

---

**From:** Sara Roos [REDACTED]  
**Sent:** Sunday, July 7, 2024 8:10 PM  
**To:** Regulations@CPPA  
**Cc:** Info@coppa  
**Subject:** Public Comment on Data Broker Registration Regulations  
**Attachments:** To Members of the CPPA Whom It May Concern.docx

---

**This Message Is From an Untrusted Sender**

Warning: This email **originated from outside of the organization!** Do not **click links**, open attachments, or reply, unless you **recognize the sender's** email.

[Report Suspicious](#)

attached.

*Thank you.*

-Sara Roos, LACDP elected delegate from AD55, CDP Children's Caucus Chair (for identification purposes only); *on behalf of two others, names available upon request.* @font-face {font-family:"Cambria Math"; panose-1:2 4 5 3 5 4 6 3 2 4; mso-font-charset:O; mso-generic-font-family:roman; mso-font-pitch:variable; mso-font-signature:-536870145 1107305727 0 0 415 O;}@font-face {font-family:Aptos; panose-1:2 1104 222224;mso-font-charset:O; mso-generic-font-family:swiss; mso-font-pitch:variable; mso-font-signature:536871559 3 0 0 415 O;}p.MsoNormal, li.MsoNormal, div.MsoNormal {mso-style-unhide:no; mso-style-qformat:yes; mso-style-parent:""; margin-top:6.0pt; margin-right:Oin; margin-bottom:6.0pt; margin-left:Oin; mso-pagination:widow-orphan; font-size:12.0pt; font-family:"Aptos",sans-serif; mso-ascii-font-family:Aptos; mso-ascii-theme-font:minor-latin; mso-fareast-font-family:Aptos; mso-fareast-theme-font:minor-latin; mso-hansi-font-family:Aptos; mso-hansi-theme-font:minor-latin; mso-bidi-font-family:"Times New Roman"; mso-bidi-theme-font:minor-bidi; mso-font-kerning:1.0pt; mso-ligatures:standardcontextual;}MsoChpDefault {mso-style-type:export-only; mso-default-props:yes; mso-ascii-font-family:Aptos; mso-ascii-theme-font:minor-latin; mso-fareast-font-family:Aptos; mso-fareast-theme-font:minor-latin; mso-hansi-font-family:Aptos; mso-hansi-theme-font:minor-latin; mso-bidi-font-family:"Times New Roman"; mso-bidi-theme-font:minor-bidi;}div.WordSection1 {page:WordSection1;}

July 7, 2024

California Privacy Protection Agency  
Attn: Elizabeth Allen  
2101 Arena Boulevard  
Sacramento, CA 95834

via email: [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

## re: Public Comment on Data Broker Registration Regulations

To Members of the CPPA Whom It May Concern:

I am concerned with the subset of 'consumer privacy' that includes minors – and in particular with respect to their data collected through third-party, educational institutions.

Beyond the "informed consent" aspect of assuring minor's data becomes available only 'knowingly', with their "consent"\*, I am concerned with the *disposition* of personal, identifiable, and potentially prejudicial data of a minor's. These data are routinely entrusted - often involuntarily (so "informed consent" really has a different meaning in this context) - with an educational institution, whether PK, K12 or post-secondary, public or private. And while these institutions are covered by the federal Family Educational Rights and Privacy Act (FERPA) and California's Student Online Personal Information Protection Act (SOPIPA) in terms of the commercialization of K12 users (customers), I believe the laws miss an accountability component. I believe they are silent on the matter of responsibility for the students whose data is managed by these institutions and their vendors, and the breaches to the security of these student's data, which is evidently inevitable: seemingly a feature not a bug.

What happens to a student's privacy right around their data, entrusted with an educational institution, when increasingly it is handled by a third-party vendor? Such vendors are contracted to aggregate, warehouse, control and repackage data for individuals, families, teachers and school administrators. Handling of this data is vulnerable as always to ransacking - it can be ransomed, monetized, shared or otherwise lost control of by the minor-subject themselves. If that data should be unsafely or improperly managed, how is accountability for a third-party managed? What are the consequences and sequelae for an individual when a third party is instrumental in this betrayal?

Some of the spur for these concerns come from the recent breaches at LAUSD. Certainly districts and schools, large and small, [across the country](#)<sup>1</sup> have been impacted by security [breaches](#)<sup>2</sup> in their data systems. But I am particularly aware of the recent revelations that large amounts of [student data is available](#)<sup>3</sup> on the "dark web", apparently unrelated to LAUSD's earlier [data breach](#)<sup>4</sup> of 2022. What data breach *is* linked to this new release?

