider*, permit the business to monitor the service provider's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.") (emphasis added). Because this term is optional, it is not appropriate to list it as a required term under Section 7051, which provides the terms that "shall" be in the service provider and contractor contracts. *See* Draft CPRA Regulation Section 7051(a).
5. Fifth, CalChamber requests that the Agency provide greater flexibility with the contract requirements under Sections 7051 and 7053 so that all of these terms are not mandatory. Instead, the Agency should permit material compliance with these terms because businesses may have already entered into data protection agreements with their services providers, contractors and third parties to address other data privacy laws and general protection requirements, which materially contain similar terms. Thus, CalChamber requests the beginning of Sections 7051 and 7053 to state that the contracts required between service providers, contractors, and third parties should "materially" contain the terms listed.

B. Proposed Language for Requested Modifications

CalChamber proposes in [Appendix F](#) edits to Sections 7501-7503 to address these issues.

7. **CalChamber Requests that the Agency Modify Section 7011(e) to Give Businesses More Flexibility in Drafting Privacy Policies (Section 7011).**

A. Reasons for Proposed Modifications: Section 7011 Contains Requirements for Privacy Policies that Exceed the Scope of CPRA and are Not Helpful for Consumers

As proposed, Section 7011 requires a significant amount of details and content for privacy policies that are not helpful to consumers. A privacy policy should fundamentally address what personal information a business collects, why a business collects it, who the business shares it with, along with a description of the consumer rights under the applicable privacy law. Indeed, even the GDPR (arguably the most stringent privacy law) requires far less detail and content under Article 13 than the draft CPRA regulations. Ultimately, all of this information will confuse consumers rather than help them understand a business's personal-information handling practices. To address this issue, we recommend modifying Section 7011 to only require businesses to materially address the requirements listed, and have flexibility to harmonize their privacy policy to address not only the CPRA, but also other applicable laws.

B. Proposed Language for Requested Modifications

CalChamber proposes in [Appendix G](#) edits to Section 7011(e) to address these issues.

8. **CalChamber Requests the Agency Reconsider Its August 22, 2022 Written Comments Requesting Revisions to the Draft CPRA Regulations.**

On [August 22, 2022, CalChamber submitted written comments](#) requesting modifications to the draft CPRA regulations. While we appreciate some of the modifications made, the majority of the issues we identified in our August 22, 2022, comment letter remain unresolved. Among other things, CalChamber identified a number of instances where the Agency exceeded its authority by proposing regulations that contradict or go beyond the scope of the CPRA statute. For example, where the draft regulations would deem an otherwise *optional* opt-out preference signal, *mandatory*. We strongly urge the Agency to revisit such provisions. Below is a list of the issues the Agency failed to address in the recent draft CPRA regulations and a citation to the pages in the August 22, 2022 CalChamber Comments, which can be found [here](#).

- **Opt-Outs and Preference Signals:** CalChamber provided extensive comments related to a number of provisions covering opt-out preference signals, which the Agency did not address in the latest version of the draft CPRA regulations. We request reconsideration of these issues and for the Agency to provide greater clarity regarding which specific signals are considered valid under the CPRA. See [August 22, 2022 Comments](#) at pp. 8-18.
- **Section 7004:** The Agency should not require a binary option for symmetry of choice. See [id.](#) at p. 22.

- **Section 7012:** The Agency should reconsider CalChamber's request to strike Section 7012(f). *See [id.](#)* at p. 27.
- **Section 7022:** The Agency should reconsider CalChamber's arguments regarding the right to delete to make the standard more reasonable. *See [id.](#)* at pp. 38-40.
- **Section 7023:** The Agency should reconsider CalChamber's arguments regarding the right to correct in order to make the standard more reasonable. *See [id.](#)* at pp. 40-43.
- **Section 7027:** The Agency should reconsider CalChamber's arguments regarding sensitive personal information, but also consider modifying Section 7027(j) to permit a business to deny an authorized agent request if there is reasonable suspicion of fraud. *See [id.](#)* at pp. 45-46.
- **Section 7050(e):** The Agency should reconsider CalChamber's arguments regarding the impact of not having a service provider/contractor contract, which was previously under Section 7051(c). *See [id.](#)* at pp. 34-35.
- **Sections 7051 and 7053:** The Agency should reconsider unaddressed comments by CalChamber regarding service provider, contractor and third-party contracts. *See [id.](#)* at pp. 29-35.
- **Section 7302:** The Agency should reconsider CalChamber's proposed revisions to modify the probable cause proceedings procedures. *See [id.](#)* at pp. 46-49.
- **Section 7304:** The Agency should reconsider CalChamber's proposed revisions to apply reasonable limits to audits. *See [id.](#)* at pp. 28-29.



Dominique Shelton Leipzig,
Partner, Cybersecurity & Data Privacy
Leader, Global Data Innovation and Ad Tech Privacy & Data Management practices
Mayer Brown

cc: Arsen Kourinian, Partner
 Sasha L. Keck, Associate
 Megan Von Borstel, Associate
 Britteny Leyva, Associate

APPENDICES

Appendix A

Proposed Revision to Section 7301(b)

(b) The Agency shall not pursue investigations of possible or alleged violations of the CCPA until one year following such time that the applicable rule which is the subject of the investigation has gone into effect, and any such investigation shall only relate to activity as of such one-year anniversary. Following such time period, ~~A~~ as part of the Agency's decision to pursue investigations of possible or alleged violations of the CCPA, the Agency ~~may~~ shall consider all relevant facts ~~it determines to be relevant~~, including the amount of time between the effective date of the statutory or regulatory requirement(s) and the possible or alleged violation(s) of those requirements, and good faith efforts to comply with those requirements.

Appendix B

Proposed Modifications to Section 7002

Preferred Modification Proposal

Section 7002(a)(1) and (2) should be deleted and replaced in its entirety with the below:

- (1) The purpose(s) for which the personal information was collected or processed, ~~which shall comply with the requirements set forth in subsection (b).~~
- (2) Another ~~disclosed~~ purpose that is compatible with a disclosed purpose, ~~the context in which the personal information was collected, which shall comply with the requirements set forth in subsection (c).~~

Section 7002(b) should be deleted and replaced in its entirety with the below:

- (b) The purpose(s) for which the personal information was collected or processed shall be consistent with the business's Notice at Collection.

Section 7002(c) and (d) should be deleted and replaced in its entirety with the below:

- (c) Whether another disclosed purpose is compatible with the context in which the personal information was collected shall be based on how clear the Notice at Collection was regarding the intended purpose of processing or whether the business gave a just-in-time supplemental notice to the consumer regarding the other disclosed purpose. For example, if an ecommerce business disclosed to the consumer in its Notice at Collection that it plans on using the consumer's personal information to deliver the goods they purchased and for marketing, it may use the personal information for marketing purposes if the Notice at Collection was clear about these intended uses or if the business provided a just-in-time notice to the consumers that their personal information will be used to not only ship the goods they purchased, but also for marketing.

Alternative Modification Proposal

Section 7002(a)(1) and (2) should be deleted and replaced in its entirety with the below:

- (1) The purpose(s) for which the personal information was collected or processed, ~~which shall comply with the requirements set forth in subsection (b).~~
- (2) Another ~~disclosed~~ purpose that is compatible with a disclosed purpose, ~~the context in which the personal information was collected, which shall comply with the requirements set forth in subsection (c).~~

Section 7002(b) and (c) should be deleted and replaced in its entirety with the below:

(b) Whether another ~~disclosed~~ purpose is compatible with a disclosed purpose the context in which the personal information was collected shall be based on the following factors:

Section 7002(b)(1)-(5) should be modified to the following:

(1) the consumer's reasonable expectations concerning how their personal information would be processed once collected.

~~(+)~~ (2) The relationship between the consumer and the business. For example, if the consumer is intentionally interacting with the business on its website to purchase a good or service, the consumer likely expects that the purpose for collecting or processing the personal information is to provide that good or service. By contrast, for example, the consumer of a business's mobile flashlight application would not expect the business to collect the consumer's geolocation information to provide the flashlight service.

~~(2)~~ (3) The type, nature, and amount of personal information that the business seeks to collect or process. For example, if a business's mobile communication application requests access to the consumer's contact list in order to call a specific individual, the consumer likely expects that the purpose of the business's use of their contact list will be to connect the consumer with the specific contact they selected. Similarly, if a business collects the consumer's fingerprint in connection with setting up the security feature of unlocking the device using the fingerprint, the consumer likely expects that the business's use of the consumer's fingerprint is for the purpose of unlocking their mobile device.

~~(3)~~ (4) The source of the personal information and the business's method for collecting or processing it. For example, if the consumer is providing their personal information directly to the business while using the business's product or service, the consumer likely expects that the business will use the personal information to provide that product or service. However, the consumer may not expect that the business will use that same personal information for an unexpected and unrelated use on a different product or service offered by the business or the business's subsidiary.

~~(4)~~ (5) The specificity, explicitness, prominence, and clarity of disclosures to the consumer(s) about the purpose for collecting or processing their personal information, such as in the Notice at Collection and in the marketing materials to the consumer(s) about the business's good or service. For example, the consumer that receives a pop-up notice that the business wants to collect the consumer's phone number to verify their identity when they log in likely expects that the business will use their phone number for the purpose of verifying the consumer's identity and not for marketing purposes. Similarly, the consumer may expect that a mobile application that markets itself as a service that finds cheap gas close to the consumer will collect and use the consumer's geolocation information for that specific purpose when they are using the service.

~~(5) The degree to which the involvement of service providers, contractors, third parties, or other entities in the collecting or processing of personal information is apparent to the consumer(s). For example, the consumer likely expects an online retailer's disclosure of the consumer's name and address to a delivery service provider in order for that service provider to deliver a purchased product, because that service provider's involvement is apparent to the consumer. By contrast, the consumer may not expect the disclosure of personal information to a service provider if the consumer is not directly interacting with the service provider or the service provider's role in the processing is not apparent to the consumer.~~

(6) The possible negative impacts on consumers posed by the business's collection or processing of the personal information. For example, a possible negative impact of collecting precise geolocation information is that it may reveal other sensitive personal information about the consumer, such as health information based on visits to healthcare providers.

(7) The existence of additional safeguards for the personal information to specifically address the possible negative impacts on consumers considered by the business in subsection (d)(2). For example, a business may consider encryption or automatic deletion of personal information within a specific window of time as potential safeguards.

...

~~(d) For each purpose identified in subsection (a)(1) or (a)(2), the collection, use, retention, and/or sharing of a consumer's personal information to achieve that purpose shall be reasonably necessary and proportionate. Whether a business's collection, use, retention, and/or sharing of a consumer's personal information is reasonably necessary and proportionate to achieve the purpose identified in subsection (a)(1) or (a)(2) shall be based on the following factors:~~

~~(1) The minimum personal information that is necessary to achieve the purpose identified in subsection (a)(1) or (a)(2). For example, to complete an online purchase and send an email confirmation of the purchase to the consumer, an online retailer may need the consumer's order information, payment and shipping information and email address.~~

~~(2) The possible negative impacts on consumers posed by the business's collection or processing of the personal information. For example, a possible negative impact of collecting precise geolocation information is that it may reveal other sensitive personal information about a consumer, such as health information based on visits to healthcare providers.~~

~~(3) The existence of additional safeguards for the personal information to specifically address the possible negative impacts on consumers considered by the business in subsection (d)(2). For example, a business may consider encryption or automatic deletion of personal information within a specific window of time as potential safeguards.~~

Appendix C

Proposed Modifications to Section 7004

§ 7004. Requirements for Methods for Submitting CCPA Requests Offering Consumer Choices.
~~and Obtaining Consumer Consent.~~

(a) Except as expressly allowed by the CCPA and these regulations, businesses shall make reasonable efforts to design and implement methods for submitting CCPA requests and offering consumer choices ~~obtaining consumer consent~~ that may incorporate the following principles. References to “consent” refer to when the statute requires explicit consent for data collection and use.

...

(2) Symmetry in choice. The path for a consumer to exercise a more privacy-protective option shall not be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option because to the extent it that would ~~impair~~ or ~~interfere~~ with the consumer’s ability to make a choice.

...

(4) Avoid choice architecture that impairs or interferes with the consumer’s ability to make a choice. Businesses should also not design their methods in a manner that would impair the consumer’s ability to exercise their choice ~~because consent must be freely given, specific, informed, and unambiguous.~~

...

~~(B) Bundling choices so that the consumer is only offered the option to consent to using personal information for purposes that meet the requirements set forth in section 7002, subsection (a), together with purposes that are incompatible with the context in which the personal information was collected is a choice architecture that impairs or interferes with the consumer’s ability to make a choice. For example, a business that provides a location based service, such as a mobile application that posts gas prices within the consumer’s location, shall not require the consumer to consent to incompatible uses (e.g., sale of the consumer’s geolocation to data brokers) together with a reasonably necessary and proportionate use of geolocation information for providing the location based services, which does not require consent. This type of choice architecture does not allow consent to be freely given, specific, informed, or unambiguous because it requires the consumer to consent to incompatible uses in order to obtain the expected service. The business should provide the consumer a separate option to consent to the business’s use of personal information that does not meet the requirements set forth in section 7002, subsection (a).~~

...

(c) A user interface is a dark pattern if it is designed in a manipulative manner with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice. A business's intent in designing the interface is not determinative in whether the user interface is a dark pattern, but a factor to be considered. If a business can show that it had a process for reviewing user interfaces for dark patterns, this may weigh against establishing a dark pattern. If a business did not intend to design the user interface to subvert or impair user choice, but the business knows of and does not remedy a user interface that has that effect, the user interface may still be a dark pattern. Similarly, a business's deliberate ignorance of the effect of its user interface may also weigh in favor of establishing a dark pattern.

Appendix D

Proposed Modifications to Section 7023

(h) A business may deny a request to correct if it has a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. The business shall inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent or abusive provided, however, that the business shall not be required to provide any information to the requestor, the disclosure of which could potentially reveal how to subvert the business's authentication, fraud prevention, or other processes designed to ensure that personal information is not improperly corrected.

. . .

(k) Whether a business, service provider, or contractor has implemented measures to ensure that personal information that is the subject of a request to correct remains corrected factors into whether that business, service provider, or contractor has complied with a consumer's request to correct in accordance with the CCPA and these regulations. For example, a business, service provider, or contractor may supplement personal information it maintains about consumers with information obtained from a data broker. Failing to consider and use reasonable efforts to address the possibility that corrected information may be overridden by inaccurate information subsequently received from a data broker may factor into whether that business, service provider, or contractor has adequately complied with a consumer's request to correct.

Appendix E

Proposed Modification to 7015(b)

(b) A business that chooses to use an Alternative Opt-out Link shall title the link, “Your Privacy Choices” or “Your California Privacy Choices,” and ~~shall~~ may include the following opt-out icon adjacent to the title. The link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business’s internet Homepage(s). The icon shall be approximately the same size as other icons used by the business in the header or footer of its webpage.

Appendix F

Proposed Modifications to Sections 7050 and 7051

For Sections 7050 to 7051, CalChamber requests all references to “Collected” to be changed to “process.”

Section 7050(a)(3):

(3) For internal use by the service provider or contractor to build or improve the quality of the services ~~it is providing to the business~~, even if this Business Purpose is not specified in the written contract required by the CCPA and these regulations.

...

Section 7051(a)(5):

(5) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it ~~Collected~~ processed pursuant to the written contract with the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or updating personal information that it ~~Collected~~ processed pursuant to the written contract with the business with personal information that it received from another source or ~~Collected~~ processed from its own interaction with the consumer, unless doing so is required to fulfill a Business Purpose or expressly permitted by the CCPA or these regulations.

...

Section 7051(a)(7):

(7) Grant the business the right to take reasonable and appropriate steps to ensure that service provider or contractor uses the personal information that it ~~Collected~~ processed pursuant to the written contract with the business in a manner consistent with the business’s obligations under the CCPA and these regulations. ~~Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider’s system and regular internal or third party assessments, audits, or other technical and operational testing at least once every 12 months.~~

Proposed Modifications to Sections 7051 and 7053

Section 7051(a) should be deleted and replaced in its entirety with the below:

(a) The contract required by the CCPA for service providers and contractors shall materially contain the following requirements:

...

Section 7053(a) should be deleted and replaced in its entirety with the below:

(a) A business that sells or shares a consumer's personal information with a third party shall enter into an agreement with the third party that materially contains the following requirements:

Appendix G

Proposed Modifications to Section 7011(e)

Subsections (e)(1)-(5) to follow unmodified.

(e) Businesses may modify the below requirements to make the privacy policy easy to understand and conform to other applicable privacy policy requirements that the business may be subject to.

The privacy policy may ~~shall~~ include the following information:

From: Ritter, Denneile <[REDACTED]>
Sent: Friday, November 18, 2022 6:01 PM
To: Regulations
Subject: CCPA Public Comment
Attachments: CCPA Modified Draft Regulations_APCIA Second Comment Letter_Final 11182022.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Mr. Soublet,

On behalf of the American Property Casualty Insurance Association, attached please find our comments for the Agency's modified draft regulations. We look forward to engaging with you and your staff as you work to implement the CPRA.

Best,
Denni

Denneile Ritter
American Property Casualty Insurance Association
Vice President State Government Relations, Western Region
1415 L Street, Suite 670, Sacramento, CA 95814
P: [REDACTED] | [REDACTED]





November 18, 2022

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

Re: Response to Request for Comments – Modifications to the California Consumer Privacy Act Draft Regulations

On behalf of the American Property Casualty Insurance Association (“APCIA”),¹ thank you for the opportunity to provide additional comment on the modifications to the California Consumer Privacy Act (“CCPA”) proposed draft regulations (the “Modified Draft Regulations”).² In our initial comments,³ APCIA sought to provide the insurance industry’s unique perspective on several key issues raised by the California Privacy Protection Agency’s (the “Agency’s”) proposed amendments to the CCPA regulations, as prescribed by the California Privacy Rights Act (“CPRA”). We greatly appreciate the continued efforts by the Agency to incorporate all the comments received as you finalize the amendments, and we reiterate and incorporate by reference APCIA’s initial comments. With the CPRA’s January 1, 2023 effective date fast-approaching, however, and given the increasing likelihood that the Agency will not address the insurance industry portion of the required changes (often referred to as “Topic #21”)⁴ before the effective date, we believe that it is critical for the Agency to provide clear guidance on how the CCPA and its regulations will apply to the insurance industry until such time as the Agency fully addresses Topic #21 and related issues. Specifically, the Agency should clarify that, until such time as it expressly addresses these issues, compliance with existing privacy laws is sufficient for compliance with CCPA.

As you know, CPRA directed the Agency in Topic #21 to review insurance laws that relate to consumer privacy, and adopt regulations for the insurance industry to the extent existing law does not provide greater protection to consumers.⁵ Providing insurance products and services involves collecting, processing, and securing consumer’s financial and other personal information and the insurance industry’s use of this information is already heavily regulated, in many cases in ways that provide consumers even greater protections than those established in CCPA.⁶ Since 1981, businesses in the insurance sector have been subject to a number of specific privacy requirements, in particular various provisions of the California Insurance Code and regulations (collectively referred to herein as “Insurance

¹ The American Property Casualty Insurance Association (APCIA) is the primary national trade association for home, auto, and business insurers. APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers, with a legacy dating back 150 years. APCIA members represent all sizes, structures, and regions—protecting families, communities, and businesses in the U.S. and across the globe.

² Notice of Modifications to Text of Proposed Regulations and Addition of Documents and Information to Rulemaking File, Nov. 3, 2022, available at https://coppa.ca.gov/regulations/pdf/20221102_15_day_notice.pdf (“Modified Proposal”).

³ See https://coppa.ca.gov/regulations/pdf/comments_51_75.pdf#page=204 for APCIA’s previous comments submitted to the Agency (“APCIA Comments”).

⁴ Cal. Civ. Code §1798.185(a)(21).

⁵ *Id.*

⁶ For a detailed comparison of relevant rights and obligations, see APCIA Comments at 4.

Laws”), under which the insurance industry has been providing robust privacy protections to California consumers. For example, the Insurance Laws require insurers to provide a detailed notice and a number of consumer rights that are similar to the CCPA’s requirements and that provide greater privacy protections than the relevant federal laws, such as the Gramm-Leach-Bliley-Act (“GLBA”) and its implementing regulations. Businesses in the insurance industry in California must maintain a robust compliance program to comply with the Insurance Laws and are subject to periodic audit and investigation by the state insurance commissioner. Additionally, the California Department of Insurance (“CDI”) also submitted comments highlighting the existing California Insurance Information and Privacy Protection Act (“IIPPA”) and the Privacy of Nonpublic Information regulations (“PNPI”), as well as efforts by the National Association of Insurance Commissioners (the “NAIC”).⁷ The NAIC Privacy Protections Working Group has recently requested adoption of a new model law that would replace the NAIC Insurance Information and Privacy Protection Model Act (#670) and the NAIC Privacy of Consumer Financial and Health Information Regulation (#672), upon which IIPPA and PNPI are based.⁸ A new NAIC model law addressing consumer protection and the corresponding obligations of entities licensed by the insurance department will affect IIPPA and PNPI when adopted in California.

Concurrently, the CCPA explicitly exempts from most of its requirements information that is subject to the GLBA and its implementing regulations and the California Financial Information Privacy Act (“FIPA”).⁹ The interplay of this exemption and Topic #21 raises important questions about the extent to which operators in the insurance industry are regulated by CCPA, especially if all the consumer financial data they collect is already subject to GLBA and FIPA (and, therefore, not subject to CCPA or the regulations adopted thereunder).

Finally, one of the core functions of the Agency is cooperating with other state agencies with jurisdiction over related privacy laws to ensure consistent application of privacy protections.¹⁰ As requested by the CDI in its letter responding to the Agency’s request for comments on the proposed CCPA revised regulations, the Agency should closely coordinate with the CDI prior to enacting any regulations applicable to the insurance industry.

We appreciate that the Agency is already considering ways to address issues raised by the timing of the effective date and the adopting of new rules. Specifically, the new language in § 7301(b) of the Modified Draft Regulations explains that the Agency may consider “timing” when deciding to undertake an investigation or enforcement action.¹¹ But this new language does not address or alleviate the concerns explained above. Without even limited guidance from the Agency on Topic #21 and related issues, APCIA’s members must attempt to answer consequential questions and make considerable investment and compliance decisions in the face of significant uncertainty, *with no discernible benefit to consumers*.

The best path forward for the Agency is to make explicit that, as to operators in the insurance industry, compliance with the privacy provisions in existing Insurance Laws is sufficient for compliance with CCPA and its implementing regulations, until such time as the Agency addresses Topic #21 and related issues. This approach protects consumers by reaffirming the importance of the privacy provisions in existing laws that apply to the insurance industry, and promotes certainty for both consumers and operators by providing concrete guidance with respect to what is expected of operators.

⁷ See Preliminary Rulemaking Written Comments – Part 3, https://cppa.ca.gov/regulations/pdf/preliminary_rulemaking_comments_3.pdf.

⁸ See https://content.naic.org/sites/default/files/inline-files/Attmt%203_MLR_670and672-Request.pdf for the NAIC Privacy Working Group’s request for NAIC Model Law Development.

⁹ Cal. Civ. Code § 1798.145(e).

¹⁰ Cal. Civ. Code § 1798.199.40.

¹¹ Modified Proposal, § 7301(b).

Thank you for the opportunity to provide comments on this important issue. The insurance industry has a long history of protecting Californians' personal information and privacy. We look forward to the Agency's guidance in implementing and operationalizing the CCPA regulations in an effective manner.

From: Nick Chiappe [REDACTED]
Sent: Friday, November 18, 2022 7:12 PM
To: Regulations
Cc: Chris Shimoda
Subject: CCPA Public Comment
Attachments: Comments to Modified Proposed CCPA Regulations_Final.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good evening,

Please find the California Trucking Association's written comments on the proposed modifications of the CPRA.

Thank you,
Nick Chiappe



Nick Chiappe | Government Affairs Associate
California Trucking Association
4148 East Commerce Way
Sacramento, CA 95834
C: [REDACTED] | E: [REDACTED]
W: www.caltrux.org



A one-stop-shop for all things testing? Your search is over.

Visit www.TSCtesting.com or email Karina Fernandez at [REDACTED] to learn more.





November 18, 2022

Via Email to regulations@coppa.ca.gov

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

Re: CPPA Public Comment

Dear Mr. Soublet:

The California Trucking Association appreciates the opportunity to submit comments to the California Privacy Protection Agency (“CPPA”) as part of the CPPA’s rulemaking process under the California Consumer Privacy Act (“CCPA”). The CTA promotes leadership in the California trucking industry, advocates sound transportation policies to all levels of government, and works to maintain a safe, environmentally-responsible and efficient California transportation goods movement system.

We have reviewed the modifications that the CPPA has proposed to the regulations proposed pursuant to the CCPA (the “Modified Proposed Regulations”) and we appreciate the consideration that the CPPA has given to our comments to the original draft regulations published on July 8, 2022. But we respectfully submit that the Modified Proposed Regulations should be clarified further to recognize the status of package transportation providers as “businesses” given that carriers, and not their retailer customers, determine the purposes and means of the processing of package-related information and addressing details.

As we explained in our comments to the original draft regulations, the package transportation industry is unique in that a significant portion of the personal information processed in core, day-to-day operations is received not directly from consumers, but instead from retailers and other corporate customers. This information takes the form of addressing details and package-related information, such as package dimensions and weight (collectively, “Shipping Information”).

Amending Section 7002 (b)(5)

“The degree to which the involvement of service providers, contractors, third parties, or other entities in the collection or processing of personal information is apparent to the consumer. For example, the consumer likely expects an online retailer’s disclosure of the consumer’s name and address to a delivery ~~business service provider~~ in order for that ~~business service provider~~ to deliver a purchased product, because that ~~business’s service provider’s~~ involvement is apparent to the consumer. By contrast, the consumer may not expect the disclosure of personal information to a ~~business service provider~~ if the consumer is not directly interacting with the ~~business service provider~~ or the ~~business’s service provider’s~~ role in the processing is not apparent to the consumer.”

When a consumer buys a product online, the online merchant provides a package to a carrier along with associated Shipping Information. Transportation providers use this information to fulfill the requested service of delivering the product, but they also process this data inherently for purposes

and via means that they, and not the online merchant, determine. This is why transportation providers are considered “controllers” under the EU General Data Protection Regulation (“GDPR”) and UK GDPR, and why they should be deemed “businesses,” not service providers, under the CCPA. Further, this sharing of Shipping Information with transportation providers should be deemed not to constitute a “sale” of personal information because the sharing is performed at the direction of the consumer who has instructed the retailer to ship the goods to the consumer’s designated address.

Amending Section 7050(a)(3)(B):

“A shipping service provider that delivers businesses’ products to their customers may use *and retain* the addresses obtained from their business clients and *its* experience delivering to those addresses *for legitimate business purposes permitted under applicable laws, including to comply with laws*, to identify faulty or incomplete addresses, ~~and thus~~, or *to* improve their delivery services. However, the shipping service provider cannot compile the addresses received from one business to send advertisements on behalf of another business, or compile addresses received from businesses to sell to data brokers.”

Why A “Service Provider” Designation is Problematic for Transportation/Shipping Companies

A “service provider” designation will create operational issues for shipping companies and the package transportation industry. Retailers and corporate customers continue to insist that carriers and shipping companies are their “service providers” under the CCPA and subject to their controls, which precludes shipping companies from using shipping data for legitimate business purposes. Allowing shipping companies to be designated as a “business” will ensure the free flow of goods, while still protecting the privacy rights of consumers.

Contents of the Package:

Shipping companies do not act as a “data controller/business” or a “data processor/service provider” with regard to information that may be contained in the packages they transport. That rationale is straightforward: shipping companies have no control over the contents, nor do they know whether personal data is contained within. These shipping companies merely act as a conduit of that personal data, without exercising any actual control over it. For a more detailed discussion of mail delivery services and their status, you may refer to the guidance from the Dutch regulator at <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/verantwoordingsplicht> and UK Data Protection Regulator (ICO), at <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf> (¶¶ 33-39).

Shipping Label Data:

Shipping companies act as a “data controller/business” for data on the Shipping Label and data necessary to provide our track and trace service, and not a “data processor/service provider” on behalf of a “business.” This position is also consistent with guidance from various European data regulators and ICO’s document referenced above. For example, the Bavarian data authority’s guidance, available at https://www.lida.bayern.de/media/info_adv.pdf, gives examples that demonstrate that, in some contexts, the transfer of personal data is an “unavoidable accessory” (unvermeidliches “Beiwerk”) (p. 3-4). The examples that are provided include courier services, cleaning services, and repair and maintenance work. These examples make clear why the transfer of personal data can be ancillary to the services provided: one has to give one’s address to the cleaner to have clothes returned or give vehicle information to the mechanic to have it worked on and give names and addresses to the courier to have a package delivered. But these providers should not be classified as “data processors/service providers” as far as the data protection laws are concerned.

The California privacy laws have placed significant restrictions on “service providers” with respect to how they can use the data. For example, the CPRA Regulations “[prohibit]s the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business for any purposes other than those specified in the contract or as otherwise permitted by the CCPA and these regulations.” Section 7051(a)(3). The Regulations also state that “the business may require the service provider or contractor to provide documentation that verifies that they no longer retain or use the personal information of consumers that have made a valid request to delete with the business.” Section 7051(a)(9). The Regulations also provide that “the service provider or contractor [must] provide the same level of privacy protection as required by businesses by, for example, cooperating with the business in responding to and complying with consumers’ requests made pursuant to the CCPA.” Section 7051(a)(6).

The practicalities for and legal requirements imposed on shipping companies demonstrate why they must be “businesses” and not “service providers.” If one sends a box to John Smith at 123 Main Street, shipping companies have John Smith at 123 Main Street in its database. If shipping companies agreed to be a “processor/service provider,” they would be obligated to only use John Smith at 123 Main Street in accordance with instructions from a business and would be obligated to delete data if asked by a business. This, however, poses a direct conflict with regulatory requirements for shipping companies that must retain certain shipping records (e.g., customs and U.S. Department of Transportation requirements that require certain records be kept, Federal Aviation Regulations that require airlines to check the “do not fly” list, etc.).

Additionally, when a business asks to have a name and address deleted, that poses a particular hardship for shipping companies because that name and address are not uniquely associated with any single shipping customer. John Smith might be a customer of another retailer who ships, or he might be a customer of the shipping company himself. John Smith may no longer want a particular retailer to hold his personal data, but that does not mean he wants the shipping company to delete his data and no longer be able to receive tracking updates of other packages he has bought from separate retailers. Shipping companies could not restrict processing or delete that data because it does not belong to any particular business.

Likewise, an address deletion request from a data subject will prove difficult. For example, John Smith may make a request to have 123 Main Street deleted from a shipping company’s records, but 123 Main Street is not only associated with him. There may be family members that live at 123 Main Street, or John Smith may have moved and 123 Main Street may now be the residence of another individual. Accordingly, shipping companies should be considered a “business” in their own right and have more discretion than a “service provider” when it comes to how personal data is processed in furtherance of individual privacy rights.

Importantly, if shipping companies are considered “businesses,” rather than “service providers,” with respect to the personal data such companies obtain as part of their business, such a classification does not adversely affect the protection of such data. Shipping companies, like all other businesses, would still need to demonstrate that they have proper security safeguards and procedures in place to ensure the protection of all individuals’ personal data they process.

For these reasons, we urge you to classify transportation and/or shipping companies as a “business,” not a merely a “service provider.” As a way to clarify that distinction while still protecting consumer data, we respectfully ask for the text of Section 7050(a)(3)(B) be amended and moved to a new Section 7002(b)(5), as detailed above.

1. Transportation Providers Are “Businesses” as to Shipping Information, not “Service Providers.”

a. Package Transportation Providers Determine the Purposes and Means of the Processing of Shipping Information and Therefore Constitute “Businesses” as to Shipping Information Within the Meaning of the CCPA.

Transportation providers use Shipping Information by necessity for more than simply to deliver individual packages to each individual address. Shipping Information is inherently embedded into the operations of transportation providers, similar to how an organization might consume and integrate fuel or other supplies into its operations. As a result, transportation companies, not their retailer and other corporate customers, “determine the purposes and means of the processing of [this] information” and therefore constitute businesses, not service providers, under the CCPA.¹ For example:

- Carriers use Shipping Information continuously and on an automated basis for package routing within their networks; transportation and delivery planning and optimization; and to make decisions about package network optimization (including locations of facilities, retail outlets, staffing, “drop boxes” where consumers can pick up and leave packages, and capital investment). They do not simply use the information to deliver a specific package and then forget it.
- Shipping Information constitutes a combination of information received from customers, information carriers append from their own historical information and operations (including very specific details of package handling, status, and routing within a package network), and information they receive from third parties. The individual elements received from customers are integrated into this data and are not reasonably capable of being pulled back out.
 - Carriers continuously and automatically update Shipping Information about individual packages with additional information concerning individual shipment attributes, and operational details and requirements for shipments meeting such attributes (e.g., handling of a particular package due to its dimensions and weight (“DimWeight”) or service level (e.g., standard vs. priority)) in order to fulfill deliveries and operate and improve the carrier’s package transportation network. Carriers do this in order to route large numbers of deliveries to the right place at the right time, to manage the transportation network, and to improve the shipping network for future deliveries.
 - One of the more prominent examples of this is addresses: annually, carriers correct tens or hundreds of millions of addresses that customers have submitted to them using information carriers collect while delivering packages, or from data acquired from, e.g., the US Postal Service. Once an address is corrected, it enables future shipments from any other corporate customer to reach that same address as desired by the consumer(s) resident at that address.

These processing activities and the means of effecting them are all determined by the transportation provider, not the retailer or other corporate customer. The transportation provider therefore clearly constitutes a “business” within the meaning of the CCPA.²

It is important to note also that carriers also have the corresponding obligations of a business under the CCPA, such as to accept and fulfill requests to know and requests to delete. But if carriers are deemed to constitute service providers, and not businesses, when the shipper happens to be a corporate customer, then the carrier’s obligation will be to direct a consumer submitting a request back to the corporate customer. This would be an inefficient result which would create a risk of consumer

¹ Cal. Civ. Code § 1798.140(d).

² Id.

confusion. Indeed, our members' experience is that consumers continue to see themselves as having direct relationships with the individual carriers delivering shipments to them, whether in connection with tracking shipment status, submitting claims, or requesting privacy-related information.

b. A "Service Provider" Designation under the CCPA Will also Create Fundamental Operational Issues for the Package Transportation Industry.

In addition to being legally incorrect, the designation of transportation providers as "service providers" would create a fundamental operational problem for the transportation industry. Section 7050(a) permits service providers to use personal information for several purposes beyond delivering the requested service back to the business. One such use is "[f]or internal use by the service provider or contractor to build or improve the quality of its services uses of personal information." The regulations provide two examples, one of which references transportation companies:

(B) A shipping service provider that delivers businesses' products to their customers may use the addresses received from their business clients and their experience delivering to those addresses to identify faulty or incomplete addresses, and thus, improve their delivery services. However, the shipping service provider cannot compile the addresses received from one business to send advertisements on behalf of another business, or compile addresses received from businesses to sell to data brokers.

But this fails to acknowledge that carriers use shipping data in the form of package level detail or "PLD" for other operational purposes beyond service improvement, such as to perform advanced route optimization and network planning. These uses are essential to improve the efficiency of the flow of goods in the economy and to the ability of carriers to compete, but would be prohibited by the Modified Proposed Regulations if shipping companies are deemed service providers. Even if this interpretation is incorrect – which the California Trucking Association believes to be the case – we anticipate corporate customers may take a different position as a risk management measure because of concerns about other potential constructions of the law.

c. Even Data Protection Authorities in the European Union Recognize that Package Transportation Providers Are Controllers, not Processors.

The European Union General Data Protection Regulation (the GDPR) is arguably the most comprehensive and protective privacy law in the world. Even in the EU, under the GDPR, and under the UK's version of the GDPR, package transportation providers are deemed controllers for the very reason that carriers determine the purposes and means of the processing of Shipping Information.

- As an example, the United Kingdom's Information Commissioner's Office issued guidance in 2014 stating that a delivery service "will be a data controller in its own right in respect of any data it holds to arrange delivery or tracking ... such as individual senders' and recipients' names and addresses."³
- The Bavarian Office for Data Protection Supervision issued 2018 guidance stating that "postal services for letter or package transportation" are generally "not data processing," but instead "specialized services" offered by "an independent controller."⁴

³ See Information Commissioner's Officer, *Data Controllers and Data Processors: What the Difference Is and What the Governance Implications Are* at 12 (June 5, 2014), available at <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf>.

⁴ See Bayerisches Landesamt für Datenschutzaufsicht [Bavarian Office for Data Protection Supervision], *FAQ zur DSGVO: Auftragsverarbeitung, Abgrenzung* [GDPR FAQs: Data Processing, Distinguishing [between Controllers and

d. The Sharing of Data by Retailers and Other Corporate Customers with Package Transportation Companies to Ship Packages Should Not be Deemed a “Sale” of Personal Information.

When a retailer provides Shipping Information to a carrier, it discloses the information as a business, as defined in the CCPA, to another business. But this disclosure does not constitute a sale of personal information, because (a) consumers are “direct[ing the retailer] to . . . intentionally disclose personal information.”⁵

- Subsection 1798.140(ad)(2)(A) provides that a business does not “sell” personal information when “a consumer uses or directs the business to . . . intentionally disclose personal information.” This is precisely what happens when consumers order goods from carriers’ corporate customers that need to be shipped.
- Specifically, when consumers buy products, they are directing retailers and other corporate customers to disclose Shipping Information to a transportation provider, instead of making their own separate arrangements with a transportation provider directly or, when applicable, retrieving the merchandise from the corporate customer’s facility. In fact, consumers generally pay a separate and extra charge for shipping, arguably affirmatively obligating the corporate customer to share information with a transportation provider for shipping purposes.
- To exempt consumer-directed data disclosures from being a “sale,” the CCPA does not require that the consumer specify precisely who should receive their personal information. Instead, the § 1798.140(ad)(2)(A) requires only that the consumer “direct” a retailer or manufacturer to “intentionally disclose” their information. Consumers who purchase merchandise from retailers or manufacturers have exactly this in mind – that their data will be provided to a carrier that will deliver the merchandise to them.

Shipping Information remains protected under the CCPA in the hands of the carrier. This information is also protected by a longstanding federal law that regulates its handling and disclosure.⁶

The California Trucking Association believes the plain meaning of the CCPA establishes that retailers and other corporate customers transfer Shipping Information to transportation providers outside the definition of a “sale” pursuant to the direction of the consumer purchasing the product. But our members are seeing certain corporate customers interpret the law differently, positioning carriers as “service providers” as defined in the CCPA, out of a concern that disclosing data to a separate “business” carries a “sale” risk. This designation would be inconsistent with the facts. Delivery providers determine the purposes and means of the processing of Shipping Information. But such a finding would also prevent package transportation providers from being able to use Shipping Information for any purpose beyond delivering each individual package – a result that will impair operations across the industry with no corresponding consumer benefit. The California Trucking Association therefore respectfully requests the CCPA to clarify the application of Section 1798.140(ad)(2)(A) to Shipping Information that transportation providers receive from businesses, pursuant to the CCPA’s rulemaking authority under Cal. Civ. Code § 1798.185(b).

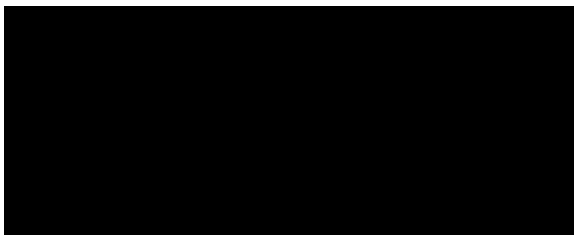
Processors]] at 2 (July 20, 2018), available (in German) at https://www.lida.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf.

⁵ Cal. Civ. Code § 1798.140(ad)(2)(A).

⁶ See 49 U.S.C. § 14908.

We appreciate the California Privacy Protection Agency's review and consideration of our comments in this letter, and look forward to the CCPA's continued efforts through the rulemaking process. For any questions or feedback, please contact Chris Shimoda. We thank the California Privacy Protection Agency for the opportunity to provide our views for consideration, and look forward to working with you to address the matters outlined above.

Sincerely,



Chris Shimoda
Senior Vice President of Government Affairs



From: [REDACTED]
Sent: Friday, November 18, 2022 8:14 PM
To: Regulations
Cc: [REDACTED]
Subject: Comment to Modified Proposed Regulations_Washington Legal Foundation
Attachments: Comment to Modified Proposed Regulation_Washington Legal Foundation.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear Mr. Soublet

Please find attached a comment submitted on behalf of Washington Legal Foundation in response to the Modified Proposed Regulations propounded by the CPPA.

Sincerely,

Andrea Maciejewski

Andrea Maciejewski
Associate

Greenberg Traurig, LLP
1144 15th Street, Suite 3300 | Denver, Colorado 80202

T [REDACTED] | www.gtlaw.com | [REDACTED]

GT GreenbergTraurig

If you are not an intended recipient of confidential and privileged information in this email, please delete it, notify us immediately at [REDACTED], and do not use or disseminate the information.

David A. Zetony

Tel

Fax

November 18, 2022

VIA EMAIL (regulations@cpha.ca.gov)

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

Re: Washington Legal Foundation's Supplemental Comment on CCPA Rulemaking/
 CCPA Public Comment

On August 17, 2022, the law firm of Greenberg Traurig LLP submitted a comment on behalf of Washington Legal Foundation. The Comment explained that the CCPA had failed to comply with administrative processes when it proposed regulations to implement the California Privacy Rights Act. Specifically, the Comment identified 46 new compliance obligations that would have been imposed by the July 8, 2022, version of the California Privacy Protection Agency's proposed regulations. The Comment itemized those new compliance obligations, explained the burden that those compliance obligations would impose on businesses, and highlighted that the CCPA had failed to account for that burden and failed to complete a Standard Regulatory Impact Analysis ("SRIA") as is required by the California Administrative Procedures Act.

On November 3, 2022, the CCPA published a Notice of Modifications to Text of Proposed Regulations. The Modified Text of Proposed Regulations deviate significantly from the Original Proposed Regulations. Indeed, a preliminary word count shows that the modifications added and/or deleted 7,400 words – about 30 double-spaced pages. Although the CCPA characterizes these changes as sufficiently related to the Original Proposed Regulations in order to justify the shorter 15-day notice and comment period, the sheer quantity of the modifications makes it difficult for the public to fully understand – let alone consider – the changes; WLF believes that the public interest would have been better served if the CCPA had provided a longer period than 15 days (particularly as the 15-day time period included a federal holiday).

WLF has attempted to review the Modified Proposed Regulations in the short amount of time provided. Based upon that initial review it appears that the CCPA has removed 19 of the 46 compliance burdens flagged in the Comment. WLF commends the CCPA for removing these

Greenberg Traurig, LLP | Attorneys at Law

1144 15th Street | Suite 3300 | Denver, Colorado 80202 | T +1 303.572.6500 | F +1 303.572.6540

Albany. Amsterdam. Atlanta. Austin. Berlin*. Boston. Charlotte. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Houston. Las Vegas. London.* Long Island. Los Angeles. Mexico City*. Miami. Milan*. Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Sacramento. Salt Lake City. San Francisco. Seoul*. Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv*. Tokyo*. Warsaw*. Washington, D.C. West Palm Beach. Westchester County.

Operates as "Greenberg Traurig Germany LLP" "A separate UK registered legal entity "Greenberg Traurig S.C." "Greenberg Traurig Santa Maria" "Greenberg Traurig LLP Foreign Legal Consultant Office" "A branch of Greenberg Traurig P.A. Florida USA" "GT Tokyo Haribu Jimusho and Greenberg Traurig Gekokuhajimusho Jimusho" "Greenberg Traurig Nowakowski-Zimoch Wysocki sp.k."

November 20, 2022

Page 2

provisions. For example, one of the compliance burdens discussed in the Comment was a Proposed Regulation that would have required a business to provide consumers with the name of the source of any allegedly inaccurate information.¹ Presumably in recognition of the significant compliance burden described in the Comment, the CPPA modified the provision to read that a business “may” provide, instead of “shall” provide, such information.

With regard to the 27 remaining compliance burdens identified in the Comment:

- **14 have not been modified, removed, or deleted.**² For the reasons stated within the Comment, these proposals should **not** be adopted as an SRIA has not been completed regarding the impact that these requirements would impose.
- **13 have been modified, but the modifications do not eliminate the compliance burdens imposed by the Original Proposed Regulations.**³ Indeed, in many cases the CPPA has added **additional** compliance burdens. For example, Proposed Regulation 7025(c)(1) would require businesses to create persistent mechanisms for known consumers. The Modified Proposed Regulation would require persistence for both “consumer profile[s] associated with [a] browser” (known consumers) as well as “pseudonymous profiles.” It is not clear what is intended by the addition of “pseudonymous profiles,” but to the extent that the new language requires businesses to attempt to associate an opt-out signal to individuals whose identities are not known by the business, the modified proposal raises a host of additional compliance burdens and costs including (a) businesses would need to determine what constitutes a “pseudonymous profile,” (b) businesses would need to create a system to update pseudonymous profiles if an opt-out signal is detected, and (c) businesses would need to create a system to reconcile updates to pseudonymous profiles with actual profiles for instances in which a pseudonymous profile is later associated with a known consumer (i.e., a consumer logs-into a known account). The CPPA considered none of these burdens or costs, let alone considered them as part of an SRIA as mandated by the APA.

While WLF is heartened by the fact that the CPPA has eliminated 19 of the compliance burdens identified in the Comment, the administrative and procedural issues identified in the Comment

¹ See Comment at Item 19 (in re Proposed Regulation § 7023(i)).

² This includes the following items in the Comment (all references are to the section numbers in the Original Proposed Regulations): Comment Item 1 (§ 7001(c)); Comment Item 9 (§ 7013(c)); Comment Item 16 (§ 7022(b)(3)); Comment Item 23 (§ 7025(c)(5)); Comment Item 26 (§ 7026(a)(4)); Comment Item 29 (§ 7027(g)(3)); Comment Item 33 (§ 7050(c)(1)); Comment Item 34 (§ 7051(a)(2)); Comment Item 26 (§ 7051(e)); Comment Item 42 (§ 7053(e)); Comment Item 43 (§ 7102(a)(1)(B)); Comment Item 44 (§ 7102(a)(1)(E)); Comment Item 45 (§ 7102(a)(1)(F)); Comment Item 46 (§ 7304(c)).

³ This includes the following items in the Comment (all references are to the section numbers in the Original Proposed Regulations): Comment Item 2 (§ 7003(c)); Comment Item 4 (§ 7004(a)(2)); Comment Item 7 (§ 7004(a)(4)(c)); Comment Item 10 (§ 7013(e)(3)(c)); Comment Item 15 (§ 7021(a)); Comment Item 17 (§ 7023(c)); Comment Item 18 (§ 7023(f)(4)); Comment Item 21 (§§ 7025(b), (c), (e), 7026(a)(1)); Comment Item 22 (§ 7025(c)(1), (7)(B), (7)(C)); Comment Item 27 (§ 7026(f)(3)); Comment Item 28 (§ 7026(i)), Comment Item 31 (§ 7027(g)(5)).

November 20, 2022

Page 3

remain in connection with 27 Modified Proposed Regulations. As expressed in the Comment, the CCPA should eliminate these 27 compliance obligations, or remedy the procedural deficiencies by completing an SRIA, submitting it to the DOF for analysis and publication, and considering alternatives that would decrease the compliance impact. Only once that process has been completed should the proposals be resubmitted for 45-day notice and comment.

Without adhering to the APA's processes, which are designed to give consumers, stakeholders, and government agencies alike proper notice of the impact a proposed regulation might have, the Modified Proposed Regulations (if adopted) will continue to be susceptible to collateral attack as invalid and unenforceable.

Best Regards



David A. Zetoon, Shareholder & Co-Chair US Privacy and Security Practice
Andrea Maciejewski, Associate
Madison Etherington, Intern

From: Rachel Michelin <[REDACTED]>
Sent: Sunday, November 20, 2022 10:57 AM
To: Regulations
Subject: Comments on Revised Rules
Attachments: CRA CCPA Reg comments Round 2.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

On behalf of the California Retailers Association, please find attached our collective comments and suggested edits on the second round of proposed rules.

If you have any questions or need additional information please do not hesitate to contact me directly.

Thank you in advance for your consideration.

Rachel Michelin

President & CEO
1121 L Street, #607
Sacramento, CA 95814
P: [REDACTED]





November 20, 2022

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

VIA Email: regulations@cppa.ca.gov.

Dear Members of the Committee:

On behalf of the California Retailers Association please see our comments related to the California Consumer Privacy Act Regulations and the formal rulemaking process to adopt regulations to implement the Consumer Privacy Rights Act of 2020 (CPRA).

General concerns around the discrepancy between the text of CPRA and the CPPA regs concerning the Opt-out Preference Signal.

CPRA makes the Global Privacy Control / Universal opt-out preference signal optional, while the CPPA is making it mandatory in its regulations. Given the text of CPRA's optional treatment of these signals, it's safe to assume many businesses have not yet stood up initiatives or have made investments to support. Now with Attorney General enforcement in this area brought upon retailers, there is concern about regulatory enforcement risk amidst ambiguity.

At a minimum, if making it mandatory, we ask the agency to provide a post-Jan 1, 2023, timeline for compliance with net-new requirements. Additionally, we ask for the establishment of more prescriptive technical standards for the preference signal. Although there are groups who provide a list of browsers that have this preference signal, there are currently 7 different browsers, uniformity in technical standards would make it easier for business to receive and honor signals.

Below are California Retailers Association comments on specific sections:

§7002(b)(3) Restrictions on the Collection and Use of Personal Information.

Revised Rule Text: *The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer. The consumer's reasonable expectations concerning the purpose for which the personal information will be collected or processed shall be based on the following factors: . . . (3) The source of the personal information and the business's method for collecting or processing it. For example, if the consumer is providing their personal information directly to the business while using the business's product or service, the consumer likely expects that the business will use the personal information to provide that product or service. However, **the consumer may not expect that the business will***

use that same personal information for a different product or service offered by the business or the business's subsidiary.

Action Requested: How a business uses collected data across its products and services should not be unduly limited where the privacy notice expressly discloses those potential uses and that it might occur across products/services. To the extent this factor is retained, it should focus on whether the use of the different product or service is unexpected and unrelated.

Proposed Edit: However, the consumer may not expect that the business will use that same personal information for **an unexpected and unrelated use on a** different product or service offered by the business or the business's subsidiary.

§7002(b)(4) Restrictions on the Collection and Use of Personal Information.

Revised Rule Text: *The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer. The consumer's reasonable expectations concerning the purpose for which the personal information will be collected or processed shall be based on the following factors: . . . (4) **The specificity, explicitness, and prominence of disclosures to the consumer about the purpose for collecting or processing the consumer's personal information, such as in the Notice at Collection and in the marketing materials to the consumer about the business's good or service.** For example, the consumer that receives a pop-up notice that the business wants to collect the consumer's phone number to verify their identity when they log in likely expects that the business will use the personal information for the purpose of verifying the consumer's identity. Similarly, the consumer may expect that a mobile application that markets itself as a service that finds cheap gas close to the consumer will collect and use the consumer's geolocation information for that specific purpose when they are using the service.*

Action Requested: Marketing and other non-privacy disclosures should not be a relevant factor in determining a consumer's reasonable expectation about the disclosures in the privacy notice. The purpose of the privacy notice is to provide a one-stop notice for consumers regarding how their data is used. In contrast, marketing materials highlight the benefits for the product or service and thus are not necessarily relevant to how data is used unless the disclosure makes that connection explicit (as occurs in the first example about the pop-up notice).

Proposed Edit: The specificity, explicitness, and prominence of disclosures to the consumer about the purpose for collecting or processing the consumer's personal information, **such as** in the Notice at Collection **and in the marketing materials to the consumer about the business's good or service.** For example, the consumer that receives a pop-up notice that the business wants to collect the consumer's phone number to verify their identity when they log in likely expects that the business will use the personal information for the purpose of verifying the consumer's identity. **Similarly, the consumer may expect that a mobile application that markets itself as a service that finds cheap gas close to the consumer will collect and use the consumer's geolocation information for that specific purpose when they are using the service.**

§7002(b)(5) Restrictions on the Collection and Use of Personal Information.

Revised Rule Text: *The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer. The consumer’s reasonable expectations concerning the purpose for which the personal information will be collected or processed shall be based on the following factors: . . . (5) **The degree to which the involvement of service providers, contractors, third parties, or other entities in the collection or processing of personal information is apparent to the consumer.** For example, the consumer likely expects an online retailer’s disclosure of the consumer’s name and address to a delivery service provider in order for that service provider to deliver a purchased product, because that service provider’s involvement is apparent to the consumer. By contrast, the consumer may not expect the disclosure of personal information to a service provider if the consumer is not directly interacting with the service provider or the service provider’s role in the processing is not apparent to the consumer.*

Action Requested: This added factor, as phrased, should not be relevant in determining a consumer’s reasonable expectation. In general, consumers do not have the business background to understand processor relationships or any reason to reflect on how a business processes their data. To the extent this factor is retained, the rule should be modified to focus on uses that are unexpected and offensive with respect to the disclosed uses.

Proposed Edit: The degree to which the involvement of service providers, contractors, third parties, or other entities in the collection or processing of personal information **would be unexpected [and offensive] is apparent to the consumer.**

§7004(a)(2) Symmetry in choice

Revised Rule Text: *The path for a consumer to exercise a more privacy-protective option shall not be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option because it impairs or interferes with the consumer’s ability to make a choice.*

Action Requested: The revised provision still places an undue burden on design to the extent it requires exact symmetry in length, which might not be appropriate in all instances. The revised suggested edit below makes clear that lack of symmetry is a dark pattern only when it results in impairing or interfering with ability to make a choice.

Proposed Edit: The path for a consumer to exercise a more privacy-protective option shall not be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option **because to the extent** it impairs or interferes with the consumer’s ability to make a choice.

§7015(b) Alternative Opt-Out Link.

Revised Rule Text: *A business that chooses to use an Alternative Opt-out Link shall title the link, “Your Privacy Choices” or “Your California Privacy Choices,” **and shall include the following opt-out icon to the right or left of adjacent to the title.** The link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business’s internet Homepage(s). The icon shall be approximately the same size as **any** other icons used by the business in the header or footer **of** on its webpage.*

Action Requested: The draft CPRA rules would mandate the opt-out icon that was only optional under the 2020 CCPA rules. This icon should not be mandated because it has the potential to confuse consumers since the static image looks like a toggle that a consumer can activate. It also prescribes a graphic feature that may not align with a business' design layout, putting unnecessary burden on a business without countervailing consumer benefit.

Proposed Edit: A business that chooses to use an Alternative Opt-out Link shall title the link, "Your Privacy Choices" or "Your California Privacy Choices," and **shall may** include the following opt-out icon adjacent to the title.

§7025(b) Opt-Out Preference Signals

Revised Rule Text: (1) *The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field or JavaScript object.*

Action Requested: Requirements to honor UOOMs should not exceed the capabilities of eligible UOOMs that are available in the marketplace (e.g., if only browser extensions can serve as UOOMs, the requirement to honor UOOM signals should only extend to browsers).

The preference signal should also offer a consumer to both turn on and off the opt-out preference. As currently drafted, the regulations deprive the consumer of the ability to fully control opt-out preference.

Proposed Edit: A business shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing:

(1) The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field.

(2) The signal shall have the capability to indicate that the consumer has selected to turn off the opt-out preference signal.

~~(2)~~(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 does not need to be tailored only to California or to refer to California.

(4) The business's obligation to process a preference signal shall not exceed the technical capability of the platform, technology, or mechanism that sends the opt-out preference signal. For instance, where a signal is in an HTTP header field format, the business shall process the signal only where it is received on a browser.

§7025(c)(7)(A) Opt-Out Preference Signal Example

Revised Rule Text: *Caleb visits Business N's website using a browser with an opt-out preference signal enabled, but he is not otherwise logged into his account and the business cannot otherwise associate Caleb's browser with a consumer profile the business maintains. Business N collects and shares Caleb's personal information tied to his browser identifier for cross-contextual advertising, but Business N does not know Caleb's real identity because he is not logged into his account.* Upon receiving the opt-out preference signal, Business N

shall stop selling and sharing Caleb’s *information linked to Caleb’s browser* identifier for cross-contextual advertising, but it would not be able to apply the request to opt-out of the sale/sharing to Caleb’s account information because the connection between Caleb’s browser and Caleb’s account is not known to the business.

Action Requested: The added language may require companies to take extra action to associate an unauthenticated visitor with an account which is less privacy friendly. The focus should be on whether the visitor is logged in to avoid any obligation for a company to process additional personal data.

Proposed Edit: Caleb visits Business N’s website using a browser with an opt-out preference signal enabled, but he is not otherwise logged into his account. ~~and the business cannot otherwise associate Caleb’s browser with a consumer profile the business maintains.~~

§7026(a)(1) Requests to Opt-Out of Sale/Sharing.

Revised Rule Text: ~~If a~~ *A* business that collects personal information from consumers online, ~~the business~~ shall, at a minimum, allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal and ~~through at least one of the following methods~~—an interactive form accessible via the “Do Not Sell or Share My Personal Information” link, the Alternative Opt-out Link, or the business’s privacy policy *if the business processes an opt-out preference signal in a frictionless manner.*

Action Requested: The Agency should remove the added limitation for processing in a frictionless manner because the alternatives and the benefits to the consumer are unclear.

Proposed Edit: A business that 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 and at least one of the following methods—an interactive form accessible via the “Do Not Sell or Share My Personal Information” link, the Alternative Opt-out Link, or the business’s privacy policy. ~~if the business processes an opt-out preference signal in a frictionless manner.~~

We seek clarity on the following sections:

§7002(a) Restrictions on the Collection and Use of Personal Information.