<sup>1</sup> <https://www.k12six.org/map>

<sup>2</sup> <https://www.npr.org/2024/03/12/1237497833/students-schools-cybersecurity-hackers-credit>

<sup>3</sup> <https://www.latimes.com/california/story/2024-06-07/lausd-investigates-claims-that-student-and-teacher-data-are-for-sale-on-the-dark-web>

<sup>4</sup> <https://www.latimes.com/california/story/2023-02-22/lausd-cyber-attack-includes-at-least-2-000-student-records>

During this time frame, LAUSD has [contracted](#)<sup>5</sup> for a huge artificial intelligence project with an inexperienced - and now [reportedly](#)<sup>6</sup> collapsed - startup, [AllHere](#)<sup>7</sup>. Coincident with these data breaches and the promiscuity of allied data contractors in our children's protected educational space, the vulnerability of student's and family's private data to failures of a tangential third party are [manifest](#)<sup>8</sup>. To date, LAUSD has neither confirmed nor denied publicly the data breaches to its contractors.

Is it possible to devise regulation in such a way that could hold educational institutions and their contracted distant vendors more tightly accountable for data they manage, including the training of AI systems, like that utilized by AllHere's "Ed the AI chatbot"? This regulation is imperative, given the data's particularly sensitive nature, originating with a minor. I worry that the ordinary contracts which govern educational institution's RFPs do not encompass the very particular protection required of minor's data in a fluid, rapidly evolving technological landscape.

Thank you for considering the implications to our students of these data breaches and the complicated systems that must now handle so much student data. I have been discussing these issues with two others: a fellow LAUSD dad and computing expert, in addition to a fellow LACDP delegate active around Prop 24-privacy matters. But none of us is an expert, maven or even especially knowledgeable about specifics regarding education or privacy law. We have a concern and see a vulnerability, and are hoping to alert experts within the legal system, to our shared obligation for protecting and incentivizing the safety of our kids' privacy and their valuable data. We stand ready to help in any way possible; we are hoping you might have creative access to a regulatory solution.

Yours,

-Sai'a Roos, LACDP elected delegate from AD55, CDP Children's Caucus Chair (for identification purposes only); *on behalf of two others, names available upon request.*



\* [AB 1949](#)<sup>9</sup> (Wicks), currently [assigned](#)<sup>10</sup> to the Senate Judicially Committee, addresses amendments to the CPRA, but I believe those amendments address *sale* of information, as opposed to the reciprocal concern I would like to address, the holding (and safety) of it.

---

<sup>5</sup><https://www.lausd.org/site/default.aspx?PageT...&pe=3&Domain/D=4&ModuleInstance/D=4466&ViewID=6446FEBB-D30C-497E-9316-3F8874B3E108&Renderloc=O&RexData/D=168886&PageID=1>

<sup>6</sup><https://www.the74million.org/article/turmoil-surrounds-las-new-ai-student-chatbot-as-tech-firm-turloughs-staff-just-3-months-after-launch/>

<sup>7</sup><https://web.archive.org/web/2024070306QZ4t/bttas:11www.allhere.com/>

<sup>8</sup><https://www.latimes.com/california/story/2024-07-03/lausds-highly-touted-ai-chatbot-to-help-students-fails-to-deliver>

<sup>9</sup>[https://leginfo.ca.gov/faces/billNavClient.xhtml?bill\\_id=20232024DAB194Q](https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=20232024DAB194Q)

<sup>10</sup>[https://leginfo.ca.gov/faces/billStatusClient.xhtml?bill\\_id=202320240AB1949](https://leginfo.ca.gov/faces/billStatusClient.xhtml?bill_id=202320240AB1949)

---

**From:** Monticollo, Allaire [REDACTED]  
**Sent:** Tuesday, August 20, 2024 7:22 AM  
**To:** Regulations@CPPA  
**Cc:** Christopher Oswald ; Travis Frazier  
**Subject:** Public Comment on Data Broker Registration Regulations  
**Attachments:** Joint Ad Trade Comments - Public Comment on Data Broker Registration Regulations (August 2024).pdf

---

**This Message Is From an Untrusted Sender**

**Warning:** This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Dear California Privacy Protection Agency:

Please find attached comments from the following advertising trade associations in response to the **July 5, 2024 Notice of Proposed Rulemaking to update California's data broker registration regulations:** the Association of National Advertisers, the American Association of Advertising Agencies, the American Advertising Federation, the Digital Advertising Alliance, and the Interactive Advertising Bureau. The advertising trade associations appreciate your consideration of these comments.