This section states the business’s information practice must be reasonably necessary and proportionate to achieve (1) the purposes for which the PI was collected or (2) another disclosed purpose that is compatible with the context in which the PI was collected. For (1), the draft states the purposes for which the PI was collected is within “reasonable expectation” narrowly by stating using PI collected in one transaction for a different product/service is not reasonably expected. See 7002(b)(3). For (2), the section then states whether “another disclosed purpose” is compatible would be based on the factors disclosed in (b) or for business purposes disclosed in 1798.140(e), which specifically excludes targeted advertising.

Reading them together, it is no longer clear whether a business can use the information collected during a transaction for subsequent direct marketing (e.g., a customer bought a washer, and the retailer uses the information to market a matching dryer). In addition, it is even more unclear whether a retailer can use the

information for subsequent targeted advertising due to the exclusion stated in (2), even if it discloses the purposes in the privacy statement.

The regulatory language deviates from the CPRA statutory language in two aspects: (1) The language is unclear as to whether it is essentially converting the CCPA from a notice and consent regime to an opt-in regime for secondary marketing use, and (2) for targeted marketing, the current CCPA is an opt-out regime, but the new language deviates from that approach.

§ 7050. Service Providers and Contractors

Proposed section 7050(b) considers someone who contracts with a business to provide cross-contextual behavioral advertising as a third party and not a service provider or contractor, which is a distinction without much value for California consumers. A company that provides cross-contextual behavioral advertising service should be considered a service provider if the business only uses personal information to provide the advertising services. If the company is not using the personal information for its own purposes and only uses it to provide services as laid out in the agreement, there is no reason why they should not be considered a service provider. As written, this section will only harm advertising businesses without benefiting consumers.

Additionally, the example noted in proposed section 7050(c)(2) of the draft regulations purports to prohibit a form of widely accepted advertising based on email addresses. This example is inconsistent with the text of CPRA, including Section 1798.140(e)(6), (j)(1)(A)(iv), and (ag)(1)(D). The example would have significant implications for businesses, particularly small retailers, that rely on these advertising tools to reach their customers with information that has been provided to them for this purpose. A customer list that a business uploads, provided they have the necessary permission to do so, helps them reach their own customers in a privacy-protective way. Restricting the ability for California businesses to continue to use such tools will make it harder for them to reach their customers on social media platforms, increase the costs these businesses incur for advertising, and disproportionately affect their ability to compete against their competitors outside of the State.

Thank you for the consideration of our concerns and our suggestions on clarification. If you have any questions or would like additional input, please do not hesitate to reach out to me directly.



Rachel Michelin
President & CEO
California Retailers Association

From: Saul Bercovitch [REDACTED]
Sent: Sunday, November 20, 2022 11:38 AM
To: Regulations
Subject: CCPA Public Comment
Attachments: CCPA Rulemaking CLA Privacy Law Section Comments - 11-20-22 FINAL.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

I have attached comments of the Privacy Law Section of the California Lawyers Association on the proposed regulations implementing the California Consumer Privacy Act that were provided for public comment beginning on November 3, 2022. Thank you.

Saul Bercovitch | Associate Executive Director, Governmental Affairs

California Lawyers Association

[400 Capitol Mall, Suite 650 | Sacramento, CA 95814](#)

O: [REDACTED] | [REDACTED]





CALAWYERS.ORG/PRIVACY

November 20, 2022

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

Sent via e-mail to regulations@coppa.ca.gov

Re: Comments on November 3, 2022 Proposed California Consumer Privacy Act Regulations

Dear Mr. Soublet:

The Privacy Law Section of the California Lawyers Association ("CLA") respectfully subjects its comments on the proposed regulations implementing the California Consumer Privacy Act ("CCPA") that were provided for public comment beginning on November 3, 2022.

CLA is the statewide bar association for California lawyers. It has approximately 72,000 members and is one of the largest statewide voluntary bar associations in the United States. CLA's mission is to promote excellence, diversity, and inclusion in the legal profession and fairness in the administration of justice and the rule of law. CLA has 18 sections that focus on specific areas of subject matter expertise.

The Privacy Law Section has over 800 members and represents a multidisciplinary group of privacy practitioners including consumer privacy advocates, government regulators, law firm practitioners, chief privacy officers, in-house privacy counsel, and policy analysts at privacy think tanks. Our members have broad-ranging expertise in areas that include consumer privacy, cybersecurity, and data protection, with experience in related regulatory, transaction, and litigation matters.

The comments submitted by the Privacy Law Section use the following format: 1) we quote the rule as proposed by the California Privacy Protection Agency ("Agency"); 2) we provide our comment regarding the proposed rule; and 3) we propose revisions to the proposed rule consistent with our comment, using strikeouts for proposed deletions and underlines for proposed additions.

EMPLOYMENT AND BUSINESS-TO-BUSINESS PERSONAL INFORMATION

In the intervening months since the first set of proposed regulations was issued by the Agency, the California Legislature did not extend the limited applicability of CCPA to employment data and business-to-business data, as set forth in Civil Code sections 1798.145(h) and 1798.145(n) that are in effect through December 31, 2022.

The impending expiration of these exemptions without regulatory guidance that “tak[es] into account the differences in the relationship between employees or independent contractors and businesses, as compared to the relationship between consumers and businesses” is creating extreme uncertainty for practitioners and consumers. CPRA Section 3(A)(8). We urge the Agency to prioritize development of regulations specific to the employment context and to do so as quickly as possible.

Article 1. GENERAL PROVISIONS

§ 7002. Restrictions on the Collection and Use of Personal Information.

Rule

§ 7002(a)(1)

(a) In accordance with Civil Code section 1798.100, subdivision (c), a business’s collection, use, retention, and/or sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve:

(1) The purpose(s) for which the personal information was collected or processed, which shall comply with the requirements set forth in subsection (b).

Comments

We recommend the Agency remove the proposed addition to Section 7002(a)(1) because it is unnecessary. If the Agency adopts the changes we recommend below in subsection 7002(b), it would be clear to businesses that the purposes for processing should consider the reasonable expectations of the consumer based on relevant factors apparent in the context of the interaction with the consumer. Moreover, section 7002(b) already instructs businesses to consider the factors, so the language in section 7002(a)(1) is redundant.

Proposed Alternative Language

(a) In accordance with Civil Code section 1798.100, subdivision (c), a business’s collection, use, retention, and/or sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve:

(1) The purpose(s) for which the personal information was collected or processed.,
~~which shall comply with the requirements set forth in subsection (b)~~

Rule

§ 7002(b). The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed. The consumer's reasonable expectations concerning the purpose for which their personal information will be collected or processed shall be based on the following: . . .

Comments

Civil Code Section 1798.185(a)(10) instructs the Agency to issue regulations “further defining and adding to the purposes for which businesses, service providers, and contractors may use consumers’ personal information consistent with consumers’ expectations.” Section 7002(b) proposes mandatory and presumably exclusive factors businesses must consider when determining a consumer’s reasonable expectations. The Privacy Law Section recommends that the Agency revise the proposed regulations to make clear that the factors are neither exclusive nor exhaustive so that businesses may be free to consider other factors which may be applicable in understanding consumers’ expectations in a particular context. For example, other relevant factors may include: (i) the necessity of personal information in providing the products or services to the consumer; (ii) whether the consumer submits personal information to the business or whether the personal information is gathered or collected based on the consumer’s activity; and (iii) the stated or reasonably apparent intent of the consumer when engaging with the business. We also recommend the Agency explain that no one factor is determinative or weighted more heavily than another. Doing so would clarify that the reasonable expectations of a consumer in a particular context should be based on a constellation of factors considered together. Finally, we recommend the Agency clarify some of the examples provided in support of the factors so that businesses can understand how the factors should be considered.

Proposed Alternative Language

The purpose(s) for which the personal information ~~was~~ are collected or processed ~~shall~~ should be consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed. Factors to be considered in determining the consumer’s reasonable expectations concerning the purpose for which their personal information will be collected or processed include the following non-exclusive factors ~~shall be based on the following~~: . . .

Rule

§ 7002(b)(1). The relationship between the consumer(s) and the business. For example, if the consumer is intentionally interacting with the business on its website to purchase a good or service, the consumer likely expects that the purpose for collecting or processing the personal information is to provide that good or service. By contrast, for example, the consumer of a business's mobile flashlight application would not expect the business to collect the consumer's geolocation information to provide the flashlight service.

Comment

Section 7002(b)(1) requires the business to consider the “relationship between the consumer(s) and the business” when determining the consumer’s reasonable expectation. However, in the two examples provided, the business-consumer relationships are not clearly distinguishable. In both examples the relationship between the business and consumers is that of the provider and acquirer of a product or service (e.g., the unnamed “good or service” in the first example and the “mobile flashlight app” in the second example). Rather than highlight differences in the business/consumer relationships, the examples distinguish the type and nature of the personal information being collected. These examples seem more appropriate with respect to the factor in subsection (b)(2).

We recommend revising this requirement to provide a more concrete example of the differing relationships between a business and a consumer. For example, the Agency could distinguish between businesses that provide consumers ongoing services versus one-time transactions or between a business acting as an employer (where a consumer may expect broader purposes for processing personal information) versus a business with whom the consumer has only limited engagement.

Proposed Alternative Language

The relationship between the consumer(s) and the business. For example, a consumer would not reasonably expect an e-commerce website to store payment card information in connection with a one-time transaction in which the consumer did not create an account. ~~if the consumer is intentionally interacting with the business on its website to purchase a good or service, the consumer likely expects that the purpose for collecting or processing the personal information is to provide that good or service. By contrast, for example, the consumer of a business's mobile flashlight application would not expect the business to collect the consumer's geolocation information to provide the flashlight service.~~

Rule

§ 7002(b)(2). The type, nature, and amount of personal information that the business seeks to collect or process. For example, if a business's mobile communication application requests access to the consumer's contact list in order to call a specific individual, the consumer who is providing their contact list likely expects that the purpose of the business's use of that contact list will be to connect the consumer with the specific contact they selected. Similarly, if a business collects the consumer's fingerprint in connection with setting up the security feature of unlocking the device using the fingerprint, the consumer likely expects that the business's use of the consumer's fingerprint is only for the purpose of unlocking their mobile device.

Comments

We recommend the Agency amend this factor to clarify what is meant by the "type" and "nature" of personal information. The examples do not clearly illustrate this. For example, the example provided regarding the request for the list of contacts to call a specific individual appears to be inconsistent with the point being made: if a contact list were provided, rather than simply requesting information for a specific individual, it would be reasonable to assume the business would use that list for other purposes, like connecting the consumer with other contacts in their contacts list. The Agency could, for example, clarify that a consumer may reasonably expect that the business will only collect and use the type of personal information necessary to provide the product, service, or feature requested by the consumer in the specific interaction with the business. Similarly, the Agency may clarify that consumers may reasonably expect Sensitive Personal Information will only be used for the primary purpose for which it is collected or a secondary purpose consistent with section 7002(c).

Proposed Alternative Language

The type, nature, and amount of personal information that the business seeks to collect or process. For example, if a business's mobile communication application requests access to one of the consumer's contacts in order to call a specific individual, the consumer who is providing their contact list likely expects that the purpose of the business's use of that contact will be to connect the consumer with the specific contact they selected because the type of personal information collected is necessary for fulfilling the consumer's request. Similarly, if a business collects the consumer's fingerprint in connection with setting up the security feature of unlocking the device using the fingerprint, the consumer likely expects that the business's use of the consumer's fingerprint is only for the purpose of unlocking their mobile device.

Rule

§ 7002(c). Whether another disclosed purpose is compatible with the context in which the personal information was collected shall be based on the following: . . .

Comments

Section 7002(c) lists additional factors for businesses to consider as to whether another disclosed purpose is compatible with the context in which the personal information was collected. The language of the proposed regulation, however, makes the factors mandatory by stating the businesses “shall” consider the factors. Civil Code section 1798.100, subdivision (c) requires that the collection, use, retention, and sharing of a consumer’s personal information “shall be reasonably necessary and proportionate,” but the creation of mandatory and presumably exclusive factors businesses must consider goes beyond the requirements of the CCPA and conflicts with the text of the statute. The Privacy Law Section recommends that the Agency revise the proposed regulations to make clear that the factors are neither exclusive nor exhaustive so that businesses may be free to consider other factors which may be applicable.

Proposed Alternative Language

Whether another disclosed purpose is compatible with the context in which the personal information was collected ~~shall~~may be based on the following: . . .

Rule

§ 7002(d). Whether a business’s collection, use, retention, and/or sharing of a consumer’s personal information is reasonably necessary and proportionate to achieve the purpose identified in subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent, shall be based on the following:

Comments

Similar to section 7002(c), the language of the proposed regulation makes the factors mandatory by stating the businesses “shall” consider the factors. The Privacy Law Section recommends that the Agency revise the proposed regulations to make clear that the factors are neither exclusive nor exhaustive so that business may be free to consider other factors which may be applicable.

Proposed Alternative Language

Whether a business’s collection, use, retention, and/or sharing of a consumer’s personal information is reasonably necessary and proportionate to achieve the purpose

identified in subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent, ~~shall~~ may be based on the following: . . .

ARTICLE 4. SERVICE PROVIDERS, CONTRACTORS, AND THIRD PARTIES

§ 7050. Service Providers and Contractors.

Rule

§ 7050(g). Whether an entity that provides services to a Nonbusiness must comply with a consumer's CCPA request depends upon whether the entity is a "business," as defined by Civil Code section 1798.140, subdivision (d).

Comments

The Privacy Law Section supports the changes made in section 7050(g), but suggests changes to clarify the scope of the personal information for which the entity may be deemed a "business" under the CCPA.

During the 45-day comment period, the Privacy Law Section submitted comments regarding current section 7050(a), which proposed section 7050(g) would replace. In its comments, the Privacy Law Section supported the overall intent of current section 7050(a) to ensure that entities providing services for Nonbusinesses are not subject to CCPA rights that the Nonbusinesses themselves are not subject to. As the Agency observed in its initial statement of reasons in July, "This unintended and undesired consequence will lead to significant disruption in the functioning of those nonprofits and governmental entities and is not in furtherance of the purposes of the CCPA, which explicitly excluded nonprofits and government entities from being subject to the CCPA." The Privacy Law Section urged the Agency to adopt regulatory language aligned with the statutory definition of a "service provider" and its requirement that services be provided "on behalf of a business."

Proposed section 7050(g) accomplishes both of those goals — it preserves the original intent of current section 7050(a) and aligns with the language of the CCPA. However, the language as drafted may be too broad; it suggests that if an entity meets the CCPA definition of a "business" in any of its business lines, it will be subject to the CCPA in all of those business lines, including its provision of services to Nonbusinesses. Therefore, the Privacy Law Section suggests inserting language that emphasizes that the determination of whether the entity is a "business" for purposes of providing services to Nonbusinesses is limited to its processing of personal information for those services.

Further, the Privacy Law Section believes that the illustrations provided in the proposed rules circulated with the agenda for the Agency Board's October 28-29 meeting are helpful and should be included as illustrative examples.

Propose Alternative Language

§ 7050(g). Whether an entity that provides services to a Nonbusiness must comply with a consumer's CCPA request depends upon whether the entity is a "business" with regard to any personal information that it collects, maintains, or sells in the provision of those services, as defined by Civil Code section 1798.140, subdivision (d). Illustrative examples follow.

- (1) Entity A is a cloud storage services company that meets the definition of a "business" under CCPA. Entity A provides cloud storage services to a Nonbusiness. If Entity A receives a request to know from a consumer pertaining to personal information it processes on behalf of the Nonbusiness, if the Nonbusiness is the only entity that determines how that personal information is processed and used, then Entity A is not acting as a "business" pursuant to Civil Code section 1798.140, subdivision (d) with respect to the Nonbusiness and does not need to comply with the consumer's request.
- (2) However, if Entity A uses the personal information it stores on behalf of the Nonbusiness for Entity A's own purposes, such as developing new products or services, Entity A may fall under the definition "business" and may have to comply with the consumer's request with regard to that personal information if it meets the remaining requirements of Civil Code section 1798.140, subdivision (d).

§ 7027. Requests to Limit Use and Disclosure of Sensitive Personal Information

Rule

§ 7027(a). The unauthorized use or disclosure of sensitive personal information creates a heightened risk of harm for the consumer . . . Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to requests to limit.

[...]

§ 7027(m). The purposes identified in Civil Code section 1798.121, subdivision (a), 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, provided that the use or disclosure is reasonably necessary and proportionate for those purposes, is not required to post a Notice of Right to Limit or provide a method for submitting a request to limit.

(1) To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services. For example, a consumer's precise geolocation may be used by a mobile application that is providing the consumer with directions on how to get to [a] specific location. A consumer's precise geolocation may not, however, be used by a gaming application where the average consumer would not expect the application to need this piece of sensitive personal information.

(2) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information. For example, a business may disclose a consumer's log-in information to a data security company that it has hired to investigate and remediate a data breach that involved that consumer's account.

(3) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions. For example, a business may use information about a consumer's ethnicity and/or the contents of email and text messages to investigate claims of racial discrimination or hate speech.

(4) To ensure the physical safety of natural persons. For example, a business may disclose a consumer's geolocation information to law enforcement to investigate an alleged kidnapping.

[. . .]

(6) To perform services on behalf of the business. For example, a business may use information for, such as maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.

(7) To verify or maintain the quality or safety of a product, service, or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the business. For example, a car rental business may use a consumer's driver's license for the purpose of testing that its internal text recognition software accurately captures license information used in car rental transactions.

(8) To collect or process sensitive personal information where such collection or processing is not for the purpose of inferring characteristics about a consumer.

For example, a business that includes a search box on their website by which consumers can search for articles related to their health condition may use the information provided by the consumer for the purpose of providing the search feature without inferring characteristics about the consumer.

Comment

The Privacy Law Section welcomes the additional language in section 7027(a) which clarifies, consistent with the statute, that sensitive personal information collected or processed without the purpose of inferring characteristics about a consumer is not subject to requests to limit. However, in making this clarification, the Agency did not align several of the use case examples in subsection (m), which attempt to illustrate the types of services a business may perform without needing to provide the right to limit. Specifically, as currently drafted, these examples describe uses of sensitive personal information that would never give rise to a right to limit in the first place because they depict uses that do not involve the generation of inferences. In other words, the example mixes apples (exceptions to right to limit sensitive information used to create inferences) and oranges (sensitive information used to deliver a service, but not to create an inference).

The inclusion of subsection (m)(8) adds to this confusion because it incorrectly suggests that the collection or processing of sensitive personal information not for the purposes of inferring characteristics is another type of use of sensitive information that is distinct from the other listed uses, such as verifying or maintaining the quality or safety of a product. However, it is not another type of use; it is a definition of the type of sensitive personal information that is out of scope for the statute. So, for example, if a business verifies the quality or safety of a product by using sensitive information without inferring characteristics, there is no right to limit.

We understand that the Agency may have simply taken language from sections of the statute verbatim when drafting this subsection of the regulations. However, Civil Code section 1798.121 is one of the more opaque sections of the statute and practitioners will be looking to regulations to provide much-needed clarity. The need for such clarity is exacerbated by the fact that the CCPA (as amended by CPRA) is the only state data privacy law that imposes restrictions on the processing of sensitive personal information only when it is used to generate inferences; other state laws (e.g., Colorado Privacy Act; Virginia Consumer Data Privacy Act) regulate sensitive personal information when it is used for any purpose whatsoever, not only inference generation.

To the extent the Agency chooses to include examples of the services that do not give rise to the right to limit, they should depict instances in which a business uses sensitive personal information to infer characteristics about an individual when providing such services. Without this clarification, the examples in this subsection are, at best, of no

utility, and, at worst, potentially confusing to practitioners by leading them to wrongly assume that the statute's provisions regarding sensitive personal information apply broadly (as is the case in other state data privacy laws), not as the statute provides: only when sensitive personal information is collected or processed to infer characteristics about a consumer. Civ. Code section 1798.121(d).

Proposed Alternative Language

§ 7027(m). The purposes identified in Civil Code section 1798.121, subdivision (a), 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, provided that the use or disclosure is reasonably necessary and proportionate for those purposes, is not required to post a Notice of Right to Limit or provide a method for submitting a request to limit.

- (1) To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services. ~~For example, a consumer's precise geolocation may be used by a mobile application that is providing the consumer with directions on how to get to [a] specific location. A consumer's precise geolocation may not, however, be used by a gaming application where the average consumer would not expect the application to need this piece of sensitive personal information.~~
- (2) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information. ~~For example, a business may disclose a consumer's log-in information to a data security company that it has hired to investigate and remediate a data breach that involved that consumer's account.~~
- (3) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions. ~~For example, a business may use information about a consumer's ethnicity and/or the contents of email and text messages to investigate claims of racial discrimination or hate speech.~~
- (4) To ensure the physical safety of natural persons. ~~For example, a business may disclose a consumer's geolocation information to law enforcement to investigate an alleged kidnapping.~~
- . . .
- (6) To perform services on behalf of the business. For example, a business may use information that infers characteristics about consumers for maintaining or

~~servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing or similar services on behalf of the business.~~

~~(7) To verify or maintain the quality or safety of a product, service, or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the business. For example, a car rental business may use a consumer's driver's license for the purpose of testing that its internal text recognition software accurately captures license information used in car rental transactions.~~

~~(8) To collect or process sensitive personal information where such collection or processing is not for the purpose of inferring characteristics about a consumer. For example, a business that includes a search box on their website by which consumers can search for articles related to their health condition may use the information provided by the consumer for the purpose of providing the search feature without inferring characteristics about the consumer.~~

§ 7053. Contract Requirements for Third Parties.

Rule

§ 7053(a). A business that sells or shares a consumer's personal information with a third party shall enter into an agreement with the third party that:

(1) Identifies the limited and specified purpose(s) for which the personal information is made available to the third party. The purpose shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.

[paragraphs (2)–(6) omitted]

Comments

The Privacy Law Sections suggests that the Agency use language throughout section 7053(a) that is consistent with the CPRA. Subsection (a)(1) is provided above as an example, but the Privacy Law Section's comment applies to subsections (a)(1) through (6). Following the 45-day comment period, the Agency replaced references to personal information that is "sold or disclosed" to a third party with references to data that is "made available" to the third party. Although the CPRA occasionally uses the terms "making available" or "disclosing" to refer to the transfer of personal information by a business, neither of those terms are defined. Instead, "making available" and "disclosing" are included as components of the defined terms "selling" and "sharing."

Because “selling” and “sharing” are defined terms and include both “making available” and “disclosing,” the Privacy Law Section urges the Agency to use the broader terms of “selling” and “sharing” with respect to third parties.

Propose Alternative Language

§ 7053(a). A business that sells or shares a consumer’s personal information with a third party shall enter into an agreement with the third party that Identifies the limited and specified purpose(s) for which the personal information is ~~made available to the third party~~ sold to or shared with a third party. The purpose shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.

[parallel revisions should be implemented in paragraphs (2)–(6)]

* * *

Respectfully submitted,

Privacy Law Section of the California Lawyers Association

From: Travis Frazier <[REDACTED]>
Sent: Sunday, November 20, 2022 12:51 PM
To: Regulations
Subject: CPPA Public Comment
Attachments: FINAL Joint Ad Trade Letter - Comments on Modifications to Proposed CPRA Regulations.pdf

Importance: High

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello,

Please find attached a joint comment from the following advertising trade associations in response to the California Privacy Protection Agency's request for comment on the modified proposed regulations to implement the California Privacy Rights Act of 2020: the Association of National Advertisers, the American Association of Advertising Agencies, the Interactive Advertising Bureau, the American Advertising Federation, and the Digital Advertising Alliance. We appreciate your consideration of this comment.

Regards,
Travis Frazier

Travis Frazier

Manager, Government Relations | [Association of National Advertisers \(ANA\)](#)

P: [REDACTED]
2020 K Street, NW, Suite 660, Washington, DC 20006

The ANA drives growth for you, your brand, our industry, and humanity. Learn how at ana.net/membership.

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

RE: Cross-Industry Advertising Trade Association Comments on the Modified Text of Proposed Regulations to Implement the California Privacy Rights Act of 2020 – CCPA Public Comment

Dear Privacy Regulations Coordinator:

On behalf of the thousands of brands, publishers, agencies and ad technology companies in our membership that represent the advertising industry, we provide the following comments in response to the California Privacy Protection Agency's ("CCPA" or "Agency") November 3, 2022 request for public comment on the modified text of proposed regulations to implement the California Privacy Rights Act of 2020 ("CPRA").¹ We and the companies we represent, many of which do substantial business in California, strongly believe consumers deserve meaningful privacy protections supported by reasonable laws and responsible industry policies. We appreciate the Agency's incorporation of certain input we provided during the 45-day comment period into the modified text of proposed rules. In this comment letter, we provide the Agency with further input and suggested changes to discrete proposed regulatory provisions to help ensure implementing regulations are consistent with the law and protect consumers while remaining workable for the business community.

We remain concerned that several provisions in the proposed regulations contravene the clear text of the CPRA. We addressed some of those concerns in our response to the Agency's initial request for comment on the proposed regulations. We renew several of those concerns—particularly with respect to the quickly approaching CPRA enforcement start date in the absence of finalized regulations; Section 7050; and the proposed opt-out icon—in [Appendix A](#). Additionally, in October 2022, we sent a letter to the Agency detailing some of our concerns related to opt-out preference signals and necessary and proportionate data processing requirements in the proposed rules. We advocated that the CCPA not advance those controversial regulatory provisions through an abridged or accelerated "consent agenda" process. That letter is attached hereto as [Appendix B](#). We discuss the points made therein, as well as an additional issue related to legal defenses under Section 7051(c), in more detail in the sections that follow below.

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country ranging from small businesses to household brands, long-standing and emerging publishers, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies that power the commercial Internet, which accounted for 12 percent of total U.S. gross domestic product ("GDP") in 2020.² Our group has more than a decade's worth of hands-on experience regarding matters related to consumer privacy and controls. We welcome the opportunity to engage with you in this process to develop practical regulations to implement the CPRA.

¹ California Privacy Protection Agency, *Notice of Modifications to Text of Proposed Regulations* (Nov. 3, 2022), located [here](#). See also California Privacy Rights Act of 2020, located [here](#) (hereinafter, "CPRA").

² John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 15 (Oct. 18, 2021), located [here](#) (hereinafter, "Deighton & Kornfeld 2021").

I. The Modified Proposed Regulations’ “Necessary and Proportionate” Requirements Should Be Amended To Align with the CPRA’s Text.

The “necessary and proportionate” data processing requirements in Section 7002 of the modified text of proposed regulations contradict the CPRA’s text. Section 7002 should be revised to implement the statute’s plain language and intent.

The modified proposed rules would completely eliminate the important, intended, and statutorily prescribed role of consumer notice within the CPRA framework. Instead of permitting businesses’ disclosures to consumers to determine necessary and proportionate data use as set forth in the CPRA, the modified proposed rules would require businesses to engage in a convoluted multi-factor analysis to determine whether certain data processing activities are permissible.³ If a proposed processing purpose does not adequately satisfy the factors, a business would be required to obtain consumer consent for data processing. In direct contrast to this rule, the CPRA itself sets forth an opt-out approach to *certain* data processing activities and does not mandate consumer consent for all data processing. And yet, Section 7002 suggests that the statutory opt-out approach could be converted to an opt-in requirement with all of the concomitant challenges associated with such a regime, such as the consent fatigue and anti-competitive concerns associated with the EU’s General Data Protection Regulation (“GDPR”).⁴ Section 7002 of the modified proposed rules thus turns the CPRA’s approach on its head, is contrary to the law’s text, and diametrically opposes the privacy framework that California voters directly approved when they approved the CPRA ballot initiative.

A. Section 7002 Should Be Modified to Permit Data Processing Described in Consumer Disclosures Instead of Requiring a Subjective Multi-Factor Analysis.

In addition to several other factors, the modified proposed rules would require businesses to consider the “reasonable expectation of the consumer” to determine whether data processing is permitted. The modified proposed rules then provide examples of activities that would or would not meet this standard without referencing any basis for those conclusions, such as consumer testing or research, or even real-world observations of actual consumer behavior. This “reasonable expectation of the consumer” consideration, along with the other factors articulated in the modified proposed rules, would require businesses to make similar amorphous and highly subjective determinations about allowed processing activity. It also vests in the Agency a high level of subjectivity which is likely not to have been contemplated by the voters or by the California APA. In contrast, the CPRA itself provides clear standards for permissible data processing tied to consumer notice. The CPRA specifically allows businesses to process data for uses described in their privacy notices, including uses that are consistent and compatible with the businesses’ disclosures.⁵ The CPRA explicitly articulates highly specific standards for consumer disclosures related to the type of personal information processed, the purpose(s) for processing, the categories of entities to which personal information is sold or shared, and the sources of personal information. These specific disclosure requirements were included in the law to ensure businesses act in furtherance of the CPRA’s stated purposes of helping consumers “become more informed counterparties in the data economy, and promot[ing] competition.”⁶ The modified proposed regulations ignore the important and statutorily provided role of consumer notice plays in the law and substitute the Agency’s views of how the CPRA text *should* read rather than honoring and furthering the letter of the law itself.

³ Cal. Code Regs. tit. 11, § 7002 (proposed).

⁴ See Kate Fazzini, *Europe’s sweeping privacy rule was supposed to change the internet, but so far it’s mostly created frustration for users, companies, and regulators* (May 5, 2019) located [here](#).

⁵ CPRA, Cal. Civ. Code § 1798.100(c) (effective Jan. 1, 2023).

⁶ *Id.* at § 2(G).

The modified proposed regulations run counter to the CPRA's text and purpose by requiring businesses to engage in a highly subjective analysis in order to proceed with data processing that has already been disclosed to consumers according to the CPRA's notice requirements.⁷ Such an approach would stifle innovation by subjecting product and service innovation to consent, which is not workable. The factor-based test would also require businesses to presuppose preferences according to each consumer's perceived "reasonable expectations," resulting in diminished choice and autonomy for consumers. The CPRA does not envision this sort of framework, but instead strives to leverage consumer disclosures to educate consumers so they can make meaningful choices about how personal information is processed.⁸

Instead of issuing regulations that plainly contradict the CPRA, the Agency should permit controllers to process personal data in line with the specified processing purposes disclosed to consumers.⁹ Only when a controller wishes to process personal data for purposes that are undisclosed should the business be required to consider a series of factors to determine if such processing is permissible.¹⁰ This approach provides much more clarity to businesses and consumers alike, as it relies on bright line, clear consumer disclosures to define the permissible purposes for data processing. Additionally, such an approach would align with the CPRA, which permits data processing if the processing is adequately disclosed to the consumer and provides an opt-out structure for certain processing activities rather than requiring consumer consent.

B. Amending Section 7002 To Permit Processing In Line With Disclosures Would Prevent Converting the CPRA's Opt-Out Structure Into an Opt-In Framework.

The CPRA clearly permits data processing that aligns with businesses' disclosures to consumers. It also allows for consumers to opt out of certain data processing activities. The law itself does not require businesses to engage in subjective, multi-factor analyses to determine if they may process data in certain ways. The CPRA also sets forth an opt-out structure for certain data processing and does not require consumer consent. Section 7002's consent requirements would consequently completely convert the fundamental opt-out structure of the CPRA into an opt-in law; this would not further the intent and purpose of the statute. Moreover, by requiring businesses to make decisions about data processing that would be "necessary and proportionate" according to each consumer's "reasonable expectations," the modified proposed regulations inject an unnecessary and unhelpful level of ambiguity into businesses' ability to determine whether certain data processing is permissible. The CPRA itself puts autonomy in the hands of consumers by placing the responsibility on businesses to inform and educate, not gate-keep by eliminating consumer choices altogether. The modified proposed regulations should be revised to ensure businesses can process personal information in line with CPRA-compliant consumer disclosures without requiring an unnecessarily chilling and uncertain multi-factor analysis to determine permissible data processing. Accordingly, Section 7002 of the modified regulations should be updated to align with the CPRA and avoid reaching beyond its mandates.

II. The Modified Regulations Should Follow the CPRA by Clarifying That Opt-Out Preference Signals Are Optional, Implementing Statutorily Required Safeguards to Authenticate Signals, and Providing Technical Specifications for Signals.

The CCPA should align the regulatory text surrounding opt-out preference signals with the CPRA itself. Prior to finalizing the regulations, the Agency should also take steps to promulgate rules

⁷ Cal. Code Regs. tit. 11, §§ 7002(b), (c) (proposed).

⁸ See CPRA, § 2(G) (effective Jan. 1, 2023)..

⁹ Colo. Regs. 6.08A, located [here](#) (proposed).

¹⁰ *Id.* at 6.08(C).

to further several key safeguards for such signals, as well as to define technical specifications for the signals so businesses know how to recognize and implement the opt-out signals they may receive, as discussed in **Appendix B**. The CPPA should also take steps to help standardize opt-out preference signal tools so businesses and consumers understand which tools meet the requirements of law. As presently drafted, the regulatory text directly contravenes the CPRA by making adherence to opt-out preference signals mandatory, and it ignores clear requirements for the Agency to promulgate specific regulations addressing safeguards and technical specifications for opt-out preference signals.

A. The CPRA Makes Opt-Out Preference Signals Optional.

The CPRA clearly states that businesses “may elect” to comply with opt-out preference signals or include a clearly labeled opt-out link in the footer of their websites.¹¹ The modified proposed rules contradict this statutory language by stating that processing such signals is mandatory.¹² The modified proposed regulations ignore clear language in the law that makes opt-out preference signals optional. Instead, the modified proposed rules suggest that a business is mandated to honor opt-out preference signals in either a “frictionless” or “non-frictionless manner,” terms that are not in the text of the CPRA itself.¹³ The modified regulations’ “frictionless” standard is extra-legal, as it is not supported by the text of the CPRA; it directly contravenes the law, which clearly makes adherence to opt-out preference signals optional.

To support making adherence to opt-out preference signals mandatory, the Agency’s Initial Statement of Reasons (“ISOR”) for the proposed rules cites the regulatory authority given to the Agency in Section 1798.185(a)(20) of the CPRA.¹⁴ According to the ISOR, adherence to opt-out preference signals is mandatory because the statute gives the Agency authority to issue rules governing how a business may provide consumers with an opportunity to subsequently consent to sales or sharing of personal information.¹⁵ This reasoning does not describe why the Agency has gone beyond the plain text of the law by instituting a mandatory standard instead of the clear, optional choice the CPRA envisions with respect to such signals. Moreover, it entirely ignores the fact that the regulatory directive in Section 1785.185(a)(20) itself even acknowledges that adherence to opt-out preference signals is optional. According to that section, the Agency must issue “regulations to govern how a business that has elected to comply with subdivision (b) of Section 1798.135,” the subdivision that describes opt-out preference signals, “responds to the opt-out preference signal.”¹⁶ By making adherence to opt-out preference signals mandatory, the Agency has ignored the clear text of the CPRA. The Agency should rewrite its opt-out preference signal regulations to reflect the CPRA’s provisions, which explicitly give businesses a choice to process such signals or offer a clearly labeled opt-out link in the footers of their websites.

B. The CPRA Requires the Agency to Address Key Safeguards and Technical Specifications for Opt-Out Preference Signals.

The Agency’s proposed opt-out preference signal rules fail to implement key provisions of the CPRA that require the CPPA to set guardrails around the development of optional opt-out preference signals and provide technical standards for such signals to clarify developers’ design obligations. The CPRA specifically tasks the Agency with “issuing regulations to define the requirements and *technical*

¹¹ CPRA, Cal. Civ. Code § 1798.135(b)(3) (effective Jan. 1, 2023).

¹² Cal. Code Regs. tit. 11, §§ 7025(b), (e) (proposed).

¹³ *Id.* at § 7025(e).

¹⁴ California Privacy Protection Agency, *Initial Statement of Reasons* at 34-35, located [here](#).

¹⁵ *Id.*

¹⁶ CPRA, Cal. Civ. Code § 1798.185(a)(20) (effective Jan. 1, 2023) (emphasis added).

specifications for an opt-out preference signal,” which would ensure the signal meets several safeguards: the signal (1) cannot unfairly disadvantage certain businesses in the ecosystem; (2) must be clearly described; (3) must clearly represent a consumer’s intent and be free of defaults presupposing such intent; (4) must not conflict with commonly-used privacy settings consumers may employ; (5) must provide a mechanism for consumers to consent to sales or sharing without affecting their preferences with respect to other businesses; and (6) must provide granular opt-out options for consumers.¹⁷ Not one of these key safeguards—which are explicitly in the text of the CPRA and which the Agency is instructed to effectuate via regulations—is addressed in the proposed rules, nor are there any proposed rules that would define technical standards for opt-out preference signals. These safeguards and technical specifications are necessary to clarify how developers must construct opt-out preference signal tools.

As written, the modified proposed regulations would create widespread confusion, because they do not clarify how opt-out preference signals can meet the safeguards requirements that are set forth in law, and they do not clarify how businesses can technically implement the ability to receive opt-out preference signals. Moreover, the modified proposed rules inject additional uncertainty into the opt-out preference signal requirements by adding an unnecessary reference to “pseudonymous profiles.” This is new term that is not defined by the CPRA or the proposed regulations.¹⁸ In this way and others, the modified proposed regulations do not set forth clear directives related to opt-out preference signals, call for any standardization of such signals, or specify how businesses are to know which opt-out signals are valid under the statute. Effectuating new signals will be a development project for many organizations, which requires months of lead time. Without sufficient lead time and specificity regarding which signals are to be respected, organizations will be left guessing or subject to security risks or consumer dissatisfaction when the mechanism does not work or is not seamlessly integrated into the online experience, thus opening up well-intentioned efforts to unnecessary liability.

C. The Agency Should Maintain a List of Approved Opt-Out Preference Tools to Reduce Consumer and Business Confusion.

To help clarify which in-market opt-out preference tools meet the requirements of the CPRA (*i.e.*, are not set by default, do not disadvantage certain businesses or models of others, etc.), the Agency should maintain a public list of recognized mechanisms that have met legal standards.¹⁹ Such a centralized repository of approved signals would benefit consumers and businesses alike. Consumers would be able to understand which opt-out preference signals are approved by the Agency and thus represent a control mechanism that must be given effect by businesses. In turn, businesses would gain clarity regarding which opt-out preference signals they must honor instead of having to constantly monitor the Internet for any in-market mechanism and independently validate or check its legality. Such a list would reduce the need for businesses to guess which signals are true expressions of consumer choice.

Regulations furthering the CPRA’s opt-out preference signal safeguards are necessary to ensure businesses can verify that the signal, or the “mechanism” or “tool” that provides the signal, has complied with various requirements under the CPRA, including those related to presentation of choices, default settings, disadvantages to businesses, and reflection of consumer intent. Similarly, technical specifications would help developers understand their design obligations with respect to opt-out preference signal tools. The Agency must first address these statutory requirements concerning mechanisms that set opt-out preference signals before adopting regulations related to honoring such

¹⁷ *Id.* at § 1798.185(a)(19)(A).

¹⁸ Cal. Code Regs. tit. 11, §§ 7025(c)(1), (2) (proposed).

¹⁹ See Colo. Regs. 5.07, located [here](#) (proposed).

signals. Guidance from the Agency to govern the mechanisms used to set signals is necessary to ensure such tools are offered in compliance with law and so businesses receiving such signals can be assured that the signals are legally set consumer preferences.

III. Businesses Should Be Required to Conduct Due Diligence of Service Providers and Contractors Only If They Reasonably Believe Such Entities Are Misusing Personal Information.

The modified proposed regulations in Section 7051(c) states that a business “might” not be permitted to rely on a defense that it did not have reason to believe a service provider or contractor intends to use personal information in violation of the CCPA if the business does not enforce the terms of its contracts or exercise rights to audit or test service providers’ and contractors’ systems.²⁰ This provision would create significant costs for businesses without providing any real benefit to consumers. If left unchanged, the provision could effectively force businesses to audit and test every one of their partners’ systems, thereby creating immense costs and the anticompetitive result of businesses limiting the number of service providers or contractors with which they do business. A better approach would be to rewrite the draft regulation to make clear that a business may not be permitted to avail itself of the defense if it *has reason to believe* a service provider or contractor is using personal information in violation of the CCPA and the business does not take steps to investigate that belief. The proposed rules should be updated to encourage businesses to take steps to exercise diligence when they have reason to believe a partner is using personal information in violation of the CCPA or the applicable contract.

IV. Sufficient Consideration Should Be Given to the Data-Driven and Ad-Supported Online Ecosystem That Benefits California Residents and Fuels Economic Growth.

Over the past several decades, data-driven advertising has created a platform for innovation and tremendous growth opportunities. A recent study found that the Internet economy’s contribution to the United States’ GDP grew 22 percent per year since 2016, in a national economy that grows between two to three percent per year.²¹ In 2020 alone, it contributed \$2.45 trillion to the U.S.’s \$21.18 trillion GDP, which marks an eightfold growth from the Internet’s contribution to GDP in 2008 of \$300 billion.²² Additionally, more than 17 million jobs in the U.S. were generated by the commercial Internet in 2020, 7 million more than four years prior.²³ More Internet jobs, 38 percent, were created by small firms and self-employed individuals than by the largest Internet companies, which generated 34 percent.²⁴ The same study found that the ad-supported Internet supported 1,096,407 full-time jobs across California, more than double the number of Internet-driven jobs from 2016.²⁵

A. Advertising Fuels Economic Growth.

Data-driven advertising supports a competitive online marketplace and contributes to tremendous economic growth. Overly restrictive regulations that significantly hinder certain

²⁰ Cal. Code Regs. tit. 11, § 7051(c)(proposed).

²¹ Deighton & Kornfeld 2021 at 5.

²² *Id.*

²³ *Id.*

²⁴ *Id.* at 6. See also Digital Advertising Alliance, *Summit Snapshot: Data Drives Small-and Mid-sized Business Online, It’s Imperative that Regulation not Short-Circuit Consumer Connections* (Aug. 17, 2021), located [here](#).

²⁵ Compare Deighton & Kornfeld 2021. at 121-123 (Oct. 18, 2021), located [here](#) with John Deighton, Leora Kornfeld, and Marlon Gerra, *Economic Value of the Advertising-Supported Internet Ecosystem*, INTERACTIVE ADVERTISING BUREAU, 106 (2017), located [here](#) (finding that Internet employment contributed 478,157 full-time jobs to the California workforce in 2016 and 1,096,407 jobs in 2020).

advertising practices, such as third-party tracking, could yield tens of billions of dollars in losses for the U.S. economy—and, importantly, not just in the advertising sector.²⁶ One recent study found that “[t]he U.S. open web’s independent publishers and companies reliant on open web tech would lose between \$32 and \$39 billion in annual revenue by 2025” if third-party tracking were to end “without mitigation.”²⁷ That same study found that the lost revenue would become absorbed by “walled gardens” or entrenched market players, thereby consolidating power and revenue in a small group of powerful entities.²⁸ Smaller news and information publishers, multi-genre content publishers, and specialized research and user-generated content would lose more than an estimated \$15.5 billion in revenue.²⁹ Data-driven advertising has thus helped to stratify economic market power and foster competition, ensuring that smaller online publishers can remain competitive with large global technology companies.

B. Advertising Supports Californians’ Access to Online Services and Content.

In addition to providing economic benefits, data-driven advertising subsidizes the vast and varied free and low-cost content that publishers offer consumers through the Internet, including public health announcements, news, and cutting-edge information. Advertising revenue is an important source of funds for digital publishers,³⁰ and decreased digital advertising budgets directly translate into lost profits for those outlets. Revenues from online advertising based on the responsible use of data support the cost of content that publishers provide and consumers value and expect.³¹ In fact, consumers valued the benefit they receive from digital advertising-subsidized online content at \$1,404 per year in 2020—a 17% increase from 2016.³² Regulatory frameworks that inhibit or restrict digital advertising can cripple news sites, blogs, online encyclopedias, and other vital information repositories, and these unintended consequences also translate into a new tax on consumers. The effects of such regulatory frameworks ultimately harm consumers by reducing the availability of free or low-cost educational content that is available online.

C. Consumers Prefer Personalized Ads & Ad-Supported Digital Content and Media.

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. One study found more than half of consumers (53 percent) desires relevant ads, and a significant majority (86 percent) desires tailored discounts for online products and services.³³ Additionally, in a recent Zogby survey conducted by the Digital Advertising Alliance, 90 percent of consumers stated that free content was important to the overall value of the Internet and 85 percent surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers

²⁶ See John Deighton, *The Socioeconomic Impact of Internet Tracking* 4 (Feb. 2020), located [here](#) (hereinafter, “Deighton 2020”)

²⁷ *Id.* at 34.

²⁸ *Id.* at 15-16. See also Damien Geradin, Theano Karanikioti & Dimitrios Katsifis, *GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech*, EUROPEAN COMPETITION JOURNAL (Dec, 18, 2020), located [here](#).

²⁹ Deighton 2020 at 28.

³⁰ See Howard Beales, *The Value of Behavioral Targeting* 3 (2010), located [here](#).

³¹ See John Deighton & Peter A. Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the US Economy* (2015), located [here](#).

³² Digital Advertising Alliance, *Americans Value Free Ad-Supported Online Services at \$1,400/Year; Annual Value Jumps More Than \$200 Since 2016* (Sept. 28, 2020), located [here](#).

³³ Mark Sableman, Heather Shoenberger & Esther Thorson, *Consumer Attitudes Toward Relevant Online Behavioral Advertising: Crucial Evidence in the Data Privacy Debates* (2013), located [here](#).

must pay for most content.³⁴ Indeed, as the Federal Trade Commission noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.³⁵

V. Conclusion

During challenging societal and economic times such as those we are experiencing, laws that restrict access to information and economic growth can have lasting and damaging effects. The ability of consumers to provide, and companies to responsibly collect and use, consumer data has been an integral part of the dissemination of information and the fabric of our economy for decades. The collection and use of data are vital to our daily lives, as much of the free and low-cost content we consume over the Internet is powered by open flows of information supported by advertising. We therefore respectfully urge you to carefully consider the proposed regulations' potential impact on advertising, the consumers who reap the benefits of such advertising, and the overall economy as you continue to refine the draft rules.

* * *

Thank you in advance for your consideration of this letter.

Sincerely,

Christopher Oswald
EVP, Government Relations
Association of National Advertisers
[REDACTED]

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's
[REDACTED]

Lartase Tiffith
Executive Vice President for Public Policy
Interactive Advertising Bureau
[REDACTED]

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
[REDACTED]

Lou Mastria, CIPP, CISSP
Executive Director
Digital Advertising Alliance
[REDACTED]

CC: Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP

³⁴ Digital Advertising Alliance, *Zogby Analytics Public Opinion Survey on Value of the Ad-Supported Internet Summary Report* (May 2016), located [here](#).

³⁵ Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located [here](#).

APPENDIX A

Additional Concerns Regarding the Modified Proposed Regulations to Implement the CPRA

I. The CPPA Should Delay Enforcement for One Year Following Finalization of Regulations.

As noted in our prior filings, the CPRA requires the Agency to finalize regulations implementing the law by July 1, 2022, providing businesses a full calendar year to ensure compliance before enforcement would begin on July 1, 2023.³⁶ Unfortunately, the statutorily-required date for finalized rules has long passed; regulations are still being developed nearly six months after the July 1, 2022 deadline. In addition, even once the Agency completes its rulemaking process, finalization of regulations is contingent on satisfactory review by the California Office of Administrative Law (“OAL”).³⁷ Given the California Administration Procedure Act’s (“CA APA”) rolling effective dates for regulations, OAL-approved regulations may not be finalized until 2023.³⁸ Thus, business stakeholders not only remain uncertain about what measures may be needed to comply with forthcoming final regulations, but also may face an impossibly tight compliance deadline before the Agency begins enforcement. The potentially very late publication of the final rules may also confuse consumers who will be given a much shorter ramp up time to learn about how take advantage of their rights in line with the new rules’ procedures. The companies we represent are eager to ensure compliance with forthcoming final regulations, but as the CPRA’s statutory timeline acknowledged, will need sufficient time to do so.

Given the ongoing rulemaking process and the additional requirements of the CA APA, the Agency should wholly align with the CPRA by stating expressly in final regulations that it will not pursue enforcement until one year after regulations are finalized. We appreciate the Agency’s acknowledgement that it will consider the “amount of time” between statutory and regulatory effective dates and the dates of alleged violations in determining whether to pursue investigatory actions.³⁹ An additional definitive statement in the regulations explicitly committing the Agency to delay enforcement for one year would not only align with the CPRA, but also would provide needed clarity for business and consumer stakeholders.

II. Section 7050(b) is Duplicative of the CPRA and Should Be Removed From the Modified Proposed Regulations.

Because Section 7050(b) of the modified proposed regulations merely restates the CPRA and provides no additional clarity, the section should be removed. Section 7050(b) of the modified proposed regulations reaffirms the CPRA’s text, which prohibits companies from offering cross-context behavioral advertising services to businesses while occupying the “service provider” role.⁴⁰ Section 7050(b) of the modified proposed regulations simply reiterates the law, which plainly permits entities to provide advertising and marketing services to businesses as “service providers,” and even permits them to combine personal information for advertising and marketing purposes in some circumstances so long as they do not “combine the personal information of opted-out consumers that the service provider... receives from, or on behalf of, the business with personal information that the service provider receives from, or on behalf of, another person or persons or collects from its own

³⁶ CPRA, Cal. Civ. Code § 1798.185(d) (effective Jan. 1, 2023).

³⁷ Cal. Gov’t. Code §§ 11349.1, 11349.3.

³⁸ *Id.* at § 11343.4.

³⁹ Cal. Code Regs. tit. 11, § 7301(b) (proposed).

⁴⁰ CPRA, Cal. Civ. Code § 1798.140(e)(6) (effective Jan. 1, 2023).

interactions with consumers.”⁴¹ The text used in Section 7050(b) of the modified proposed regulations is virtually identical to the text of the CPRA on this point. Because the modified proposed regulation restates the CPRA provision explaining that an entity may provide advertising and marketing services as a service provider, but may not engage in cross-context behavioral advertising (the targeting of advertisements to consumers based on personal information combined from multiple businesses),⁴² Section 7050(b) adds no additional clarity to the CPRA and should thus be removed from the modified proposed regulations.

III. The Modified Proposed Regulations Should Permit Businesses to Leverage Existing In-Market Icons and Choice Mechanisms.

Under the CPRA, businesses are permitted to offer a “single, clearly-labeled link” to enable consumers to easily opt out of the sale or sharing of personal information and limit the use or disclosure of sensitive personal information instead of posting separate ‘Do Not Sell or Share My Personal Information’ and ‘Limit the Use of My Sensitive Personal Information’ links.”⁴³ The proposed rules would require the title for that “Alternative Opt-out Link” to be “Your Privacy Choices” or “Your California Privacy Choices,” and would require it to direct a consumer to a webpage that enables them to make choices to opt out of sales, opt out of sharing, and limit the use and disclosure of sensitive personal information.⁴⁴ For entities that use such an Alternative Opt-out Link,” the proposed regulations would require them also to include the following graphic adjacent to the link:



The proposed graphic icon is confusing. Its inclusion of just one check mark and one “x” suggests just *one choice* will be made via the alternative opt-out link, when in reality the link would provide consumers the ability to make three choices: (1) the choice to opt out of personal information sales; (2) the choice to opt out of personal information sharing; and (3) the choice to limit the use and disclosure of sensitive personal information. The study used to support the use of the Agency’s chosen icon found that several different icons (including the DAA Privacy Rights Icon) performed roughly the same when paired with a text link.⁴⁵ The market should be permitted to determine icons that work best to facilitate awareness and effectuation of rights for consumers. The CPPA should remove the prescriptive opt-out icon requirement and instead allow the marketplace to continue to leverage new and existing, widely deployed iconography provided the mandatory language for the link—“Your Privacy Choices” or “Your California Privacy Choices”—is present.⁴⁶

* * *

⁴¹ *Id.*

⁴² *Id.* at § 1798.140(k).

⁴³ CPRA, Cal. Civ. Code 1798.135(a)(3) (effective Jan. 1, 2023).

⁴⁴ Cal. Code Regs. tit. 11, § 7015(b) & (c) (proposed).

⁴⁵ Lorrie Faith Cranor, et. al., *Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA* at 27 (Feb. 4, 2020), located [here](#).

⁴⁶ See, e.g., Digital Advertising Alliance, *YourAdChoices*, located [here](#).



October 19, 2022

Chairperson Jennifer M. Urban
California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834

Board Member Chris Thompson
California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834

Board Member Lydia de la Torre
California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834

Board Member Vinhcent Le
California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834

Board Member Alastair Mactaggart
California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834

Executive Director Ashkan Soltani
California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834

RE: Joint Ad Trade Comments on the CPPA's Proposed Consent Agenda to Resolve "Non-Controversial" Issues in the CPRA Rulemaking Process

Dear California Privacy Protection Agency Board Members and Executive Director Ashkan Soltani:

On behalf of the advertising industry, we respectfully urge the California Privacy Protection Agency ("CPPA" or "Agency") to decline to consider or approve certain controversial regulatory provisions through a "consent agenda" process to expedite the proposed regulations implementing the California Privacy Rights Act of 2020 ("CPRA"). During the CPPA's September 23 meeting, the Agency expressed interest in placing certain regulatory provisions on a consent agenda for "non-controversial" issues. Shortly thereafter, the Agency published modified proposed regulations to implement the CPRA.¹ There are several issues in the modified proposed regulations that are controversial and unsettled, and therefore should not qualify for any potential consent agenda. Specifically, the following two areas are particularly in need of further discussion and consideration, as they were not addressed by the modifications to the proposed regulations and remain controversial:

- I. Proposed regulations related to opt-out preference signals are missing statutorily mandated safeguards; and
- II. Consumer notice should fulfill the CPRA's "necessary and proportionate" requirements rather than tying "necessary and proportionate" processing requirements to "average" or "reasonable" consumer expectations.

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country and in California. These companies range

¹ CPPA, *Modified Text of Proposed Regulations*, located [here](#).

from small businesses to household brands, long-standing and emerging publishers, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies that power the commercial Internet, which accounted for 12 percent of total U.S. gross domestic product (“GDP”) in 2020.² Our group has more than a decade’s worth of hands-on experience relating to matters involving consumer privacy and controls. We and the companies we represent, many of whom do substantial business in California, strongly believe consumers deserve meaningful privacy protections supported by reasonable laws and responsible industry policies. We have participated in every proceeding under this CPRA rulemaking, including filing comments in response to the initial draft of proposed regulations. We welcome the opportunity to continue to engage with you to develop regulations to implement the CPRA.

I. The Issue of Opt-Out Preference Signals Is Unfit for a Potential Consent Agenda Given Outstanding and Unaddressed Statutorily Required Safeguards

As the current proposed regulations do not address important statutory safeguards for opt-out preference signals that the CPRA requires, the issue of opt-out preference signals remains controversial and should not be summarily settled via consent agenda consideration. Under the CPRA, the Agency *must* promulgate specific rules to define the scope and form of opt-out preference signals. Specifically, the regulations must “define the requirements and technical specifications for an opt-out preference signal . . . The requirements and specifications for the opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses, and should” ensure the signal meets several safeguards: (1) avoids unfairly disadvantaging certain businesses or business models over others in the ecosystem, (2) is clearly described; (3) clearly represents a consumer’s intent and does not employ defaults that presuppose such intent; (4) does not conflict with commonly-used privacy settings consumers may employ; (5) provides a mechanism for consumers to consent to sales or sharing without affecting their preferences with respect to other businesses; and (6) provides granular opt-out options for consumers.³

The statute requires CPRA implementing regulations to include such safeguards while “considering the legitimate operational interests of businesses.”⁴ However, such technical specifications and safeguards appear nowhere in the current proposed regulations.⁵ If the Agency has not resolved where it stands on these statutorily mandated details or made them available for review by interested parties, the issue of opt-out preference signals cannot fairly be considered undisputed or proper for a consent agenda.

The lack of clarity about opt-out preference signals is further exacerbated by a possible truncated window between finalized CPRA implementing regulations and their enforcement date. The CPRA tasks the Agency with finalizing the regulations implementing the law by July 1, 2022, but unfortunately this deadline passed without the Agency issuing final regulations.⁶ Yet,

² John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 15 (Oct. 18, 2021), located [here](#) (hereinafter, “Deighton & Kornfeld 2021”).

³ Cal. Civ. Code § 1798.185(a)(19)(A) (effective Jan. 1, 2023).

⁴ *Id.* at § 1798.185(a)(19)(C).

⁵ See, e.g., Cal. Code Regs. tit. 11, § 7025 (proposed).

⁶ Cal. Civ. Code § 1798.185(d) (effective Jan. 1, 2023).

enforcement of the CPRA regulations could begin on July 1, 2023.⁷ Such an enforcement timeline would grant businesses less than the statutorily intended one-year period to bring themselves into compliance with new regulatory provisions, including provisions on the novel and technically complex subject of opt-out preference signals. The lingering ambiguity surrounding these signals, coupled with a potentially shortened enforcement window, highlights the importance of the statute's intent that the Agency first promulgate proposed regulations that address all statutorily required terms before mandating that businesses comply.

II. The Proposed Regulations Overlook the CPRA's Recognition of Consumer Notice as a Valid Basis for Data Use, Presenting a Significant Dispute

The CPRA sets out permissible business purposes for data use *and expressly* states personal information may be used for “other notified purposes.”⁸ Despite this statutory text, the proposed regulations introduce an “average” or “reasonable” consumer expectation standard that would make consumer notice obsolete under the statute.⁹ The disharmony between the statutory text of the CPRA and well-established consumer privacy principles and what the proposed rules set forth underscores the importance of addressing this issue completely in regular order and not via a consent agenda. The issue deserves a thorough discussion of the benefits of permitting businesses' data use consistent with their notices to consumers, as well as an explanation of the Agency's perceived authority to contravene a standard stated clearly in the text of the CPRA itself.

III. Conclusion

We and our members strongly support protecting consumer choice and privacy and preserving responsible data use by commercial businesses operating in California. Given the discussion during the Agency's September 23 meeting, we urge you to refrain from considering the matters we have mentioned above during any condensed consent agenda process. We will continue to raise these and other critical points in future comments to the CCPA so they may hopefully help to facilitate the CCPA's rulemaking proceedings. Again, we thank you for the opportunity to participate in the CPRA rulemaking process.

* * *

⁷ *Id.*

⁸ “A business's collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, *or for another disclosed purpose* that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.” *Id.* at §§ 1798.100(c), 140(e).

⁹ The proposed regulations would require “a business's collection, use, retention, and/or sharing” of personal information to be “reasonably necessary and proportionate to achieve... the purpose(s) for which the personal information was collected or processed... [or] another disclosed purpose that is compatible with the context in which the personal information was collected...” Cal. Code Regs. tit. 11, § 7002(a) (proposed). Both permitted uses of personal information require a consideration of average or “reasonable” consumer expectations. *Id.* at §§ 7002(b); (c)(1).

Thank you in advance for consideration of this letter.

Sincerely,

Christopher Oswald
EVP, Government Relations
Association of National Advertisers
[REDACTED]

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's
[REDACTED]

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
[REDACTED]

Lartease Tiffith
Executive Vice President for Public Policy
Interactive Advertising Bureau
[REDACTED]

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
[REDACTED]

Lou Mastria, CIPP, CISSP
Executive Director
Digital Advertising Alliance
[REDACTED]

CC: Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP

From: Kate Goodloe <[REDACTED]>
Sent: Sunday, November 20, 2022 2:54 PM
To: Regulations
Cc: Olga Medina; Matthew Lenz; Abigail Wilson
Subject: CPPA Public Comment - BSA | The Software Alliance
Attachments: 2022.11.20 - BSA Comments on Modified Regulations - Final.pdf

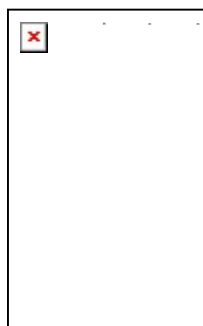
WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Mr. Soublet,

BSA | The Software Alliance appreciates the opportunity to submit comments regarding the modified text of the proposed regulations implementing the California Privacy Rights Act of 2020. Please find our comments attached. We welcome an opportunity to further engage with the CPPA on these important issues.

Best,

Kate Goodloe



Kate Goodloe
Senior Director, Policy
BSA | The Software Alliance
P [REDACTED]
W bsa.org





BSA | The Software Alliance

Submission to the California Privacy Protection Agency on Modified Proposed Regulations Implementing the Consumer Privacy Rights Act of 2020

BSA | The Software Alliance appreciates the opportunity to submit comments regarding the modified text of the proposed regulations (“Modified Proposed Regulations”) implementing the California Privacy Rights Act of 2020 (“CPRA”), which amended the California Consumer Privacy Act (“CCPA”). We appreciate the California Privacy Protection Agency’s (“CPPA’s”) work to address consumer privacy and to develop regulations that protect the privacy of Californians’ personal information.

BSA is the leading advocate for the global software industry before governments and in the international marketplace.¹ Our members are enterprise software companies that create the technology products and services that power other businesses. They offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, and collaboration software.

Businesses entrust some of their most sensitive data — including personal information — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members’ operations. Indeed, many businesses depend on BSA members to help them better protect privacy and our companies compete to provide privacy-protective products and services. BSA members recognize that companies must earn consumers’ trust and act responsibly with their data, and their business models do not depend on monetizing users’ personal information.

Our comments focus on three aspects of the Modified Proposed Regulations:

1. **Role of Service Providers.** The CCPA recognizes that businesses and service providers play different roles in protecting consumer privacy — and are therefore assigned different obligations under the statute based on their different relationships with consumers. We appreciate a range of changes made in the Modified Proposed Regulations to better reflect these distinct roles. However, we strongly suggest revising three aspects of the Modified Proposed Regulations to carry those changes throughout the regulations. First, the Modified Proposed Regulations should be revised to further clarify a service provider’s role in responding to consumer rights requests — including by continuing to recognize that service providers may fulfill their

¹ BSA’s members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Prokon, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

role of assisting businesses by creating tools that enable a business to respond to consumer rights requests for data held by the service provider. Second, the Modified Proposed Regulations should avoid creating data minimization obligations that depend on a consumer expectations about the role of service providers or how “apparent” a service provider’s activity is to consumers. Third, the contractual requirements for service providers in the Modified Proposed Regulations should be revised to align with the CCPA’s statutory text.

2. ***Global Opt-Out Mechanism.*** The CPPA is tasked with issuing regulations to implement a global opt-out mechanism. Although we believe the CCPA is best read to permit (but not require) companies to honor requests submitted through global opt-out mechanisms, it is critical that any opt-out mechanism recognized by the Modified Proposed Regulations (whether mandatory or voluntary) be interoperable with mechanisms recognized by other states and function in practice. Accordingly, the Modified Proposed Regulations should account for potentially conflicting opt-out requirements and the CPPA should work with other state regulators to ensure that opt-out requirements are consistent across state lines. We also strongly recommend the CPPA prioritize addressing practical issues around implementing opt-out mechanisms, including how businesses are to determine a mechanism meets the CCPA’s requirements. For example, one way to address such concerns is for the CPPA to publish a list of the signals that meet CCPA’s requirements and thus identify the mechanisms that businesses should honor.
3. ***Agency Audits.*** The Modified Proposed Regulations provide few details on the agency’s audit authority — and create few guardrails to ensure the agency exercises its audit authority in a manner that does not inadvertently create privacy and security risks. We recommend revising the Modified Proposed Regulations to create such guardrails, including limiting the use of on-site audits, which can present significant privacy and security risks not accounted for in the Modified Proposed Regulations.

I. Role of Service Providers

Although the CCPA primarily focuses on businesses, which “determine[] the purposes and means of the processing of consumers’ personal information,”² the statute also recognizes that businesses may engage service providers to “process[] personal information on behalf of a business.”³ Service providers must enter into written contracts with businesses they serve, limiting how the service provider can retain, use, and disclose personal information provided to them by a business. In this way, the CCPA ensures that personal information is subject to statutory protections both when a business collects and processes a consumer’s personal information itself, and when that business hires service providers to process a consumer’s personal information on its behalf. The statute also recognizes the distinct roles of businesses and service providers by assigning them different obligations based on their different roles in handling consumers’ personal information.

We urge three types of revisions to the Modified Proposed Regulations to better reflect the role of service providers, consistent with the CCPA’s statutory text.

A. The Modified Proposed Regulations Should Be Revised to Better Reflect the Role of Service Providers in Responding to Consumer Rights Requests

Under the CCPA, businesses are assigned the responsibility of responding to consumers’ requests to access, correct, and delete their personal information. This is consistent with all

² Cal. Civ. Code § 1798.140(d)(1).

³ Cal. Civ. Code § 1798.140(ag)(1).

other state consumer privacy laws and leading data protection laws worldwide, which place this obligation on companies that decide how and why to collect consumers' data – rather than the service providers acting on behalf of such companies.

Of course, consumer rights must work in practice — even when personal information is held by a service provider. That is why the CCPA requires service providers to assist a business in fulfilling rights requests for personal information. Under the CCPA, service providers may either execute consumer rights requests directly or enable a business to do so. This second option — enabling the business to respond to requests — is critical to ensuring that companies can respond to large volumes of consumer rights requests efficiently and effectively. For example, many service providers offer services at scale that are used by hundreds of business customers, each of which may receive thousands of consumer rights requests. Service providers can help their business customers efficiently respond to those requests by creating scalable tools that the business can use to access, correct, and delete information held by the service provider — and thereby establish processes for assessing and responding to a large volume of requests.

We appreciate several changes made by the Modified Proposed Regulations to address this issue, including in Section 7022. We strongly agree with retaining the proposed text throughout Section 7022(b) that clarifies a business is either to notify a service provider to delete a consumer's personal information or, if enabled to do so by the service provider, delete the personal information itself. We encourage two further revisions to carry these changes throughout the Modified Proposed Regulations.

Recommendation: The Modified Proposed Regulations should be further revised to align with the CCPA's clear recognition that service providers may fulfil their role in handling consumer rights requests by either executing those requests or by enabling the business to do so. We strongly recommend two sets of changes:

1. Section 7022(f)(4), which addresses instances in which a business denies a consumer's request to delete in whole or part, should either be deleted or should be revised in line with changes made throughout this section that recognize a service provider may enable the business to comply with requests for data held by the service provider. If this provision is retained, we strongly recommend revising it to state a business is required to: "Instruct its service providers and contractors to delete the consumer's personal information that is not subject to the exception and to not use the consumer's personal information retained for any purpose other than the purpose provided for by that exception, or if enabled to by the service provider, the business shall comply with the portion of the request not subject to the exception."
2. Three of the modified provisions in Section 7022 should be further revised to focus on personal information a service provider "processes" pursuant to a contract, rather than information it "collects." This change better aligns with the CPRA's statutory language, which defines a service provider as "a person that processes personal information on behalf of a business" rather than one that collects personal information on behalf of a business.⁴ Moreover, the CPRA defines processing broadly, to include "any operation" performed on personal information. Aligning the regulations with this statutory definition ensures their scope mirrors the scope of a service provider's role under the statute. We suggest:

⁴ Cal. Civ. Code § 1798.140(ag)(1) (emphasis added).

- i. Revising Section 7022(b)(2) to state: “Notifying the business’s service providers or contractors to delete from their records the consumer’s personal information that they ~~Processed-Collect~~ pursuant to their written contract with the business, or if enabled to do so by the service provider or contractor, the business shall delete the personal information that the service provider or contractor ~~Processed-Collect~~ pursuant to their written contract with the business; and”
- ii. Revising Section 7022(c) to state: “A service provider or contractor shall, with respect to personal information that they ~~Processed-Collect~~ pursuant to their written contract with the business and upon notification by the business, cooperate with the business in responding to a request to delete by:
- iii. Revising Section 7022(c)(3) to state: “Notifying any of its own service providers or contractors to delete from their records in the same manner the consumer’s personal information that they ~~Processed-Collect~~ pursuant to their written contract with the service provider or contractor.”

B. The Modified Proposed Regulations Should Not Focus on the Degree to Which The Involvement of Service Providers is “Apparent” to Consumers

The Modified Proposed Regulations include a range of obligations intended to ensure a business’s collection, use, retention and/or sharing of personal information is reasonably necessary and proportionate to achieve certain purposes permitted by the statute. Section 7002, for example, focuses on ensuring that the purposes for which personal information are collected or processed are consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed. Section 7002(b) sets out several factors that may bear on a consumer’s expectations about why her data will be used, including the relationship between the consumer and the business and the type, nature, and amount of personal information that the business seeks to collect or process.

Section 7002(b)(5)’s treatment of service providers creates significant concerns. Although several other factors addressed in Section 7002(b) may appropriately bear on consumer expectations, Section 7002(b)(5) treats the “degree to which the involvement of service providers” is “apparent” to consumers as a factor in determining consumer expectations.

This provision is fundamentally at odds with the role of service providers, which process personal information on behalf of businesses. Consumers generally expect to interact with consumer-facing businesses, and not the dozens or more service providers who may process personal information on behalf of a single business. Of course, personal information should be safeguarded when processed by service providers, which is why CCPA and other leading privacy and data protection laws apply a range of other requirements to service providers to ensure they only process data on behalf of and at the direction of businesses. But those safeguards do not — and should not — turn on whether consumers expect a business to use a service provider, or whether the service provider’s role is “apparent” to a consumer.

Service providers are most valuable to both consumers and businesses when they help companies deliver products seamlessly. In many cases, a business will rely on a range of service providers to deliver a single product, with each service provider acting on behalf of and at the direction of that business. For example, a grocery store that accepts online and mobile orders may have many service providers: one service provider to store consumers’ orders and other information in the cloud; a second service provider to text consumers when their orders are out for delivery; and a third service provider to maintain the store’s mobile application. Even though these activities rely on service providers, the text messages and

mobile app bear the grocery store's name — because the service providers are merely processing personal information on its behalf and at its direction. If businesses were required to make the use of service providers “apparent” to consumers, the ability to offer these seamless services in the name of the consumer-facing business that an individual expects to interact with would decrease significantly. We strongly recommend deleting Section 7002(b)(5), to avoid this result.

Recommendation: Section 7002(b)(5) should be deleted in its entirety. Alternatively, we recommend revising this provision to delete references to service providers, which are subject to additional safeguards in handling personal information under CCPA not applicable to other entities such as third parties.

1. If Section 7002(b)(5) is not deleted, it should be revised to state: “The degree to which the involvement of ~~service providers~~, contractors, third parties, or other entities in the collecting or processing of personal information is apparent to the consumer(s). For example, the consumer likely expects an online retailer's disclosure of the consumer's name and address to a delivery service provider in order for that service provider to deliver a purchased product, because that service provider's involvement is apparent to the consumer. By contrast, the consumer may not expect the disclosure of personal information to a third party ~~service provider~~ if the consumer is not directly interacting with the third party ~~service provider~~ or the third party's ~~service provider's~~ role in the processing is not apparent to the consumer.

C. The Modified Proposed Regulations Should Not Create Contractual Obligations Beyond Those Set out in the CCPA's Text.

Two provisions of the CCPA create statutory requirements for contracts between businesses and service providers. First, Section 1798.100(d) requires businesses that engage service providers to enter into agreements with such providers. Second, in the CCPA's definition of the term “service provider” in Section 1798.140(ag), the statute requires that service providers be subject to contractual limitations in handling data on behalf of businesses.⁵ Beyond these requirements, the CCPA allows businesses and service providers to craft their own contracts. This is important, because it allows the parties to evaluate the nature of their relationship, the information to be processed, and the role of the service provider, and tailor the agreement accordingly.

⁵ Under Section 1798.140(ag), a service provider must process data pursuant to a contract that prohibits it from:

- “[S]elling or sharing the personal information[.]”
- “Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business, or as otherwise permitted by [the CCPA].”
- “Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business.”
- “Combining the personal information that the service provider receives from, or on behalf of, the business with [other] personal information . . . provided that the service provider may combine personal information to perform any business purpose as defined in regulations [to the CCPA]” other than in connection with cross-context behavioral advertising, or marking and advertising for consumers who exercised their opt-out rights.

This provision goes on to note that “the contract may, subject to agreement with the service provider, permit the business to monitor the service provider's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.”

However, the Modified Proposed Regulations create contractual requirements that go beyond those in the statute. We recommend revising the Modified Proposed Regulations to better align with the CCPA's requirements.

1. Section 7051(a)(7) of the Modified Proposed Regulations appears to conflate two separate provisions of the CCPA.

Section 7051(a)(7) of the Modified Proposed Regulations states that contracts between a business and a service provider must:

Grant the business the right to take reasonable and appropriate steps to ensure that service provider uses the personal information that it Collected pursuant to the written contract with the business in a manner consistent with the business's obligations under the CCPA and these regulations. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months.⁶

This provision combines two separate statutory requirements, in a manner that can be read to impose additional contractual obligations beyond those in the statute. The first part of this provision is based on CCPA Section 1798.100(d)(3), which states that a contract between a service provider and a business must “[g]rant[] the business rights to take reasonable and appropriate steps to help ensure that the . . . service provider . . . uses the personal information transferred in a manner consistent with the business' obligations under this title.”⁷ The second part is based on the CCPA's definition of service provider in 1798.140(ag)(1)(D), which states that the contract “may, subject to agreement with the service provider, permit the business to monitor the service provider's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.”⁸

Section 7051(a)(7) of the Modified Proposed Regulations combines these two statutory provisions, in a manner that suggests several contractual commitments may be mandatory — even though the CCPA clearly makes those commitments permissive rather than required. Specifically, Section 7051(a)(7) could be read to suggest that the compliance monitoring steps set out in the CCPA's definition of a service provider (as actions that may be taken “subject to agreement with the service provider”) could be viewed as required provisions of a service provider contract. This is not consistent with the text of the statute, which allows parties to agree to the “reasonable and appropriate steps” suitable in the context of a given service. The Modified Proposed Regulations should be revised to avoid suggesting otherwise.

Recommendation: Section 7051(a)(7) of the Modified Proposed Regulations should be revised to delete this ambiguous language, so that the provision states that contracts between businesses and service providers shall: “(7) Grant the business the right to take reasonable and appropriate steps to ensure that service provider or contractor uses the personal information that it Collected pursuant to the written contract with the business in a manner consistent with the business's obligations under the CCPA and these regulations. ~~Reasonable and appropriate steps may include ongoing manual reviews and automated~~

⁶ Mod. Prop. Reg. § 7051(a)(7).

⁷ Cal. Civ. Code § 1798.100(d)(3).

⁸ Cal. Civ. Code § 1798.140(ag)(1)(D) (emphasis added).

~~scans of the service provider's system and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months."~~

2. Section 7051(a)(2) of the Modified Proposed Regulations appears to require specificity in contracts that goes beyond the CCPA's requirements.

Section 7051(a)(2) of the Modified Proposed Regulations requires service provider contracts to "[i]dentify the specific Business Purpose(s) for which the service provider or contractor is processing personal information pursuant to the written contract with the business."⁹ It also states: "[t]he Business Purpose shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific."¹⁰

This requirement to provide "specific" business purposes goes beyond the requirements of the CCPA. The statute affords service providers and businesses greater flexibility to identify the business purposes for which a service provider may process personal information — including by referring to their contract as appropriate. This flexibility is important because it helps to avoid the need for businesses and service providers to continually amend and re-negotiate data processing terms as new services are added to a contract. The requirement to provide each "specific" business purpose is not necessary to ensure that data remains protected when processed by a service provider, because the service provider is already required to handle data in line with the contract with the business and subject to safeguards set out in the statute. Requiring greater specificity about the "specific" purposes for processing covered by a contract is also unlikely to create a substantial benefit to consumers, given the statutory limits already imposed on both businesses and service providers.

Recommendation: Section 7051(a)(2) of the Modified Proposed Regulations should be revised to be consistent with the CCPA, as follows: "Identify the specific Business Purpose(s) for which the service provider or contractor is processing personal information pursuant to the written contract with the business and specify that the business is disclosing the personal information to the service provider or contractor only for the limited and specified Business Purpose(s) set forth within the contract. ~~The Business Purpose shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.~~"

3. Sections 7050 and 7051 Should Be Revised to Recognize that Service Providers "Process" Personal Information

Sections 7050 and 7051 address a number of contractual and other obligations placed on service providers under the CCPA. Throughout the recently-revised text, however, the Modified Proposed Regulations refer to personal information that a service provider "collected" pursuant to its written contract with a business. We strongly recommend revising this language to better align with the CCPA's statutory text, which defines a service provider as "a person that processes personal information on behalf of a business" rather than one that *collects* personal information on behalf of a business.¹¹

Recommendation: In addition to other recommended edits addressed above, seven provisions in Sections 7050 and 7051 should be revised to replace "collect" with "process":

⁹ Mod. Prop. Reg. § 7051(a)(2).

¹⁰ *Id.*

¹¹ Cal. Civ. Code § 1798.140(ag)(1) (emphasis added).

1. Section 7050(a) should be revised to state: “A service provider or contractor shall not retain, use, or disclose personal information Processed~~Collected~~ pursuant to its written contract with the business except.”
2. Section 7051(a)(1) should be revised to state: “Prohibit the service provider or contractor from selling or sharing personal information it Processes~~Collects~~ pursuant to the written contract with the business.”
3. Section 7051(a)(3) should be revised to state: “Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Processes~~Collected~~ pursuant to the written contract with the business for any purpose other than the Business Purpose(s) specified in the contract or as otherwise permitted by the CCPA and these regulations.”
4. Section 7051(a)(4) should be revised to state: “Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Processes~~Collected~~ pursuant to the written contract with the business for any commercial purpose other than the Business Purposes specified in the contract, unless expressly permitted by the CCPA or these regulations.”
5. Section 7051(a)(5) should be revised to state: “Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Processes~~Collected~~ pursuant to the written contract with received from, or on behalf of, the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or updating personal information that it Processes~~Collected~~ pursuant to the written contract with received from, or on behalf of, the business with personal information that it received from another source or Processes~~Collected~~ from its own interaction with the consumer, unless expressly permitted by the CCPA or these regulations.”
6. Section 7051(a)(6) should be revised to state: “Require the service provider or contractor to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that it Processes~~Collected~~ pursuant to the written contract with the business—providing the same level of privacy protection as required by of businesses by the CCPA and these regulations. For example, the contract may require the service provider or contractor to cooperate with the business in responding to and complying with consumers’ requests made pursuant to the CCPA, and to implementing reasonable security procedures and practices appropriate to the nature of the personal information received from, or on behalf of, the business to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.”
7. Section 7051(a)(7) should be revised to state: “Grant the business the right to take reasonable and appropriate steps to ensure that service provider or contractor uses the personal information that it Processes~~p~~ pursuant to the written contract with the business in a manner consistent with the business’s obligations under the CCPA and these regulations. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider’s system and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months.”

II. Global Opt-Out Mechanism

A. Any Global Opt-Out Mechanism Should be Consistent and Interoperable with Mechanisms Recognized by Other State Privacy Laws.

BSA believes that consumers should have clear and easy-to-use methods for exercising new rights given to them by any privacy law.

Under the CCPA, the CPPA is tasked with issuing regulations that define the requirements and technical specifications for an opt-out preference signal that indicates a consumer's intent to opt out of the sale or sharing of that consumer's personal information, and to limit the use or disclosure of the consumer's sensitive personal information. In our view, the best reading of the CCPA, as amended by CPRA, is that any such opt-out mechanism is permitted, but not required, by the statute.¹² The Modified Proposed Regulations, however, contemplate a mandatory opt-out preference mechanism and require businesses to process opt-out preference signals meeting the requirements in Section 7025.

Regardless of whether a global opt-out mechanism is permissive or required, it is critically important that businesses understand which mechanism(s) they are to honor — and that those mechanisms be interoperable with any similar mechanisms recognized by other states. In particular, the new consumer privacy laws in Colorado and Connecticut create clear statutory requirements for companies to honor global opt-out mechanisms starting July 1, 2024 (for Colorado) and January 1, 2025 (for Connecticut). We strongly recommend the CPPA engage with regulators in those states to ensure that any global opt-out mechanism recognized in California is consistent and interoperable with opt-outs under these other state laws.

Recommendation: The CPPA should work with regulators in other states to ensure any opt-out mechanism recognized in California is interoperable with mechanisms recognized in other states.

B. Any Global Opt-Out Mechanism Must Function in Practice.

It is also critical that both businesses and consumers be able to use global opt-out mechanisms in practice. However, the Modified Proposed Regulations do not address a range of practical issues that will confront businesses and consumers as these mechanisms are implemented.

For example, is not clear from the Modified Proposed Regulations how a business will be able to determine that a particular signal meets the requirements of Section 7025(b), or if that determination will be left to each business. Likewise, consumers will not know which mechanisms will be honored or to what extent a mechanism will be honored across state lines. One way to address such concerns is for the CPPA to publish a list of the signals that meet CCPA's requirements and thus identify the mechanisms that businesses should honor, but the Modified Proposed Regulations do not clearly contemplate such a process. Creating a clear way for businesses to understand which mechanisms they must honor is important to ensuring that these mechanisms function in practice.

The CPPA should address such practical issues, to help ensure that businesses have fair notice of the mechanisms they may use to comply with obligations under the CCPA and can implement them in a manner that is easy for consumers to use. Companies will require time

¹² See Cal. Civ. Code 1798.135(b)(3) (stating that a business that complies with provisions for providing consumers certain opt-out links "is not required to comply with subdivision (b) [governing opt-out preference signals]. For the purpose of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b)").

to build tools to respond to global opt-out mechanisms — and focusing on practical issues early on will help foster the development and implementation of tools that work in practice.

Recommendation: The CPPA should address practical considerations including how a business will recognize if a particular signal meets the regulations' requirements. For example, the CPPA could develop a process for approving an opt-out signal and then publish a list of compliant signals; it could also work with stakeholders to create a process for nominating additional signals for the agency's approval, to help companies and consumers implement opt-out mechanisms in practice.

C. Consumer Education Around Global Opt Outs and Their Potential Limitations Will be Critical.

The CPPA should also prioritize educating consumers about global opt-out mechanisms and specifically the scope of what such mechanisms do, as well as their limitations. For example, if a consumer uses a browser-based mechanism to opt out of the sale or sharing of the consumer's personal information, the browser may be able to effectuate that request for activity that occurs within the browser, but not activity outside of the browser. Consumers should be aware of this and other limitations. The CPPA, and developers of compliant opt-out signals, are well-positioned to provide that education.

Recommendation: The CPPA should prioritize educating consumers about global opt-out mechanisms, including their scope and their limitations.

III. Agency Audits

A. The CPPA Should Exercise its Audit Authority in a Manner that Minimizes Privacy and Security Risks to Consumers, Including by Limiting On-Site Audits.

Under the CCPA, the CPPA is granted authority to audit compliance with the law and is tasked with issuing regulations to define the scope of the agency's authority and the process for exercising that authority. In particular, the statute requires that these regulations include establishing criteria for both selecting persons to audit and for "protect[ing] consumers' personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena."¹³

The Modified Proposed Regulations provide few details about — or guardrails for — this authority. Section 7304 of the Modified Proposed Regulations states that the CPPA "may audit a business, service provider, contractor, or person to ensure compliance with any provision of the CCPA."¹⁴ But the regulations do not address how personal information will be protected from disclosure in the absence of a court order, warrant, or subpoena, as required by the statute. Nor do the Modified Proposed Regulations clearly state how privileged information will be handled. Rather, the Modified Proposed Regulations state only that consumers' personal information disclosed to the agency during an audit will be maintained in compliance with the state's Information Practices Act of 1977.

We strongly recommend that the Modified Proposed Regulations create additional safeguards to ensure that audits further the CCPA's goal of protecting consumer privacy — and also that ensure the audit authority is not exercised in a manner that could inadvertently undermine consumer privacy or cybersecurity.

¹³ Cal. Civ. Code § 1798.185(a)(18).

¹⁴ Mod. Prop. Reg. § 7304(a).

In particular, the Modified Proposed Regulations should be revised to address how audits will be conducted — including whether they will occur on-site or off site — and to specifically limit the use of on-site audits absent specific circumstances warranting an on-site audit. Any audit should require guardrails to mitigate the potentially significant privacy and security concerns involved. For example, an audit of a service provider that serves hundreds of businesses can create a range of privacy and security risks. This is particularly true when the audit is on-site, as opposed to remote. An on-site audit may inadvertently expose to auditors information relating to a range of businesses and consumers whose activities are not the intended focus of the audit, creating significant privacy risks. Moreover, in this context on-site audits would typically not provide information beyond that available through a remote audit, because the relevant information is accessible in either case. Indeed, remote audits can be more efficient in identifying relevant information without the attendant privacy and security risks of an on-site audit.

We recommend revising the Modified Proposed Regulations to limit the use of on-site audits and specifically endorse the use of remote audits, particularly when there are no special circumstances that merit the audit being conducted on-site and when an on-site audit may create privacy and security concerns. Given the privacy and security risks that arise from exercising the agency's audit authority, we urge the CPPA to limit the use of its audit authority to circumstances in which there is a "significant" concern that the statute has been violated. The agency may define such circumstances by example, consistent with other aspects of the Modified Proposed Regulations.

Recommendation: We make two recommendations to focus the Agency's audit authority:

1. Section 7304(a) should be revised to state: "(a) Scope. The Agency may audit a business, service provider, contractor, or person to ensure compliance with any provision of the CCPA. Audits will be conducted remotely, absent specific circumstances warranting an on-site audit. Where specific circumstances warrant more immediate intervention, the Agency shall require in writing the preservation of documents and information."
2. Section 7304(b) should be revised to state: "(b) Criteria for Selection. The Agency may conduct an audit in circumstances that create a significant risk of ~~to investigate~~ possible violations of the CCPA. 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.~~"

* * *

BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide these comments. We welcome an opportunity to further engage with the CPPA on these important issues.

For further information, please contact:
Kate Goodloe, Senior Director, Policy

From: Andrew Kingman <[REDACTED]>
Sent: Sunday, November 20, 2022 2:59 PM
To: Regulations
Subject: State Privacy & Security Coalition - CCPA Modified Regulations - Comments
Attachments: SPSC - CCPA Modified Regulations Comments.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good afternoon,
Attached please find comments submitted on behalf of the State Privacy & Security Coalition. Thank you very much.

Respectfully submitted,
Andrew A. Kingman

Andrew Kingman

President
[REDACTED]
[REDACTED]



STATE PRIVACY & SECURITY COALITION

November 21, 2022

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd
Sacramento, CA 95834
regulations@coppa.ca.gov

Re: State Privacy & Security Coalition Comments on CCPA Regulations

Dear Mr. Soublet and Members of the California Privacy Protection Agency:

The State Privacy & Security Coalition, a coalition of over 30 companies and trade associations in the retail, technology, automobile, telecommunications, and payment card sectors, respectfully submits the following comments regarding the modified California Consumer Privacy Act (CCPA) regulations (modified regulations).

Our coalition works in all 50 states on data privacy and cybersecurity legislation and regulations. We evaluate proposals to ensure that they appropriately balance increased control and transparency for consumers, operational workability for businesses, and cybersecurity protections for all stakeholders.

While we appreciate that the modified regulations provide helpful clarity in a number of respects, we remain concerned that the modified regulations that the California Privacy Protection Agency (CPPA, or the Agency) has proposed have not fixed its fatal flaw, which is that a number of provisions in this draft clearly exceed the Agency's statutory authority granted by its enabling text. By continuing to do so, this draft still does not meaningfully benefit consumers, nor does it increase the operational workability for businesses. These comments detail those provision, and we reiterate our request that they be struck from the final regulations due to this violation of statutory authority.

We expect that this final 15-day comment period and subsequent review by the Agency provides an opportunity to correct these significant issues.

Additionally, SPSC is alarmed about a number of procedural irregularities throughout this rulemaking process, including the potential conflicts of interest posed by recent CPPA board appointments, opacity in the decision-making that led this rulemaking to be considered a non-major rulemaking, and the removal of the Department of Finance's study on the initial implementation costs of the CCPA from the state's website.

Below, we add to and reiterate our feedback on those provisions in the modified rules that SPSC believes are not supported, and indeed go beyond the text of the statute and the authority granted to the CPPA by the Administrative Procedure Act.

STATE PRIVACY & SECURITY COALITION

Standard of Review

As we noted in our initial comments, a regulation is invalid if: 1) it is not “consistent” with the enacting statute; 2) it is “in conflict” with the statute; 3) it is not “reasonably necessary to effectuate the purpose of the statute”; or 4) it is “not within the scope of authority conferred” by the statute.¹

Opt-Out Preference Signal (OPS)

The modified regulations still do not address the concern we raised in our initial comments – the Agency has clearly exceeded its authority by using the modified regulations to state that the OPS is mandatory for businesses to recognize. While this may be the Agency’s preference, the edict is in conflict with the plain text of the statute.

The California Privacy Rights Act (CPRA) modifies §1798.135 by renaming the section “Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Personal Information.” This section provides that a business may choose one of two methods to allow consumers to opt-out of the sale of personal information, the sharing of personal information, and to limit the use of sensitive personal information:

Method 1 (using clear and conspicuous links):

- a. Provide a clear and conspicuous link on each website page that collects personal information titled “Do Not Sell or Share My Personal Information;” and
- b. Provide a clear and conspicuous link on each website page that collects personal information, titled “Limit the Use of My Sensitive Personal Information;” or
- c. At the business’s discretion, a single link that accomplishes both tasks, “if such a link easily allows” a consumer to both opt-out of the sale/share of personal information and limit the use of sensitive personal information; or

Method 2:

- a. Recognizing an OPS.

Critically, subparagraph (b) of §1798.135 states that: “A business *shall not be required to comply with subdivision (a)* if the business allows consumers to opt-out of the sale or sharing of the personal information and to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer’s consent by a platform, technology, or mechanism...” (emphasis added). Section 1798.135(b) of the statute reinforces the optional nature of the OPS, stating that “A business that complies with subdivision (a) of this Section [posting links] *is not required to comply with subdivision (b)* [using OPS]. For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b).” Put quite simply, the CPRA sets forth two ways that a business may allow a consumer to opt-out/limit the use of their personal information and sensitive personal information: the first, by offering either two separate links or one combined link (subdivision (a)), or the second by recognizing an OPS (subdivision (b)).

However, in direct contradiction with the clear language of the statute, the Agency seeks to *require* businesses to recognize an OPS. Specifically, in §7026(e), the Agency ignores the statutory language and proposes an unusual regulation, stating in part that “Civil Code Section 1798.135...does not give the

¹ Cal. Gov. Code §§ 11342.1; 11342.2.

STATE PRIVACY & SECURITY COALITION

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...” The Agency contorts the plain text of the statute into a reading that a business *must* recognize an OPS, but *may* choose to post the links. The Agency states in its Initial Statement of Reasons that its modified regulation making the OPS mandatory “is...necessary to address a common misinterpretation of Civil Code section 1798.135, subdivisions (b)(3) and (e), that complying with an opt-out preference signal is optional for the business. Not so.” Notably, the Agency does not cite any statutory language to support its position. There is, in fact, no basis in the statute for this interpretation.

The plain text of the statute contradicts the Agency’s assertion of its policy preferences. The OPS is quite clearly a provision designed to be optional, not mandatory. Section 1798.185(a)(20) directs the CCPA to “[i]ssu[e] regulations to govern how a business *that has elected to comply with subdivision (b)* responds to the opt-out preference signal....” (emphasis added).

California courts have rejected regulatory interpretations that contradict the plain text of the governing statute when the agency’s interpretation is “at war with the straightforward textual conclusion.”² We are confronted with such a direct conflict here, where the “straightforward textual conclusion” regarding the CPRA’s intent could not be more clear: in fulfilling their obligation to provide consumers an opt-out mechanism (or mechanism to limit the use and disclosure of sensitive data), businesses can *choose* whether to recognize an opt-out preference signal *or* provide the links described in the statute. They are not required to do both. What the Agency mischaracterizes as business’s “common misinterpretation” is in fact a plain reading of the statutory language. California courts have made clear that the Agency cannot substitute its policy preference, manifested in these regulations, for the clear language of the statute. The Agency’s policy position, manifested in these regulations, is not simply inconsistent with the statute – it is in direct conflict. The regulations stating the OPS is mandatory must, by law, be removed from the Agency’s final version.

Additionally, these regulations fail to set forth common, clear technical guidance or disclosure requirements for opt-out signal developers. The current regulations ignore important requirements set forth in §1798.185(a)(19) of the CPRA, such as ensuring the opt-out signal clearly represents a consumer’s intent, is free of defaults presupposing such intent, and does not conflict with other commonly used privacy settings and tools. These requirements cannot be satisfied unless an opt-out signal is capable of identifying California residents and presenting the user with specific information about any technical limitations of the signal and the applicable Do Not Sell or Do Not Share My Personal Information under the CPRA.

Put another way, responsibility should lie with the OPS developers to ensure that its users understand how the signal works, as well as its limitations. Otherwise, the lack of guidance puts an unreasonable burden on businesses to sort through various signals with differing specifications, which will considerably impede the adoption and workability of the OPS.

Processing of Personal Information

The OPS is not the only area where the Agency’s modified regulations exceed the scope of the statute. The Agency also exceeded its authority in promulgating regulations governing the collection of personal

² *In re McGhee*, 34 Cal.App.5th at 905

STATE PRIVACY & SECURITY COALITION

information and limiting how collected personal information can be used. The CCPA as amended by the CPRA requires that:

[C]ollection, use, retention, and sharing of a consumer's personal information shall be *reasonably necessary and proportionate* to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is *compatible with the context in which the personal information was collected*, and not further processed in a manner that is incompatible with those purposes. (emphasis added).³

This paragraph sets forth two standards for the processing of a consumer's personal information. Processing is permissible when:

1. The collection, use, retention, and sharing of a consumer's personal information is reasonably necessary and proportionate to achieve the purposes for which the information was collected or processed;
2. The collection, use, retention, and sharing of a consumer's personal information shall be:
 - a. reasonably necessary and proportionate to achieve...another disclosed purpose that is compatible with the context in which the personal information was collected, and
 - b. not further processed in a manner incompatible with those purposes.

In other words, the necessary tests for processing information are either the reasonably necessary and proportionate standard, or the compatible purpose standard. While we appreciate that the Agency has modified the regulations to remove the initially proposed "average consumer" standard, we are concerned that the Agency's substitution of an overbroad multi-factor standard continues the conflict with the statutory standard and gives the Agency unbridled discretion. As proposed by the Agency, the focus for all data collection and use practices would be framed by this standard, rather than by disclosures and compatibility to disclosures with respect to further processing. The better outcome, which is both aligned with the statute and other frameworks (like the GDPR), is to limit collection and processing to notices at the time of collection and to limit further processing to a compatibility test. This approach ensures that the statutory standard is meaningfully retained by focusing the analysis on the clarity of consumer disclosure and on the data practices rather than on the ambiguous viewpoint of a reasonable consumer. It avoids a conflict of reasonable minds, and a *de facto* grant of authority for the Agency to supplant its discretion and analysis over a business's reasonable assessment.

Additionally, §7002(b)(5) of the modified regulations is unrealistic and runs counter to the real-world way that controllers and processors interact; this provision will not be helpful to consumers. Consumers are not in a position to judge whether a business's reliance on service providers or contractors is reasonable or not, particularly not with regard to the collection and processing of personal information. We fear that the optics of using any number of service providers and contractors may harm small and medium-size businesses who rely on a network of service providers to help them function, but which might be performed internally by larger entities.

In straying from the language and clear intent of the CCPA as amended by the CPRA, the Agency also exceeds its statutory limits with these modified rules because the CPRA *does not grant rulemaking authority on this point*. In its Initial Statement of Reasons, the Agency cites §1798.185(a)(10), stating that §7002 "reflects the mandate set forth in...1798.185, subdivision (a)(10), that the purposes for which

³ Cal. Civ. Code §1798.100(c)

STATE PRIVACY & SECURITY COALITION

businesses may use consumers' personal information should be consistent with consumers' expectations."

However, there is no text in this section that provides the Agency *any authority* to regulate the *methods of collection*; it gives the Agency authority to delineate specific business purposes in addition to those set forth in §1798.140(e). Section 1798.185(a)(10) gives the Agency authority *only* for "further defining and adding to the business purposes, including other notified purposes, for which businesses, service providers, and contractors may use consumers' personal information with consumers' expectations, and further defining the business purposes for which service providers and contractors may combine consumers' personal information obtained from different sources..."

The Agency does not have the statutory authority to issue these regulations, which impermissibly and enlarge the scope of the statute, and SPSC requests that this provision be removed from the final regulations.

A better, more helpful approach would be to look to Europe's General Data Protection Regulation (GDPR), where Recital 50 sets forth an interpretation of compatibility that many companies already employ in Europe.⁴ The guidance promulgated by the European Commission sets forth several considerations that help entities determine whether their uses are compatible with the purposes for collection, including:

- The link between the original purpose and the new purpose;
- The context within which the data was collected;
- The type and nature of the data;
- The possible consequences of the intended further processing; and
- The existence of appropriate safeguards (e.g., encryption or pseudonymization).

The Agency's lack of interest in creating interoperability between California's privacy regime and other regimes continues to be a source of frustration for businesses who are attempting to comply with this global patchwork. Further, the Agency's lack of positive examples that could illustrate any reasonable path to compliance is also frustrating to companies that are diligently working to ensure their programs are consistent with the CPRA. As the Agency works to adjust its regulations to be consistent with its authority under the statute, it should strive for rules that are interoperable and include positive examples.

The Modified Regulations Impermissibly Alter the Scope of the Business and Service Provider Duties and Responsibilities

As we discussed extensively in our initial comments, the CPPA further exceeds the limits of the statute by impermissibly attempting to impose a duty of diligence for businesses that is simply not contemplated in the text of the CPRA, and adding in prohibitions to the regulations that are not contemplated by the statute.

a. The Modified Regulations Impose Requirements on Service Providers that Do Not Have a Basis in the Statute.

⁴ <https://www.privacy-regulation.eu/en/recital-50-GDPR.htm>

STATE PRIVACY & SECURITY COALITION

The regulations attempt to impose a duty of diligence on businesses with regard to service provider and contractor compliance with these laws. This duty of diligence is not contemplated in either the original CCPA or the CPRA amendments.

A company must be able to rely on the representations made in a contract with a service provider or contractor, as is reflected in §1798.145(i) (providing that a business “shall not be liable” if a service provider or contractor violates the statute, so long as “at the time of disclosing personal information, the business does not have actual knowledge, or reason to believe,” that the service provider or contractor “intends to commit such a violation”). However, §7053(e) of the modified regulations undermines these protections. The illustrative example, that a business that “*never exercises its rights to audit or test the service provider or contractor’s systems might not be able to rely on this defense...*” may be read as a de-facto monitoring obligation, above and beyond the requirements of CPRA. While many companies have in place auditing programs of their service providers/contractors, the frequency of such audits is generally correlated with the level of risk that the personal information being processed represents, depending on the nature of the contract and the services. The modified regulations could therefore require unduly onerous ongoing obligations of service providers or contractors which erodes the principles of service provider/contractor responsibility in the CPRA.

b. The Modified Regulations Attempt to Prohibit Statutorily Permissible Advertising Activity

The illustrative example in §7050(b)(1) of the modified rules goes beyond the textual bounds of the statute and raises new questions and creates uncertainty for businesses beyond those called out in the example.

The illustrative example purports to prohibit a form of advertising based on email addresses, and it is unclear what the basis is for doing so. The CPRA’s delineation of “advertising and marketing services” as a permissible business purpose prohibits the combination of personal information for a business’s opted-out consumers with a service provider’s information obtained on its own or from other entities. However, the illustrative example appears to suggest that *any* combination of information by a service provider is impermissible, not just the combination of personal information of opted-out consumers.

The implications of this example would be significant; this would create uncertainty regarding CPRA's treatment of relationships between businesses and service providers with respect to advertising as well as more broadly with respect to future contracts between businesses and service providers. SPSC proposes clarifying the example as follows:

“The social media company can also use a customer list provided by Business S to serve Business S’s advertisements to Business S’s customers. However, it cannot use a list of customer email addresses provided by Business S to then target those customers with advertisements based on information obtained from other third-party businesses’ websites, applications, or services.”

Right to Correct

While the statute gives the Agency authority to promulgate rules about the right to correct, the Agency has drafted these modified rules to contradict core features of the statutory framework.

Most notably, provisions requiring a business to “disclose all the specific pieces of personal information that the business maintains and has collected about the consumer to allow the consumer to confirm

STATE PRIVACY & SECURITY COALITION

that the business has corrected the inaccurate information that was the subject of the consumer's request to correct" is overly broad. At a minimum, this should only apply to the specific pieces of PI relevant to the request to correct and should be subject to the same protections to which the right to know responses are subject. Otherwise, this overly broad access rule would serve as a loophole for the reasonable security parameters in place to protect against the access right being used to harm rather than help consumers—which is foundational to the CCPA framework.

In order to address the security concerns created by disclosing the information required in this section, we propose the following sentence be added to the end §7023(h):

"A business shall not be required to provide any information to the requestor if the disclosure of such information could potentially reveal how to subvert the business's authentication, fraud prevention, or other processes designed to ensure that personal information is not improperly corrected, accessed, or acquired."

Alternatively, we would encourage the Agency to look at the language that all other state privacy laws have adopted in order to protect not just unauthorized access or acquisition of information, but other types of activities that are objectively harmful to both consumers and businesses alike:

"Nothing in this Act shall be construed to restrict a [business's] or [service provider's] ability to prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems, or investigate, report or prosecute those responsible for any such action."⁵

It is likely that many requests to correct personal information do not require this type of burdensome disclosure. The Agency is also required to promulgate rules pertaining to corrections with "the goal of minimizing the administrative burden" on consumers."⁶

Lastly, we recommend recognizing that businesses shall use reasonable efforts to keep corrected information accurate, but that these are scenarios where "foot-fault" technical omissions can occur; to that end, we would suggest adding the following phrase to §7023(f):

"Failing to consider and use reasonable efforts to address the possibility that corrected information may be overridden by inaccurate information subsequently received from a data broker may factor into whether that business, service provider, or contractor has adequately complied with a consumer's request to correct."

Many companies already offer consumers convenient and readily-usable "self-service" methods to correct their personal information. The draft regulations under the Colorado Privacy Act recognize these self-service methods as an acceptable way to facilitate consumers' correction rights. CTIA suggests the Regulations harmonize with Colorado's approach by adding the following new subsection (l) to §7023:

If a Consumer submits a request to correct and the requested correction could be made by the Consumer through the Consumer's account settings, a business may respond to the Consumer's

⁵ See, e.g., Connecticut Data Privacy Act, Public Act No. 22-15, §10(a)(9)

⁶ Cal. Civ. Code 1798.185(a)(7)

STATE PRIVACY & SECURITY COALITION

request by providing instructions on how the Consumer may correct the personal information so long as:

- (1) The correction process is not unduly burdensome to the Consumer;
- (2) The instructions are clear, accessible, and understandable to Consumers so that Consumers can understand and are able to exercise the full scope of their rights under this Act;
- (3) The Business's response is compliant with the timing requirements set forth in this Act;
and
- (4) The process described in the instructions enable the Consumer to make the specific requested correction.

12-Month Look-Back Period

The regulations continue to further exceed the scope of the CPRA by requiring businesses to provide personal information beyond the 12-month period contemplated by the CCPA as amended by the CPRA. There, §1798.30 explicitly sets forth the process for granting a consumer request:

“the disclosure of the required information shall cover the 12-month period preceding the business’s receipt of the verifiable consumer request, provided that, upon the adoption of a regulation...**a consumer may request** that the business disclose the required information beyond the 12-month period and the business shall be required to provide such information unless doing so proves impossible or would involve a disproportionate effort.” (emphasis added).

The referenced statutory section (§1798.185(9)) states that the CPPA shall establish “the standard to govern a business’s determination...that providing information beyond the 12-month period in a response to a verifiable consumer request is impossible or would involve a disproportionate effort.”

However, the modified regulation neither recognizes the centrality of the consumer’s role in requesting personal information beyond the 12-month period, nor does it attempt to elucidate a standard to govern a business’s determination of impossibility/disproportionate effort.

Instead, the modified regulation eviscerates the distinction between information provided within and outside the 12-month period, stating that a business is responsible for providing all personal information in response to a request to know, “including beyond the 12-month period preceding the business’s receipt of the request, unless doing so proves impossible or would involve disproportionate effort.”

Even the Agency’s own summary of its regulations concede that it ignores the text of the statute, stating that the regulations in part “[e]stablish procedures to extend the 12-month period of disclosure of information” in response to a consumer request.⁷

In the body of the Initial Statement of Reasons, the Agency claims that the regulations have “been revised to align the regulation with the revised language of the statute.” As demonstrated above, however, *nowhere does the regulation permit the Agency to extend this time period* by default and without a consumer request. It *only* provides the Agency with authority to clarify how a business may

⁷ Initial Statement of Reasons, p.2 par. 2

STATE PRIVACY & SECURITY COALITION

determine that providing the personal information beyond the 12-month period is impossible or involves disproportionate effort.

There are significant operational implications to this overreach. In the effort to meet the January 1, 2023 implementation deadline, businesses and service providers are designing their data storage architecture to be able to retain, store, and retrieve consumer personal information in ways that are sufficient for statutory compliance. By changing the default time period for retrieving personal information from “12 months” to “indefinitely,” the Agency is not only significantly altering the statute’s expressed policy preference, but is also making it operationally difficult to build compliant systems.

Again, this modified regulation is a clear case of the Agency using this process as a way to expand the scope of the CPRA – something which is not permitted by California law.⁸ Policy aspirations do not trump the plain text of the governing statute.⁹

Dark Patterns

SPSC does not dispute the criteria that the Agency sets forth in section 7004(a) provides strong guidance to avoiding the implementation of a dark pattern. However, we would like to ensure recognition of the fact that not all websites or user interfaces contain the features discussed in subsection (a), or similarly, that not all of the elements of subsection (a) are present for each website or user interface. As such, we reiterate our request from our initial comments that subsection (b) be modified as follows:

(b) A method that does not reasonably comply with subsection (a) may be considered a dark pattern.

Again, this does not weaken the importance of the elements listed, but provides some recognition that not all the listed elements are relevant to all user interfaces.

However, the Agency should strike the example provided in Section 7004(a)(3)(B) regarding “on” or “off” toggles being confusing. On/off toggles are pro-privacy and intended to clearly and simply give consumers options. The regulations should not call them into question and imply that the use of these type of pro-consumer tools could be a confusing or constitute a dark pattern. Already, the regulations state that “Toggle or button must clearly indicate the consumer’s choice.” This language is sufficient to protect against confusing practices.

Additionally, given the revised – although still ambiguous - standards set forth in section 7004(c) for what the CPPA may decide is a dark pattern and what is not, we believe it would be helpful to insert an additional factor as to whether a user interface constitutes a dark pattern that is based on internal process; more specifically, that a business which has an internal process to review products for dark patterns may be a factor in determining whether a user interface is in fact a dark pattern. We propose the following language after the sentence ending with the phrase “but a factor to be considered.”:

If a business can demonstrate a documented process for reviewing user interfaces to avoid dark patterns, this may weigh against a user interface being a dark pattern.

⁸ *In re McGhee*, 34 Cal.App.5th at 905.

⁹ *Id.*

STATE PRIVACY & SECURITY COALITION

New Notice Requirements

Section 7011 (Privacy Policy): The regs should not require granular mapping between purpose and data type. We would request to strike the following specifically:

- Section 7011(e)(1)(E): *“For each category of personal information identified in subsection (e)(1)(D),”*
- Section 7011(e)(1)(I): *“For each category of personal information identified in subsection (e)(1)(H),”*

§7024 (Privacy Policy): The regs should not require granular mapping between purpose and data type. We would request to strike, in §7024(k)(5) and (6) strike the language “and for each category identified.”

One-Year Enforcement

The intent of the CPRA’s language regarding enforcement is that it should begin no earlier than one year following adoption of the final regulations. The CPRA states that final regulations shall be adopted by July 1, 2022. Clearly, the regulations will be adopted substantially later than this, likely not being finalized until 2023.

Accordingly, SPSC believes that in order to appropriately honor the CPRA’s – and indeed, California voters’ - intention regarding enforcement, that the Agency must refrain from any enforcement action for a period of one year following the final adoption of these regulations, and enforce violations only from that time period forward. We appreciate the new language setting forth criteria for the Agency to exercise discretion in its enforcement prior to the July 1, 2023 deadline; however, this still does not comport with the intent of the CPRA’s language. The enforcement deadline should be extended to a full one-year following approval of the final regulations, and enforcement should apply to activity occurring after that date.

These regulations contain substantial modifications and additions to the CPRA, and businesses need time to rework many of the systems they were in process of implementing in order to be in a compliance posture. They should not be held to an artificial timeline for implementing the rules that themselves took longer than anticipated to finalize in order to substantively change requirements toward which businesses have been building for multiple years,, and which still have significant topics left to tackle.

Audit/Enforcement Powers

While SPSC does not argue that the CPRA provides authority for the CPPA to establish processes for the Agency to audit companies, we take strong issue with the process set forth in these regulations. It would be difficult to imagine a process designed to be more heavily weighted in the government’s favor and with less due process for California businesses than the one set forth in §7304. In sharp contrast to the process set forth in §7302 which is closely tied to a recognizable legal standard, the process described in §7304 lacks any limits on the Agency’s power or the delineation of standards to which businesses and service providers can expect to be held. We raised these concerns in our initial comments, but the Agency has not addressed them to this point. We reiterate our concerns here.

STATE PRIVACY & SECURITY COALITION

If this section is adopted as is, the Agency appears to seek the right to a) audit companies without notice; b) make what appears to be a unilateral determination without any opportunity for rebuttal that a subject's processing of personal information presents "significant risk to consumer privacy," and states that the consequence for any company's "failure to cooperate" during an unannounced, unjustified audit is a "subpoena...warrant, or otherwise exercising [the CPPA's] powers."

Surely, more narrowly tailored audit provisions can be drafted while still retaining strong enforcement powers. SPSC proposes removing the ability of the Agency to: 1) conduct unannounced audits; 2) make a unilateral "significant risk" determination with no documentation, process, or justification. We recommend giving companies the ability to respond to an audit request in a manner that, if legitimately reasonable, would obviate the need for such request.

SPSC also proposes that the scope of any audit request should be approved by Agency Board members prior to being issued, and that a business's election to participate in an audit be considered a mitigating factor in any subsequent enforcement decision.

Conclusion

A regulation is invalid if it is not "consistent" with the statute, if it is "in conflict" with the statute, if it is not "reasonably necessary to effectuate the purpose of the statute", or if it is "not within the scope of authority conferred" by the statute. The Agency has clearly exceeded its authority in several sections. The State Privacy & Security Coalition therefore respectfully requests that the above-referenced modified regulation provisions be removed or amended as indicated by adopting the State Privacy & Security Coalition's recommended language.

Respectfully submitted,



Andrew A. Kingman
Counsel, State Privacy & Security Coalition

From: McArthur, Webb [REDACTED]
Sent: Sunday, November 20, 2022 3:29 PM
To: Regulations
Cc: Eric Ellman
Subject: CPPA Public Comment
Attachments: CDIA CPPA CPRA Rulemaking Comment Letter Nov 2022 4871-3268-6398 v.2.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good afternoon –

Please see the attached comments of the Consumer Data Industry Association on the proposed revisions to the CCPA regulations.

Webb McArthur
Partner | Admitted in the District of Columbia, Maryland, and Virginia
Hudson Cook, LLP
Direct: [REDACTED] | Cell: [REDACTED]
1909 K St., NW | 4th Floor | Washington, DC 20006



HUDSON
COOK 

The information contained in this transmission may be privileged and may constitute attorney work product. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact Webb McArthur at [REDACTED] and destroy all copies of the original message and any attachments.

* * * *



Consumer Data Industry Association ^{W125}
1090
Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

P [REDACTED]

Writer's direct dial: + [REDACTED]

CDIAONLINE.ORG

November 20, 2022

Via Electronic Delivery to
regulations@coppa.ca.gov

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

RE: CCPA Public Comment in response to Notice of Modifications to Text of Proposed Regulations concerning the California Consumer Privacy Act

Dear Mr. Soublet,

The Consumer Data Industry Association submits this comment letter in response to the California Privacy Protection Agency ("CCPA") Notice of Modifications to Text of Proposed Regulations on proposed changes to California Consumer Privacy Act ("CCPA") regulations related to the California Privacy Rights Act ("CPRA").

The Consumer Data Industry Association ("CDIA") is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumers' access to financial and other products suited to their unique needs.

CDIA members have been complying with laws and regulations governing the consumer reporting industry for decades. Members have complied with the Fair Credit Reporting Act ("FCRA"), which has been called the original federal consumer privacy law. The FCRA governs the collection, assembly, and use of consumer report information and provides the framework for the U.S. credit reporting system. In particular, the FCRA outlines many consumer rights with respect to the use and accuracy of the information contained in consumer reports. Under the FCRA, consumer reports may be accessed only for permissible purposes, and a consumer has the right to dispute the accuracy of any information included in his or her consumer report with a consumer reporting agency ("CRA").

CDIA members have been at the forefront of consumer privacy protection. Fair, accurate, and permissioned use of consumer information is necessary for any CDIA member client to do business effectively.

CDIA appreciates the CPPA's invitation to comment on this important rulemaking process. CDIA also appreciates the CPPA's consideration of CDIA's previous comments, like on issues related to consumer disclosure font size and color, requests to know, and third party deletion requests. However, CDIA remains concerned with certain proposed sections and urges the CCPA to clearly provide that businesses may engage in purposes consistent with previous disclosures, businesses may retain information corrected by a consumer, businesses may retain sensitive personal information to prevent fraud, and service providers and contractors may sell or share personal information if the law otherwise permits it.

To assist the agency in finalizing clear and effective regulations that allow businesses to best support customers and consumers, CDIA offers the following comments on the proposed revisions:

I. Delaying Enforcement of New Rules

As an initial matter, CDIA strongly encourages the CPPA to postpone enforcement of the CPRA until one year after regulations are finalized. The CPRA required the CPPA to finalize regulations by July 1, 2022, providing one year until enforcement would begin, on July 1, 2023. Further, September 2022 developments in the California legislature now require businesses to assess personal information for CCPA compliance previously exempted from the law.

Because the regulations were not finalized as provided for in the CPRA, enforcement should be postponed to one year after the regulations are finalized. In particular, CDIA strongly urges the CPPA to provide at proposed section 7301 that investigations may not be initiated until a year after regulations are finalized.

II. Restrictions on the Collection and Use of Personal Information

The CPRA, at Cal. Civ. Code § 1798.100(a)(1), provides that a “business shall not . . . use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, without providing the consumer with notice consistent with this section.” Further, section 1798.100(c) provides that a “business’s collection [and] use . . . of a consumer’s personal information shall be reasonably necessary to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with these purposes.” Considering these two sections together, it is clear that a business can use personal information for the purpose it disclosed to the consumer at collection (limited to what is reasonably necessary and proportionate to achieve that purpose) or for a purpose *later*

disclosed to the consumer, so long as that later-disclosed purpose is not inconsistent with the first disclosed purpose.

Proposed section 7002(a) states that a business' collection, use, retention, and/or sharing of consumer personal information must be necessary and proportionate to achieve the purpose or purposes for which the personal information was collected or processed or another disclosed purpose that is compatible with the context in which the personal information was collected. The proposed section goes beyond the text of the statute and lays out a complex and confusing 5-factor formula to assess whether actual uses are reasonably necessary and proportionate, and then whether they are compatible, with consumer expectation, not the previous disclosures. In particular, it seems the CPPA is expressing a view on compatibility that is far narrower than what is reflected in the statute. While the drafted language is ambiguous, it may be the case that the CPPA may envision that later-disclosed but compatible purposes must be a Business Purpose listed in Cal. Civ. Code § 1798.140(e)(1) through (8), while a plain reading of the statute would lead one to believe that later-disclosed purposes are only impermissible when they contradict, undermine, or stand opposed to *the initially-disclosed purposes*.

What results from the ambiguity of the draft language is an excessive amount of discretion placed into the hands of the CPPA, more than the CPRA contemplates. The five factors ultimately provide no helpful guidance to businesses and create confusion and risk for businesses mapping out their processing uses. CDIA believes that the standards here should depend on disclosures and compatibility with prior disclosures, not on other factors not articulated by the CPRA under a consumer expectations umbrella.

CDIA encourages the CPPA to revisit this section to reflect the collection and use permissibility as articulated by the CPPA. CDIA welcomes guidance from the CPPA, but that guidance needs to be both clear and consistent with the law.

III. Requests to Delete

Proposed section 7022(b) requires businesses to notify third parties to whom the business has sold or shared personal information of a consumer's request to delete personal information. However, the proposed rule includes no limitations on this notification requirement, such as limiting where the business sold or shared personal information within the previous year. CDIA strongly urges the CPPA to provide for reasonable limits so that businesses are not required to retain records of the personal data, transfers, and uses indefinitely simply to comply with this notification requirement.

IV. Requests to Correct

Proposed section 7023 states, in part:

“(c) A business that complies with a consumer's request to correct shall correct the

personal information at issue on its existing systems.”

Businesses that retain information for the purpose of detecting and preventing fraud, identity theft, or security incidents need to be able to retain personal information in original form, despite any request to correct. For example, if a consumer contacts a business, verifies their identity, and updates their address, businesses need the flexibility to retain the former address for use in future identity verification needs, rather than being required to update it and delete the old information. Further, businesses need to be able to retain previously-collected personal information for other reasons, particularly complying with legal obligations (for example, legal holds), complying with contract obligations (for example, updating information through third-party sources like USPS address change notifications), processing the information for other limited internal uses not incompatible with previously disclosed purposes. This proposed section does not clearly permit businesses to retain information it updates as previous data points, and CDIA urges the CPPA to explicitly permit retention of personal information for the purposes already detailed in the CCPA for the right to delete, at Cal. Civ. Code § 1798.105(d).

Additionally, the proposed “totality of circumstances” test provides new and broader criteria for business to consider when determining whether to deny a consumer’s request to correct personal information. In particular, the proposed rule states that in the case that the business is not the original source of the personal information, “the consumer’s assertion of inaccuracy may be sufficient to establish that the personal information is inaccurate.” Under the proposed test, businesses would be required to accept, review, and consider any documentation that the consumer provides and explain the basis for denial to the consumer. This would prove challenging to businesses that do not have direct interaction with the consumer in question. These challenges would be particularly acute with regard to the requirement to provide a detailed explanation of the basis for the denial and could create confusion for consumers. CDIA thus respectfully requests that businesses be granted the option to treat a request to correct in the same manner as a request to delete.

V. Requests to Limit Use and Disclosure of Sensitive Personal Information

Proposed section 7027(l)(3) permits businesses to use and disclose sensitive personal information in order to resist malicious, deceptive, fraudulent, or illegal actions directed at the business without requiring those businesses to offer consumers a right to limit. However, this exception does not clearly extend to a business’ efforts to prevent fraud or other malicious, deceptive, or illegal actions on other businesses. Conversely, the CPRA, at Civil Code, § 1798.121(a), provides for a broader exception, permitting the use and disclosure of sensitive personal information to help to ensure security and integrity. Cal. Civ. Code § 1798.140(e)(2).

CDIA members provide “security and integrity” services, like fraud detection and identity verification services, to their business customers. Providing these services may involve comparing inquiry data with data available elsewhere, detecting anomalies in provided data, and otherwise analyzing multiple data sets, all with the goal of detecting—and thus preventing—identity theft, fraud, and other illegal actions on businesses and consumers. These efforts reduce

business costs and protect consumers, whether such consumers are business customers or not, and thus further consumer privacy.

If fraud prevention services providers are unable even to use sensitive personal information to prevent fraud on third parties, consumer privacy may be affected significantly and detrimentally. CDIA strongly urges the CPPA to expand this exception to align with the CPRA and allow businesses to use sensitive personal information for fraud prevention and detection services related third parties to further consumer privacy and identity theft prevention efforts.

VI. Requests to Know or Delete Household Information

Section 7031 is proposed to be deleted in its entirety. This section provides for requirements under which consumers may provide requests with regard to household information, which is personal information under the CCPA. These requirements ensure that all members of the household agreed to such request, that the identity of all members would have to be verified, and that the members would have to be confirmed as current members of the household. Without this guidance, it is unclear how businesses would be expected to process household information requests, and whether businesses could deny such requests if they are unable to perform these reasonable checks to ensure the privacy of household members.

VII. Service Providers and Contractors and Contract Requirements

Proposed section 7051(a)(1) restricts service providers from selling or sharing personal information they collect on behalf of the businesses to which they provide services. Other subsections impose other restrictions, including on retaining, using, or disclosing personal information other than those specified in the service provider agreement, “unless otherwise permitted by the CCPA and these regulations,” like subsection (a)(3). CDIA members provide fraud detection and prevention services and may do so, in some contexts, as a service provider to a business. Those services may involve the disclosure of personal information received on behalf of the business to third parties in relation to providing fraud detection and prevention services. CCPA regulations—notably proposed section 7050(a)(4)—specifically permit service providers to process data in their position to “prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent, or illegal activity, even if this Business Purpose is not specified in the written contract required by the CCPA and these regulations.” In order to ensure that fraud prevention and detection service providers can continue to provide their important services related to minimizing identity theft and fraud on consumers and businesses, CDIA strongly urges the CPPA to add “unless otherwise permitted by the CCPA and these regulations” to subsection (a)(1), as it does with other contract requirements.

* * *

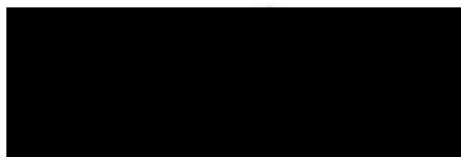
Brian Souble – California Privacy Protection Agency (CPPA)

November 20, 2022

Page 6

Thank you for the opportunity to share our views on the anticipated rulemaking under the CPRA. Please contact us if you have any questions or need further information based on comments.

Sincerely,



Eric J. Ellman

Senior Vice President, Public Policy & Legal Affairs

From: Pavan Kochar [REDACTED]
Sent: Sunday, November 20, 2022 3:33 PM
To: Regulations
Cc: Soltani, Ashkan [REDACTED]; Urban, Jennifer [REDACTED]
Subject: CPPA Public Comment: Data Brokers Threaten Worker Privacy
Attachments: Certree CPPA Letter 11.21.22.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear Mr. Soublet,

We write to inform you that several of the nation's largest data brokers, including Equifax and Experian, create unique harms to consumer privacy in California and exhibit a pattern of stifling competition in the employment and income verification space.

Every week, millions of US employers send their workers' detailed salary and employment data to giant data brokers, which then sell that data to lenders, landlords, debt collectors, and more. Employers do this to outsource the task of verifying employee records for third parties, but this system leads to flawed data, mass data breaches, and other threats to consumers' well-being. Moreover, most workers never give well-informed consent to this practice, and they have virtually no ability to opt out. Equifax alone collects payroll data on more than half of the entire US workforce. *Recently, these brokers have started to buy payroll data from payroll companies and employers, without employee consent or awareness, stifling competition that would benefit California consumers.*

The attached comment describes these dynamics in detail and calls for an investigation into these practices.

We hope that CCPA will continue to protect employee data from being sold by employers and payroll companies to data brokers. We thank you for your attention to this important matter, and we stand ready to address any comments or questions you may have.

My best,
-Pavan



Pavan Kochar
CEO

[REDACTED]
M: [REDACTED]
www.certree.com

November 21, 2022



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

Dear Mr. Soublet,

We write to express serious concern regarding the anti-privacy and anti-consumer practices of the nation's largest providers of verification services for income and employment backgrounds, as well as the near-ubiquitous collection and sale of payroll data, including personal identifiable information. We respectfully request that the California Privacy Protection Agency (CPPA) undertake an investigation of these practices and take them into account in future rulemakings under the California Consumer Privacy Act (CCPA).

The CCPA outlines several core rights that will extend to California workers beginning in January 2023.¹ These include the “right to know” how their data is used, the “right to delete” their personal information, and the “right to opt-out of sale” so that businesses cannot sell their personal data – all of which stand in direct opposition to major data brokers’ longstanding business practices.²

Using their historically dominant positions in the credit reporting industry, companies like Equifax and Experian have collected hundreds of millions of payroll records on everyday American consumers, which they sell to lenders, landlords, debt collectors, and other customers as part of their workforce verification services. More recently, these same data brokers have aimed to secure exclusive access to payroll data through partnerships with major HR software providers, effectively turning the market for payroll data into an oligopoly. In turn, this business model has created unique harms to consumer privacy, data security, choice, and financial security, and it has led to business practices that stifle innovation and competition.

For context, millions of employers send their workers’ income and employment data to large-scale data brokers.³ In theory, employers save money by

¹ Garhart, N. & Stephens, R. (2022, October 5). Employee Data Under the CCPA: Expiration of Employer Exemptions Requires Compliance as of January 1, 2023. Farella Braun + Martel LLP. ([link](#))

² California Privacy Protection Agency. Frequently Asked Questions (FAQs). ([link](#))

³ Chmura, C. (2022, February 15). A data broker has millions of workers' paystubs; see if they have yours. NBC Bay Area. ([link](#))

outsourcing the work of handling requests for employment and income verification from third parties, such as landlords, lenders, and potential employers. Rather than contacting an employer's human resources (HR) department to verify a worker's background, these third parties purchase employment and income data from brokers that collect and sell hundreds of billions of personal records.⁴ This verification system has dominated the California workforce for decades, partly because for many years, there was no clear alternative to this process.

However, new technologies are emerging every day that provide workers with safer, more secure, and more empowering tools to manage both their personal data and the verification process. For example, Certree provides workers with personal, private vaults where only they can review their data and safely share that tamper-free information with specific third parties with guaranteed authenticity. Yet companies like ours face enormous obstacles competing in a market where major players use their overwhelming scale and to undercut competitors. Meanwhile, Californians are suffering under a verification system in which workers are treated like products, not consumers.

In this letter, we discuss how:

- Brokers' employment verification services have dangerous ramifications for consumer privacy due to an abundance of inaccurate data and a systemic lack of consent that makes consumers bystanders in their own careers and financial lives.
 - Major data brokers use anti-competitive practices to weaken consumer power and extract premium pricing by securing exclusive access to payroll data.
 - The CCPA should investigate these practices, as they represent systemic threats to workers' privacy and digital security.
- 1. Between deceptive messaging around data uses, flawed data, and a systemic lack of well-informed consent, major brokers threaten consumer privacy and choice.**

In a January 2022 statement, Rohit Chopra, Director of the Consumer Financial Protection Bureau (CFPB), argued that "America's credit reporting oligopoly has

⁴ Equifax Inc., (2022). 2021 Annual Report ([link](#))

little incentive to treat consumers fairly.”⁵ That same statement highlighted how “consumers submitted more than 700,000 complaints to the CFPB regarding the nation’s largest data brokers from January 2020 through September 2021, which represented more than 50% of all complaints received by the agency for that period.”

A. Deceptive Practices

California’s largest credit agencies have a history of misleading everyday consumers. In 2005, for instance, Experian reached a settlement with the FTC after it was charged with deceiving consumers by offering a “free” credit report through a system that charged \$79.95 if customers did not cancel the service within 30 days.⁶ In another instance, major data brokers received CFPB fines totaling more than \$25 million in 2017 for “deceiving consumers in marketing credit scores.”^{7 8}

When it comes to the broad, unchecked uses of worker payroll data, Equifax has recently been telling one story to the public and an entirely different story to its investors. In August, Duke Senior Fellow Justin Sherman published an analysis that addressed Equifax Senior Vice President Joe Muchnick’s March 2022 interview with the Washington Post, in which he is quoted saying that the payroll data shared with The Work Number, the subsidiary that houses Equifax’s employment verification services, “is not passed on to other parts of Equifax, and is stored completely separately.”⁹ But as Sherman points out, Equifax boasts in its 2021 Annual Report that its data fabric “unifies more than 100 data silos into a single platform,” and the first dataset listed is The Work Number Database, which includes “136 million active payroll records, over 500 million historic records, from more than 2 million different US employers.”¹⁰ This integration is part of Equifax’s campaign to build a “360 degree consumer view” by providing

⁵ Consumer Financial Protection Bureau. (2022, January 5). CFPB Releases Report Detailing Consumer Complaint Response Deficiencies of the Big Three Credit Bureaus. Release. ([link](#))

⁶ Federal Trade Commission. (2005, August 16). Marketer of Free Credit Reports Settles FTC Charges. ([link](#))

⁷ Consumer Financial Protection Bureau. (2017, March 23). CFPB Fines Experian \$3 Million for Deceiving Consumers in Marketing Credit Scores. Release. ([link](#))

⁸ Consumer Financial Protection Bureau. (2017, January 3). CFPB Orders TransUnion and Equifax to Pay for Deceiving Consumers in Marketing Credit Scores and Credit Products. Release. ([link](#))

⁹ Sherman, J. (2022, August 24). Examining data broker Equifax’s relationships with millions of employers. Duke University’s Sanford School of Public Policy. ([link](#))

¹⁰ Equifax 2021 Annual Report ([link](#))

its corporate customers with data on a person's income, employment, education, credit, bank balances, criminal history, and more.¹¹

B. Flawed Data

When brokers collect and sell inaccurate data, it poses a huge threat to workers' well-being. In 2016 and 2017, for example, job seekers filed lawsuits against Starbucks claiming they were denied jobs at the company due to flawed data in their background checks.¹² Starbucks denied the charges but reached a class-action settlement with roughly 8,000 job seekers, with the largest settlements going to people who "were unable to get any job or a similar job for at least 30 days."¹³ And this is just one example of the types of lawsuits under the Fair Credit Reporting Act (FCRA) that have surged over the past ten years. Since 2011, the number of FCRA-related lawsuits has nearly tripled, reaching more than 5,400 lawsuits in 2021 alone.¹⁴

In the broker-centered system for verifying backgrounds, this type of large-scale data error is largely unavoidable. CNBC reports that major data brokers must now update more than one billion pieces of data every month.¹⁵ At this enormous scale, it is perhaps unsurprising that one FTC study of consumers, lenders, and brokers found that 21% of respondents had successfully disputed at least one data error in their reports.¹⁶ As a result of this faulty data, workers are denied opportunities for jobs, loans, apartments, and more every year.

And because the broker-centered model of employment verification completely bypasses the workers whose data is being verified, many workers never know that flawed data is the cause of these missed opportunities.

Moreover, even when consumers find errors in the data collected by major brokers, it can be nearly impossible to resolve those errors. According to a recent

¹¹ Equifax Decision 360. (2010, May 10). Decision 360. ([link](#))

¹² Thibodeau, P. & Holland, M. (2021, December 20). Employee background check errors harm thousands of workers. TechTarget. ([link](#))

¹³ Ibid.

¹⁴ True Hire.com (2022, May 12). FCRA lawsuits reach new record in 2021 after decade of steady increase. ([link](#))

¹⁵ Klein, A. (2017, September 27). The real problem with credit reports is the astounding number of errors. CNBC. ([link](#))

¹⁶ Federal Trade Commission. (2015, January). Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003. ([link](#))

CFPB report, “In 2021, the nation’s largest data brokers together reported relief in response to less than 2% of covered complaints.”¹⁷

C. Abuse of Consent and Inability to Opt Out

Despite the breadth of the broker-centered system for employment verification, many workers are unaware that their employers share their private salary data with major brokers. Earlier this year, the Washington Post outlined that many workers at Google were unaware their employer regularly shared their payroll data with Equifax’s The Work Number service, with Google workers identifying this practice as one of the top concerns they wanted executives to address.¹⁸ Around the same time, many Apple workers learned from national headlines that their employer recorded former workers as “associates” regardless of their actual titles.¹⁹ Once again, some workers were surprised to learn this inaccurate data was regularly shared with InVerify, a verification service owned by Equifax.

Payroll data is distinct in the discussion of digital privacy as workers have virtually no practical ability to opt out of this system. Equifax alone collects payroll data from most US employers, and other major brokers collect data on a sizable share of the remaining workforce.²⁰ Therefore, job seekers face a steep uphill climb to find a viable employer that is also willing to protect their digital privacy. As Justin Sherman argues in the same analysis discussed above, consumers “are forced to have their data collected, monetized, and shared in order to access employment opportunities.”²¹

Moreover, since the consent form for income verification is normally presented by a lender during the application process for a loan or mortgage, it is highly unlikely that most workers are presented with the full scope of how brokers like Equifax will use their data once the consent is granted. As noted above, Equifax is creating a “360 degree” view of consumers, and it is difficult to see how tens of millions of workers gave well-informed consent for their payroll data to be part of this venture.

¹⁷ Consumer Financial Protection Bureau. (2022, January 5). CFPB Releases Report Detailing Consumer Complaint Response Deficiencies.

¹⁸ Albergotti, R. & De Vynck, G. (2022, March 23). Tech workers are upset their companies are sharing payroll data with Equifax. Here’s what’s going on. The Washington Post. ([link](#))

¹⁹ Albergotti, R. (2022, February 10). Every employee who leaves Apple becomes an ‘associate’. The Washington Post. ([link](#))

²⁰ Chmura, C. (2022, May 6). Your Pay Stub is Probably in the Cloud; Silicon Valley Startup Recommends a ‘Vault’ Instead. NBC Bay Area. ([link](#))

²¹ Sherman, J. (2022, August 24). Examining Equifax’s relationships. Duke. ([link](#))

Sherman concludes his analysis of this broker-centered verification system saying that “a market [...] in which workers are essentially powerless to the sharing and monetization of their own information is not one in which that consent is full, informed, and freely given.”²²

Additionally, Equifax and Experian do not always directly verify the consent behind the data they sell. Rather, they often rely on intermediary data buyers to obtain that consent, and major brokers take it for granted that this consent is well-informed and authentic.

D. Pattern of Large-Scale Data Breaches

A lack of meaningful consent from workers, combined with clear incentives for brokers to collect and share as much data as possible, is especially dangerous because the nation’s largest brokers have a history of exposing the highly sensitive data they collect. In 2017, for example, Equifax announced a data breach that exposed the personal information of 147 million people.²³ An FTC investigation into this breach later noted Equifax’s “failure to take reasonable steps to secure its network.”²⁴ That same year, it was reported that hackers had begun using Americans’ dates of birth and Social Security Numbers, which had been exposed during the large-scale data breach, in order to change workers’ PIN numbers and steal their W-2s using Equifax’s Work Number subsidiary.²⁵ This security failure led to numerous independent breaches of worker data for employers such as Allegis, Northrop Grumman, Erickson Living, Saint-Gobain Group, and The University of Louisville, among others.²⁶

Experian has also struggled with data security. In August, Krebs on Security reported that Experian now faces a class-action lawsuit in the California Central District Court after the public learned that Experian “did little to prevent identity thieves from hijacking consumer accounts [...] simply by signing up for new accounts using the victim’s personal information and a different email

²² Ibid.

²³ Siegel Bernard, T. (2020, January 22). Equifax Breach Affected 147 Million, but Most Sit Out Settlement. The New York Times. ([link](#))

²⁴ Federal Trade Commission. (2019, July 22). Equifax to Pay \$575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach. Release. ([link](#))

²⁵ Krebs, B. (2017, May 18). Fraudsters Exploited Lax Security at Equifax’s TALX Payroll Division ([link](#))

²⁶ Ibid.

address.”²⁷ In 2021, Experian API exposed the credit scores of most Americans.²⁸ In 2020, close to 800,000 businesses’ private data was breached.²⁹ And in 2015, a breach at Experian exposed the Social Security numbers of roughly 15 million consumers.³⁰

With so much sensitive data held by just a few data brokers, it is perhaps unavoidable that these brokers would be perennial targets for both large-scale and amateur hackers. In Equifax’s 2021 Security Annual Report, the company even admits that it receives roughly 35 million cyber threats every single day.³¹

And with massive data breaches that expose consumers’ Social Security numbers, dates of birth, and other personal details, brokers are also arming fraudsters with all the information they need to hack consumer accounts.³²

Breaches like these have powerful and permanent consequences for individuals whose data is stolen and abused. And in this broker-centered market, workers are not consumers who can withhold spending to spur better security practices. Additionally, workers are not suppliers who can withhold their data. Rather, workers are treated as commodities with no influence over the system that buys and sells their personal data.

2. Major payroll data brokers use financial considerations, service bundling, and historically dominant market positions to secure exclusivity deals and stifle competition.

Payroll data has become a highly prized commodity for data brokers. Late last year, one market expert estimated the total addressable market for payroll connectivity and data software at roughly \$10 billion.³³ Alongside this development, brokers like Equifax and Experian have substantially increased the amount of payroll data they collect and sell, expanded the partnerships that supply them with payroll data, and found ways to combine payroll data with other information sources to undercut competitors.

²⁷ Krebs, B. (2022, August 5). Class Action Targets Experian Over Account Security. Krebs on Security. ([link](#))

²⁸ Krebs, B. (2021, April 28). Experian API Exposed Credit Scores of Most Americans. Krebs on Security. ([link](#))

²⁹ Reuters Staff. (2020, August 19). S.African fraudster tricks credit bureau Experian into handing over data. ([link](#))

³⁰ Krebs, B. (2015, October 2). Experian Breach Affects 15 Million Consumers. Krebs on Security. ([link](#))

³¹ Equifax Inc. (2022). 2021 Security Annual Report. ([link](#))

³² Krebs, B. (2017, October 8). Equifax Breach Fallout: Your Salary History. Krebs on Security. ([link](#))

³³ Pimentel, B. (2021, August 31). Payroll data is fintech’s \$10 billion ‘holy grail’. Protocol. ([link](#))

It is our understanding that these brokers even offer distinct financial incentives to employers to gain exclusive access to their workers' personal data. Our experience in this industry has yielded several conversations with salespeople, former executives, and other workers at these brokers' client companies, many of whom attest to "loyalty-rewards" that brokers offer to employers that consider ending their contracts and withholding their payroll data from these brokers. In some cases, we understand that brokers have offered to share the revenue derived from worker data with that worker's employer, often guaranteeing the employer a minimum amount of revenue. This system enables both the brokers and the employers to monetize a worker's most personal information, leading to the neglect of worker privacy, data security, and consumer choice.

A. Equifax

As early as 2017, it was reported that The Work Number collected payroll data on 85% of the federal government workforce, 75% of Fortune 500 companies, and countless state governments, agencies, courts, colleges, and small businesses.³⁴ As of 2022, Equifax collects payroll data on more than half of the entire US workforce, and the company claims to hold more than 250 billion personal records.³⁵

This immense scale is largely the product of partnerships, exclusivity deals, and acquisitions that inhibit competition. Intuit recently told the 1.4 million small businesses using its QuickBooks and Intuit Online Payroll Systems that their payroll information would be shared with Equifax.³⁶ In May, Equifax became the exclusive provider of income and employment verifications for Paycor, an HR software company that claims to support more than 2 million users.³⁷ On the Workforce Partners section of its website, Equifax states this new partnership means "Paycor has a secure integration connection to provide employee data each pay cycle..."³⁸ That same page lists more than 30 partners in HR software,³⁹

³⁴ Winston, J. (2017, November 8). Facebook and America's largest companies quietly give worker data to Equifax. Fast Company. ([link](#))

³⁵ Equifax 2021 Annual Report ([link](#))

³⁶ Krebs, B. (2021, July 1). Intuit to Share Payroll Data from 1.4M Small Businesses With Equifax. Krebs on Security. ([link](#))

³⁷ Paycor. (2022, May 4). Equifax Workforce Solution and Paycor Launch An Integrated Partnership To Automate Income and Employment Verification. PR Newswire. ([link](#))

³⁸ Equifax Inc. (n.d.). Workforce Solutions, Partner Network. ([link](#))

³⁹ Ibid.

including ADP (with more than 20 million users on its mobile platform alone)⁴⁰, Ceridian (5.1 million users),⁴¹ and PrismHR (2 million users)⁴², among others. Like Paycor, many of these partners agree to provide Equifax with direct access to the millions of payroll records they collect. Brokers like Equifax often buy payroll data without explicit consent from the payroll companies' customers, or from the employees of those corporate customers. Much of the time, these are exclusive arrangements.

All this adds Equifax's persistent efforts to concentrate the market by acquiring verification services that may challenge the company's access to consumer data. In fiscal 2021 alone, Equifax made acquisitions worth almost \$3 billion, including the purchase of employee screening and verification services HIREtech and i2Verify.⁴³

The incentives to seal off sources of payroll data are clear. In its 2021 Annual Report, Equifax described its Workforce Solutions segment, which broadly captures employee screening and verification, as "our fastest growing, highest margin and most valuable business [...] Workforce Solutions has grown from about 25% of our total revenue 3 years ago to over 40% in 2021 and will likely grow to over 50% of Equifax in the coming years."⁴⁴ Meanwhile, Equifax increased the price of its employment verification services by 31% between August 2020 and March 2022, forcing consumers applying for loans, mortgages, and apartment rentals to pay higher fees as part of their application process.⁴⁵

B. Experian

Similar to Equifax, Experian has made sizable acquisitions in the employment verification space. In fiscal 2020 alone, the company spent more than \$580 million in cash on acquisitions, including payroll data competitors like Tax Credit Co, Corporate Cost Control, and Emptech.⁴⁶ On its own, the acquisition of Tax Credit Co required "a cash consideration of US\$252m and contingent consideration of up to US\$110m, determined by revenue and profit

⁴⁰ ADP, LLC (2019, March 28). ADP Mobile App Surpasses 20 Million Registered Users as the Mobile-First Movement Arrives in the Workplace. PR Newswire. ([link](#))

⁴¹ Ceridian HCM Holding Inc. (2022, February 9). Ceridian Reports Fourth Quarter and Full Year 2021 Results. ([link](#))

⁴² PrismHR. (n.d.). About. ([link](#))

⁴³ Equifax 2021 Annual Report ([link](#))

⁴⁴ Equifax Inc. (2022). Notice of 2022 Annual Meeting and Proxy Statement. ([link](#))

⁴⁵ Wells, D. (2022, March 21). How The Work Number Cheats American Consumers. RealClearPolicy. ([link](#))

⁴⁶ Experian plc. (2021, May 19). Full-year financial report. Release. ([link](#))

performance.”⁴⁷ All this, combined with Experian’s data on over 300 million consumers,⁴⁸ culminated in the launch of Experian’s own employment verification service in May 2021.⁴⁹

Importantly, in addition to acquisitions and partnerships, Experian is also known to use its dominant market position to cut out competition by bundling its services or offering revenue-sharing to provide a lower overall cost to clients that small-scale competitors cannot match. Again, our experience in this industry has yielded several conversations with executives and industry experts who have described this practice.

Unprecedented market practices and broad uses of personal payroll data require investigation by the CPPA.

These practices pose a significant threat to worker safety, and they clash with the objectives of the CCPA, especially given the CCPA’s expanded worker protections that will go into effect in January 2023. The CPPA should investigate Equifax and Experian, including their respective employment verification services, market practices, and methods for collecting and selling payroll data. Specifically, the CPPA should seek answers from these brokers to the following questions:

- When your company collects or receives payroll data, is that data used for your company’s other business segments or any other purpose? Is that data aggregated, referenced, or used for any other business purposes or products?
- What processes does your company employ to ensure the income and employment data you sell is accurate?
- When an employer contracts with your employment verification services, are there any limits on how your company can use payroll records once the worker concerned has given consent?
- What steps do you take to ensure workers fully consent to all the potential and actual uses of their payroll data by your company?

⁴⁷ Experian plc. (2022). Experian Annual Report 2022. ([link](#))

⁴⁸ Experian plc. (2018). ConsumerView. ([link](#))

⁴⁹ Experian plc. (2021, May 24). Experian Announces New Employer Services Business and Real-time Income and Employment Verification Solution. businesswire. ([link](#))

- What steps do you take to ensure worker consent is authentic in order to prevent identity fraud and theft?
- Do you pay (or provide consideration to) employers that use your employment verification services in order to access their payroll data? If you do, are those relationships with employers exclusive?
- Has your company ever offered a financial incentive (or rebate) to a customer that was considering ending, or had already ended, their relationship with your employment verification service?
- Have you ever proactively influenced an employer to have them add financial reward or service bundling in its pending RFP?

When California Attorney General Rob Bonta announced a \$600 million settlement with Equifax in 2019, he decried that Equifax “had a responsibility to secure and protect Americans’ data. Instead, it breached public trust.”⁵⁰

As Federal Trade Commission Chair Lina Khan noted this year, “businesses’ access to and control over such vast troves of granular data on individuals can give those firms enormous power to predict, influence, and control human behavior. In other words, what’s at stake with these business practices is not just one’s subjective preference for privacy, but—over the long term—one’s freedom, dignity, and equal participation in our economy and society.”⁵¹

We wholeheartedly agree with their sentiments, and we thank you for your attention to this matter.

Respectfully Submitted,



Pavan Kochar
Chief Executive Officer, Certree

⁵⁰ Office of the Attorney General. (2019, July 22). Attorney General Becerra Announces Settlement Against Equifax Providing \$600 Million in Consumer Restitution and State Penalties. Release. ([link](#))

⁵¹ Khan, L. (2022, April 11). Remarks of Chair Lina M. Khan As Prepared for Delivery IAPP Global Privacy Summit 2022 Washington, D.C. ([link](#))

Cc:

Jennifer Urban

Board Chair, California Privacy Protection Agency

Ashkan Soltani

Executive Director, California Privacy Protection Agency

From: Ben Winters [REDACTED]
Sent: Sunday, November 20, 2022 3:53 PM
To: Regulations
Subject: CPPA Public Comment
Attachments: EPIC-CPPA-Comments-Nov 20.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good evening,

EPIC's comments to the CPPA in response to the Public Notice of Proposed Modifications and Additional Materials Relied Upon published on November 3rd are attached.

Please let me know if you have any questions or difficulties opening the attachment.

Best,
Ben Winters (pronouns: he/him)
Counsel
Electronic Privacy Information Center (EPIC)
[REDACTED]



Nov 20, 2022

California Privacy Protection Agency
2101 Arena Blvd
info@cppa.ca.gov

Re: CPPA rulemaking

Dear Chairperson Urban and Board Members de la Torre, Le, Mactaggart, and Thompson,

The Electronic Privacy Information Center (EPIC) writes to submit recommendations to the California Privacy Protection Agency (CPPA) published regulations on November 3, 2022. EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues and to protect privacy, the First Amendment, and constitutional values. EPIC supports the establishment of strong privacy rules to protect consumers from invasive commercial surveillance practices. EPIC has previously provided comments on the CCPA¹ and published a detailed analysis of the California Privacy Rights Act (CPRA) before its approval by California voters.²

In Fall 2021, EPIC and three peer organizations urged the CPPA to implement strong, privacy-protective regulations under the state's new data protection law. Specifically EPIC, Consumer Action, the Consumer Federation of America, and New America's Open Technology Institute urged the agency "to continue 'protect[ing] consumers' rights' and 'strengthening consumer privacy' at every opportunity, consistent with the expressed will of California voters." Specifically, we encouraged the agency "to impose rigorous risk assessment obligations on businesses whose data processing activities could reasonably harm individuals' privacy or security; to maximize the transparency of automated decision-making systems and minimize the burdens on individuals who wish to opt out of such systems; and to prevent any exceptions to user-directed limits on the use and disclosure of sensitive personal information from swallowing the rule." In June 2022, EPIC and five peer organizations urged the agency to promulgate strong rules regarding the use of Universal Opt-Out Mechanisms.³ In August 2022, EPIC, along with the California Public Interest Research Group Education Fund, Center for Digital Democracy, Consumer Action, the Consumer Federation of America, Ranking Digital Rights, and the U.S. Public Interest Research Group, sent comments to the

¹ Comments of EPIC to Cal. Office of the Att'y Gen. (Feb. 25, 2020), <https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf>; Comments of EPIC to Cal. Office of the Att'y Gen. (Dec. 6, 2019), <https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Dec2019.pdf>.

² EPIC, *California's Proposition 24* (2020), <https://epic.org/californias-proposition-24/>.

³ EPIC, *Six Consumer Protection Groups to CPPA: Global Opt-Outs Are Essential to Protect Consumers and Mandatory for Businesses Under the CPRA* (June 8, 2022) <https://epic.org/epic-coalition-commend-cppa-for-affirming-obligation-for-global-opt-out-signal/>

agency regarding proposed regulations under the California Consumer Privacy Act.⁴ We focused in particular on the need to strengthen the substantive restrictions on expansive and exploitative data collection in the online ecosystem. We stressed that “Californians’ most urgent need is not for more notices about their rights; it is for substantive, meaningful limitations on the use and disclosure of their sensitive personal information.”

In this letter, EPIC will provide further responses and recommendations to the proposed regulations in sections 7002, 7004, 7011, 7012, 7022, 7023, 7027, 7050, and 7052. Specifically, we believe that the agency should modify these proposed regulations to:

- Further clarify and strengthen the data minimization rules.
- Clarify that businesses providing services to nonbusiness are still subject to the regulations, and further specifying contractor obligations.
- Restore the deleted examples about symmetry of choice and manipulative choice architecture in the consumer consent section.
- Avoid ambiguity in methods for calculating the value of consumer data.
- Ensure that businesses disclose all purposes for using sensitive personal information.
- Require that Notice at Collection of personal information should include an initial, short-form notice.
- Make clear that consumer requests to delete or correct data will be passed through to and honored by third parties.
- Expressly restrict the collection and processing of sensitive data beyond strictly necessary and enumerated purposes.

Throughout this comment, EPIC provides suggested edits to revised proposed regulatory text in *italics* and ~~strikethrough~~.

EPIC recommends the agency further refine the data minimization rule in §7002 to avoid ambiguity and make clear that consent is not an adequate independent basis to collect and process data.

In our comments on the initial draft regulations, we urged the agency to prohibit businesses from processing personal information in ways that are incompatible with the reasonable expectations of consumers and with the context in which the data was collected. EPIC commends the CPPA for modifying the proposed rules in §7002 to strengthen these restrictions. However, we are concerned that certain provisions in the revised proposed regulations could be ambiguous or confusing. We are also concerned that under the proposed regulations consent would still act as an independent basis to collect and process data, rather than being one of many factors to consider.

We believe that §7002 of the regulations could be clarified and strengthened in the following ways:

⁴ Comments of EPIC et. Al to Cal. Priv. Protec. Agency (Aug. 23, 2020) available at <https://epic.org/documents/epic-comments-cppa-aug2022/>

- Revise the second subparagraph of §7002(c) to simplify the clause and make the meaning clear. The purpose of the subparagraph appears to be that the other disclosed purpose should be compared with the list of business purposes in §1798.140(e) and that being within that scope of one of those enumerated purposes weighs in favor of compatibility.
- Delete the third subparagraph in §7002(c) and move the example up to the second paragraph. It is not clear what the agency means by the “strength of the link between subsection(c)(1) and subsection (c)(2).” The preamble in subsection (c) already states that the standard is whether the other disclosed purpose is “compatible with the context” based on the two factors in (c)(1) and (c)(2), so the current third subsection is not necessary. And the example should illustrate how the
- Move §7002(e) into a new subparagraph (3) of §7002(c). The consent provision in E should not be an independent basis for which to collect or process data, but it should be considered as a factor in evaluating the compatibility of another disclosed purpose. The act of obtaining the consumer’s consent under section 7004 will necessarily involve disclosing the new purpose, and consent can therefore be factored into the compatibility analysis under §7002(c).
- Revise §7002(d) to simplify the preamble and make it clear that the subparagraphs are factors that businesses should evaluate to determine whether their purposes are necessary and proportionate. As currently written the preamble and subparagraphs are difficult to parse and do not provide a sufficiently clear instruction of how to evaluate the factors.

EPIC recommends that §7002 be revised as follows:

§ 7002. Restrictions on the Collection and Use of Personal Information

* * *

(c) Whether another disclosed purpose is compatible with the context in which the personal information was collected shall be based on the following:

(1) At the time of collection of the personal information, the reasonable expectations of the consumer(s) whose personal information is collected or processed concerning the purpose for which their personal information will be collected or processed, based on the factors set forth in subsection (b) *For example, when a consumer uses a map app, the app may collect and use her personal information, including her location data, to optimize the best route to her destination and may retain that information for the limited purpose of suggesting that destination to the consumer again. These purposes are sufficiently within consumer expectation for the original purpose of the data collection and the secondary uses.*

(2) The other disclosed purpose for which the business seeks to further collect or process the consumer’s personal information, including whether it is a Business Purpose listed in Civil Code section 1798.140, subdivisions (e)(1) through (e)(8). *For example, when a consumer expects that their personal information is used to provide them with a requested service at the time of collection, the later use of that information to repair errors that impair the intended functionality of that requested service would be*

compatible. By contrast, for example, a consumer whose personal information is provided to a requested cloud storage service at the time of collection may not expect that their personal information will later be used to research and develop a facial recognition service.

~~(3) The strength of the link between subsection (c)(1) and subsection (c)(2). Whether a business has obtained the consumer's consent in accordance with section 7004 before collecting or processing personal information for any purpose that does not meet the requirements set forth in subsection (a).~~

~~For example, a strong link exists between the consumer's expectations that the personal information will be provided to a company for with a requested service at the time of collection, and the use of the information to repair errors that impair the intended functionality of that requested service are sufficiently related to a consumer's reasonable expectation when. This would weigh in favor of compatibility. By contrast, for example, a weak link exists between the consumer's reasonable expectations that the personal information will be collected to provide a requested cloud storage service at the time of collection, and the use of the information to research and develop an unrelated facial recognition service.~~

~~(d) For each purpose identified in subsection (a)(1) or (a)(2), the collection, use, retention, and/or sharing of a consumer's personal information to achieve that purpose shall be reasonably necessary and proportionate. The business's collection, use, retention, and/or sharing of a consumer's personal information shall also be reasonably necessary and proportionate to achieve any purpose for which the business obtains the consumer's consent in compliance with subsection (e).~~ Whether a business's collection, use, retention, and/or sharing of a consumer's personal information is reasonably necessary and proportionate to achieve the purpose identified in subsection (a)(1) or (a)(2), ~~or any purpose for which the business obtains consent~~, shall be based on the following:

(1) The minimum personal information that is necessary to achieve the purpose identified in subsection (a)(1) or (a)(2), ~~or any purpose for which the business obtains consent~~. For example, to complete an online purchase and send an email confirmation of the purchase to the consumer, an online retailer may need the consumer's order information, payment and shipping information, and email address.

(2) The possible negative impacts on consumers posed by the business's collection or processing of the personal information. For example, a possible negative impact of collecting precise geolocation information is that it may reveal other sensitive personal information about the consumer, such as health information based on visits to

healthcare providers.

(3) The existence of additional safeguards for the personal information to specifically address the possible negative impacts on consumers considered by the business in subsection (d)(2). For example, a business may ~~consider~~ *use* encryption or automatic deletion of personal information within a specific window of time as potential safeguards

~~(e) A business shall obtain the consumer's consent in accordance with section 7004 before collecting or processing personal information for any purpose that does not meet the requirement set forth in subsection (a).~~

EPIC recommends the agency to restore the examples in §7004 that clarify specific categories of harmful choice architecture.

The agency in its revisions to the proposed regulations has removed several examples that provide helpful guidance on harmful choice architecture. For example, the illustrative in 7004(a)(4)(A) that described user interface phrasing designed to shame a consumer into making a choice that benefits the company and discourages exercise of consumer rights had provided useful clarification.⁵ Similarly, the two examples related to “symmetry in choice” in subsections 7004(a)(2)(E) and (F) were useful examples of improperly manipulative presentation of choices that would encourage consumers to click yes or pass through without making a meaningful choice. EPIC urges the CPPA to keep these original examples.

EPIC recommends the agency not permit too much variation in business' calculation of the value of consumer data in §7081.

EPIC is concerned about how the revised draft regulations permit businesses to use indeterminate and untested methods to calculate the value of consumer data in the good-faith provision. The use of this provision is likely to lead to businesses' significantly undervaluing consumer data or valuing some consumers' data more than others. We would recommend deleting clause (8) from § 7081(a), and the CPPA adjust it to reflect the following:

§ 7081. Calculating the Value of Consumer Data

(a) A business offering a financial incentive or price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer's data. The business shall consider one or more of the following:

⁵ “When offering a financial incentive, pairing choices such as, “Yes” (to accept the financial incentive) with “No, I like paying full price” or “No, I don’t want to save money,” is manipulative and shaming.

- (1) The marginal value to the business of the sale, collection, or deletion of a consumer's data.
- (2) The average value to the business of the sale, collection, or deletion of a consumer's data.
- (3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers.
- (4) Revenue generated by the business from sale, collection, or retention of consumers' personal information.
- (5) Expenses related to the sale, collection, or retention of consumers' personal information.
- (6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference.
- (7) Profit generated by the business from sale, collection, or retention of consumers' personal information.
- ~~(8) Any other practical and reasonably reliable method of calculation used in good faith.~~

EPIC recommends the agency explicitly require in §7011 that businesses disclose all purposes for using sensitive personal information.

The proposed regulations rely in many cases on the representations of businesses regarding the purpose and means of their collection of personal information. The contents of the privacy policies posted by businesses are an important mechanism by which to evaluate the businesses claims about their data practices and to ensure that consumers are adequately protected. The agency should add specific provisions to the "Information Practices" section of the privacy policy requirements to ensure that the sensitive personal information protections are operationalizable and to ensure that consumers do not lose out when businesses make material changes to their policies. We recommend that the following two subparagraphs be added to subsection 7011(e)(1):

§7011. Privacy Policy.

(e) The privacy policy shall include the following information:

- (1) A comprehensive description of the business's online and offline Information Practices, which includes the following:

(L) Identification of the specific business or commercial purpose for which the business uses or discloses sensitive personal information regardless of whether it falls within a §7027(L) exception or not.

(M) A log of material changes retained as copies of previous versions of its privacy policy for at least 10 years beginning after the date of enactment of this Act and publish them on its website. The business shall make publicly available, in a clear, conspicuous, and readily accessible manner, a log describing the date and nature of

each material change to its privacy policy over the past 10 years. The description shall be sufficient for a reasonably individual to understand the material effect of each material change.

EPIC recommends that notice at collection of personal information should include an initial, short-form notice in §7012.

While EPIC commends the agency for its work to refine the guidance for initial collection notices, we recommends that the agency include a requirement for short-form notice in certain circumstances. Consumers interact with so many businesses every day that they cannot meaningfully review even clear terms included in longer form notices. The most effective way to communicate an overview of individual rights and disclosures required for Notice and Collection at the initial stage is, in many cases, through a short-form notice. We recommend that the agency add a new subsection on short-form notice at the end of section 7012 as follows:

§7012 Notice at Collection of Personal Information

(j) At or before the point of collection, the business shall provide a short-form notice of the categories of personal information to be collected from them, the purposes for which the personal information is collected or used, and whether the personal information is sold or shared. The business must provide a short-form notice of the business' covered data practices in a manner that is concise, clear, conspicuous, and not misleading. The short-form notice should be readily accessible to the individual, based on what is reasonably anticipated within the context of the relationship between the individual and the large data holder. The short-term notice shall be inclusive of an overview of individual rights and disclosures to reasonably draw attention to data practices that may reasonably be unexpected to a reasonable person or that involve sensitive covered data and no more than 500 words in length. The business should provide further notice by linking directly to the privacy policy. For example, a mobile app user is prompted with a short-form notice that informs them the categories of personal information to be collected from them, the purposes for which it is collected, and whether it is sold or shared the first time that the user uses the app.

EPIC recommends the agency make clear in §§7022-7023 that consumer requests to delete or correct data will be passed through to and honored by third parties.

The regulations governing consumer requests to delete or correct their data need to make clear that businesses are obliged to pass such requests through to third parties as appropriate and that such third parties are required to comply. We believe that the following modifications to sections 7022 and 7023 are necessary to ensure that these notifications and obligations flow to third parties.

§7022. Requests to Delete.

(c) A *business*, service provider, contractor, *or third party* shall, with respect to personal information that they collected pursuant to their written contract with the business and upon notification by the business, cooperate with the business in responding to a request to delete by:

(d) If a business, service provider, contractor, *or third party* stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the 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.

(f) In cases where a business denies a consumer's request to delete in whole or in part, the business shall do all of the following:

(4) Instruct *all* service providers, *contractors, or third parties* to delete the consumer's personal information that is not subject to the exception and to not use the consumer's personal information retained for any purpose other than the purpose provided for by that exception.

§7023. Requests to Correct.

(c) A business that complies with a consumer's request to correct shall correct the personal information at issue on its existing systems. The business shall also instruct all service providers and contractors that maintain the personal information at issue pursuant to their written contract with the business to make necessary corrections in their respective systems. Service providers and contractors shall comply with the business's instructions to correct the personal information or enable the business to make corrections. If a business, service provider, or contractor stores any personal information that is the subject of the request to correct on archived or backup systems, it may delay compliance with the consumer's request to correct, with respect to data stored in the archived or backup system, until the archived or backup system relating to that data is restored to an active system or is next accessed or used. *The business shall also instruct all third parties to which it has sold or shared the personal information at issue to make the necessary corrections in their systems. Third parties shall comply with the business' instructions to correct the information and should take steps to ensure that the personal information at issue remains corrected. For example, if Business N has sold or shared personal information to a third party and Business N later receives a request to correct from a consumer. Business N complies and corrects the personal information in its system and notifies the third party of the correction.*

EPIC recommends the agency add an explicit and affirmative limitation of disclosure of sensitive data in §7027.

Excessive data collection and retention can be particularly harmful when it includes sensitive personal information. As EPIC explained in its comments on the initial draft regulations, “Consumers should be protected from the harms associated with the collection, use, and disclosure of their sensitive personal information regardless of whether they have taken steps to prevent this harm.”⁶ Therefore, the right to limit should not be the only rule specifically restricting the collection, processing, and sale of sensitive personal information. The rules for handling sensitive personal information should be more restrictive than those for non-sensitive information, and the structure of the CPPA as amended supports this construction. We recommend that the Agency promulgate rules that substantively restrict the permissible purposes for using sensitive data to read as follows:

§7027 ~~Requests to Limit~~ *Prohibition Against the* Use and Disclosure of Sensitive Personal Information

(a) The unauthorized use or disclosure of sensitive personal information creates a heightened risk of harm for the consumer. *Therefore, businesses should limit the use and disclosure of sensitive personal information to what is necessary to perform the function for which it was collected with certain limited exceptions set forth in (m).* The purpose of the *prohibition against the use and disclosure of sensitive personal information is to protect how consumers’ 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~~ limits 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 (m). *The consumer should have the right 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, or is necessary to carry out one of the purposes set for in subsection (m).* Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to ~~requests to limit the prohibition.~~

(m) *The exceptions for which a business may use or disclose sensitive personal information are as follows.* The purposes identified in Civil Code section 1798.121, subdivision (a), 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, provided that the use or disclosure *is necessary to perform the services or provide the goods reasonably expected by an average consumers who requests those goods or services,* reasonably necessary and proportionate to

⁶ Comments of EPIC et. Al to Cal. Priv. Protec. Agency (Aug. 23, 2020) available at <https://epic.org/documents/epic-comments-cppa-aug2022/>

for those purposes, is not required to post a Notice of Right to Limit or provide a method for submitting a request to limit.

(1) To perform the services or provide the goods reasonably expected by an average consumer who requests those good or services *to the consumer who requests the goods or services whose sensitive personal information is being used or disclosed*. For example, a consumer's precise geolocation may be used by a mobile application that is providing the consumer with directions on how to get to specific location. A consumer's precise geolocation may not, however, be used by a gaming application where the average consumer would not expect the application to need this piece of sensitive personal information.

(4) To ensure the physical safety of natural persons *prevent an individual, or group of individuals, from suffering harm where the business believes in good faith that the individual, or group of individuals, is at risk of death, serious physical injury, or other serious health risk, provided that the use of the consumer's personal information is reasonably necessary and proportionate for this purpose*. For example, a business may disclose a consumer's geolocation information to law enforcement to ~~investigate~~ *locate the victim of an* alleged kidnapping *to prevent death or serious physical injury*.

(7) To verify or maintain the quality or safety of a product, service, or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the business, *provided that the service or device being maintained, repaired, or enhanced was the purpose for which the sensitive data was being collected*. For example, a car rental business may use a consumer's driver's license for the purpose of testing *insofar as it is reasonably necessary to test* that its internal text recognition software accurately captures license information in car rental transactions.

EPIC supports the clarification in §7050 that businesses providing services to nonbusiness are still subject to the regulations, and recommends further specifying contractor obligations in §7052.

EPIC commends and supports the CPPA clarifying that businesses providing services to nonbusinesses are *not* exempt from requirements under the regulations, as articulated in the revised proposed text of subsection 7050(g).

We recommend that section 7052 be updated to clarify that third parties must comply not only with deletion and opt out requests from consumers, but correction and access requests as well. EPIC recommends the regulation be adjusted to the following:

§ 7052 Third Parties

(b) A third party shall comply with the terms of the contract required by the CCPA and these regulations, which include treating the personal information that the business made available to it in a manner consistent with the business's obligations under the CCPA and these regulations, *including deletion and opt-out request from consumers*.

Conclusion

The agency's proposed regulations would establish important protections for Californians and EPIC supports their promulgation. Our recommendations above are intended to ensure that the agency's regulations establish clear and strong rules that can help to limit the spread of invasive commercial surveillance practices in California.

x [REDACTED]
Alan Butler
EPIC Executive Director

x [REDACTED]
John Davisson
EPIC Litigation Director

X [REDACTED]
Sara Geoghegan
EPIC Counsel

x [REDACTED]
Caitriona Fitzgerald
EPIC Deputy Director

x [REDACTED]
Ben Winters
EPIC Counsel

x [REDACTED]
Suzanne Bernstein
EPIC Law Fellow

From: Kevin Gould [REDACTED]
Sent: Sunday, November 20, 2022 6:22 PM
To: Regulations
Subject: CCPA Public Comment -- CCPA CPRA Modifications to Text of Proposed Regulations Comment Letter
Attachments: CCPA CPRA Modifications to Text of Proposed Regulations Comment Letter.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Thank you for the opportunity to provide comments on the modifications to the text of the proposed regulations implementing the California Privacy Rights Act of 2020. Please let us know if you have any questions regarding our attached comment letter. Thank you.



Kevin Gould
EVP, Director of Government Relations
California Bankers Association
1303 J Street, Suite 600 | Sacramento, CA 95814
T: [REDACTED]
F: [REDACTED]

November 20, 2022

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Boulevard
Sacramento, CA 95834
regulations@coppa.ca.gov

RE: Comments on Modified Text of the Proposed Regulations Implementing the California Privacy Rights Act of 2020

Dear Mr. Soublet:

The California Bankers Association (CBA) appreciates the opportunity to submit comments to the California Privacy Protection Agency (Agency) on the modifications to the text of the proposed regulations implementing the California Privacy Rights Act of 2020. CBA is one of the largest banking trade associations in the United States advocating on legislative, regulatory, and legal matters on behalf of banks doing business in California.

The Proposed Regulations are Inconsistent and Go Beyond the Statute in Several Areas.

We wish to thank the Agency and express our appreciation for modifications to the text of the proposed regulations that are responsive to comments we previously provided. However, we respectfully urge the Agency to re-consider comments from our letter dated August 23, 2022, since the modified text of the proposed regulations do not address a number of issues we raised.

We remain concerned with provisions that are inconsistent or go beyond the statute, and we respectfully request that such provisions either align with the statute or be deleted. We refrain from restating the entirety of our previous arguments and instead encourage the Agency to review our August 23, 2022, letter which contains a more detailed analysis and justification in each of the four sections referenced immediately below.

➤ Section 7025: Opt-Out Preference Signals.

The draft regulations require businesses to provide opt-out links on their internet homepage and to honor universal opt-out preference signals. We urge that the regulations align with the statute, thereby permitting businesses the option granted in statute.

➤ Section 7026: Requests to Opt-Out of Sale/Sharing.

This section requires a business to comply with a request to opt-out of the sale or sharing of personal information by notifying “all third parties to whom the business has sold or shared the consumer’s personal information” of the consumer’s request to opt-out of the sale or sharing and to forward the consumer’s opt-out request to “any other person to whom the third party has made the personal information available during that time period.” These requirements go beyond the statute and should be deleted.

➤ Section 7051: Contract Requirements for Service Providers and Contractors.

This section requires that agreements between a business and service provider or contractor identify specific purposes for which personal information is disclosed, which cannot be described in “generic terms” and states that a business that never enforces the terms of its contract nor exercises its rights to audit or test might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intended to use the personal information in violation of the California Consumer Privacy Act (CCPA). These provisions go beyond statutory requirements and should be removed.

➤ Section 7053: Contract Requirements for Third Parties.

The draft regulations require that a business identify, in each agreement, the specified purpose for which personal information is made available to the third party and states that a business that never enforces the terms of its contract might not be able to rely on the defense that it did not have reason to believe that the third party intended to use the personal information in violation of the CCPA. These provisions go beyond statutory requirements and should be removed.

Section 7002: Restrictions on the Collection and Use of Personal Information.

Section 7002(b) adds a standard “consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed”, that goes beyond the statute. Civil Code Section 1798.100(c) states that a “business’ collection, use, retention, and sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.”

The new standard shifts focus from the business’s purpose for collecting the personal information to the consumer’s perception of an allowable use of the personal information. This

shift in focus is unnecessary because the purpose for collecting personal information has already been disclosed to the consumer.

Section 7002(d)(2)-(3) contains factors to determine whether a business's collection, use, retention, and/or sharing of a consumer's personal information is reasonably necessary and proportionate. 7002(d)(2) includes a factor of the "possible negative impacts on consumers posed by the business's collection or processing of personal information" and 7002(d)(3) requires the consideration of the "existence of additional safeguards for the personal information to specifically address the possible negative impacts on consumers considered by the business in subsection (d)(2)."

Collecting only the minimum personal information necessary to achieve the purpose for collecting the information as provided for in 7002(d)(1) is an appropriate way to ensure that the collection is reasonably necessary and proportionate. However, the additional provisions in 7002(d)(2)-(3) suggest that possible negative impacts on consumers without additional safeguards could mean that no amount of information is reasonably necessary and proportionate to meet the business's purposes, going beyond what is anticipated by the statute.

Section 7002(e) now requires the consumer's "consent" before collecting or processing personal information for any purpose that does not meet specified requirements. To the contrary, Civil Code Section 1798.100(a)(1) permits the collection or use of personal information for additional purposes that are incompatible with the disclosed purposes as long as the business notifies the consumer of the additional purposes. Accordingly, we believe requiring "consent" goes beyond the statute. We urge that the regulations be consistent with the statute by requiring notice, not consent.

Section 7012: Notice at Collection of Personal Information.

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

The highly prescriptive nature of these notice requirements is inconsistent with the statute and increases consumer confusion. The requirement that the notice at collection direct consumers to a specific section of the privacy policy, rather than the beginning, fails to account for the fact that multiple sections of a privacy policy may be relevant. Additionally, these requirements complicate efforts to provide transparent notices, particularly where a business is subject to additional privacy frameworks. We request that this requirement be removed.

Section 7023: Requests to Correct.

Section 7023(k) states that, “Failing to consider and address the possibility that corrected information may be overridden by inaccurate information subsequently received from a data broker may factor into whether that business, service provider, or contractor has adequately complied with a consumer’s request to correct.”

This section is vague because it raises the possibility that a business is in violation of the law if it doesn’t “address the possibility” that corrected information may be overwritten. The section does not provide any guidance for how a business should go about addressing the possibility. Further, this section is unnecessary because the consumer has multiple opportunities to request their information and ask for it to be corrected. Tracking what information was corrected for which consumer to prevent that data from being overwritten is overly burdensome.

Section 7026: Requests to Opt-Out of Sale/Sharing.

Section 7026 applies to personal information that a business sells or shares. This section should not apply to information that a business “makes available” to a third party. Accordingly, the language in 7026(a) should follow the original draft and more accurately state “personal information that it *sells to or shares with* third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of sale/sharing.” (emphasis added).

Section 7027: Requests to Limit Use and Disclosure of Sensitive Personal Information.

Section 7027(a) includes new language where sensitive personal information “that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to requests to limit.” We request that the Agency provide more guidance on how businesses determine whether personal information is used for inferences.

Section 7027(m) states that a “business that only uses or discloses sensitive personal information for these purposes, provided that the use or disclosure is reasonably necessary and proportionate for those purposes, is not required to post a Notice of Right to Limit or provide a method for submitting a request to limit.”

Civil Code Section 1798.121(a) allows businesses to use sensitive personal information, without offering the right to limit, in three circumstances: 1) consistent with consumer expectations; 2) for certain purposes set forth in the definition of “business purpose” in Civil Code Section 1798.140(e); and, 3) additional purposes authorized by regulation. We request that “provided that the use or disclosure is reasonably necessary and proportionate for those purposes” be deleted as this limitation goes beyond the statute.

Employee and Business-to-Business Data.

The modified regulations lack guidance related to the expiration of the employee and business-to-business exemptions in Civil Code Section 1798.145(m)-(n), respectively. Beginning January 1, 2023, the CCPA will apply to employee personal information and personal information belonging to an employee or other individual associated with another legal entity involved in a commercial transaction with a business.

Applying the CCPA to employee and business-to-business data will create compliance challenges not easily solved without guidance. The consumer focus of the law and its regulations makes applying the law to non-consumer data impractical, impossible, or unreasonable. We respectfully request that the Agency issue guidance regarding CCPA obligations with respect to employee and business-to-business data.

Thank you for the opportunity to comment on the modifications to the text of the proposed regulations.

Sincerely,

A black rectangular redaction box covering the signature of Kevin Gould.

Kevin Gould
EVP/Director of Government Relations