If you have any questions about these comments, please feel free to reach out to Chris Oswald at [REDACTED]

Kind Regards,  
Allaire Monticollo

\*\*\*\*\*  
This electronic mail transmission may contain confidential or privileged information. If you believe you have received this message in error, please notify the sender by reply transmission and delete the message without copying or disclosing it.  
\*\*\*\*\*

August 20, 2024

California Privacy Protection Agency  
Attn: Elizabeth Allen  
2101 Arena Boulevard  
Sacramento, CA 95834

**RE: Public Comment on Data Broker Registration Regulations**

Dear California Privacy Protection Agency:

On behalf of the advertising industry, we provide these comments in response to the California Privacy Protection Agency's ("CPPA") notice of proposed rulemaking to update the state's regulations governing data broker registration ("NPRM").<sup>1</sup> Below we comment on three discrete areas the CPPA should consider as it develops updated data broker registration rules: (1) the breadth of the proposed definition of "direct relationship" and the negative impacts that would result from adopting such a definition; (2) the proposed requirement for parent companies and subsidiaries to register as separate data brokers; and (3) unclear proposed requirements related to disclosing the "approximate proportion" of data processed subject to certain U.S. sectoral laws in comparison to total data processing activities and products "covered" by such laws. We submit these comments with the goal of preserving the meaning and intent of the underlying data broker registration statute, as enacted by the legislature, and reducing confusion and frustration for companies and consumers alike.

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country, including California. These companies range from small businesses to household brands, publishers, nonprofits, 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.<sup>2</sup> Our group has more than a decade's worth of hands-on experience it can bring to bear on matters related to consumer privacy and controls. We would welcome the opportunity to engage with the CPPA further on the points we discuss in these comments.

**I. The proposed definition of "direct relationship" would sweep virtually any entity doing business in California into the definition of "data broker" and would contravene the intent of the data broker registration law.**

California law defines a data broker as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship."<sup>3</sup> Through the NPRM, the CPPA has proposed to define "direct relationship" to mean

<sup>1</sup> See *Notice of Proposed Rulemaking*, CALIFORNIA PRIVACY PROTECTION AGENCY (July 5, 2024), available [here](#).

<sup>2</sup> John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 15 (Oct. 18, 2021), available [here](#).

<sup>3</sup> Cal. Civ. Code § 1798.99.80(d).

a consumer’s intentional interaction with a business “for the purpose of obtaining information about accessing, purchasing, using, or requesting the business’s products or services within the preceding three years.”<sup>4</sup> In addition, under the proposed rules, “[a] business is still a data broker if it has a direct relationship with a consumer *but also sells personal information about the consumer that the business did not collect directly from the consumer.*”<sup>5</sup>

PC1 The proposed definition of “direct relationship” is overly broad. Adopting it would make virtually *every business* in California a data broker, thus rendering the data broker registry meaningless, as the registry would amount to a list of all entities doing business in the state rather than the discrete list of data brokers intended by the legislature. The vast majority of businesses receive personal information about consumers from sources other than consumers themselves. These sources may include government sources, publicly available sources of information, and third-party information service providers in addition to myriad other sources. Information from these sources can be used for consumer-focused benefits, including address correction, email verification purposes, and even marketing hygiene to reduce the frequency and number of promotions consumers receive for various products or services, among others. In addition, many businesses engage in sales of personal information, as “sale” is defined broadly in the California Consumer Privacy Act (“CCPA”) to mean any transfer of personal information in exchange for monetary or other valuable consideration.<sup>6</sup> As a result, by defining “direct relationship” in a way that would require any business that sells personal information it did not collect directly from a consumer to register, the registration requirement would be transformed from a requirement for data brokers into a requirement for all businesses to register with the CPPA.

The proposed definition of “direct relationship” also contravenes the stated intent of California’s data broker registration law, as passed by the legislature. California’s original data broker registration bill stated the legislature’s intentions to preserve within law key differences between data brokers and other businesses with which consumers have a direct relationship.<sup>7</sup> When data broker registration requirements were first passed in California under AB 1202 in 2019, the legislature stated:

“There are important differences between data brokers and businesses with whom consumers have a direct relationship. Consumers who have a direct relationship with businesses... may have some level of knowledge about and control over the collection of data by those businesses, including: the choice to use the business’ products or services, the ability to review and consider data collection policies, the ability to opt out of certain data collection practices, the ability to identify and contact customer representatives, and the knowledge necessary to complain to law enforcement.”<sup>8</sup>

<sup>4</sup> Cal. Code Regs. tit. 11, § 7601(a) (proposed), *available* [here](#).

<sup>5</sup> *Id.* (emphasis added).

<sup>6</sup> Cal. Civ. Code § 1798.140(ad).

<sup>7</sup> See California AB 1202 (Reg. Sess. 2019), Sec. 1(g), *available* [here](#).

<sup>8</sup> *Id.*

As such, the bill required “data brokers,” as defined—and not all businesses in the state—to register with the California government. The CPPA’s proposed definition of “direct relationship” would turn the California legislature’s intent on its head by extending the term “data broker” to cover virtually every business in California. The CPPA should not use its regulatory authority to contravene clear provisions set forth in law. We ask the CPPA to decline to incorporate the proposed definition of “direct relationship” into California’s data broker registration regulations, as the definition extends beyond the scope and intent of the law.

**II. The proposed requirement for parent companies and subsidiaries to register as separate data brokers would confuse consumers and eliminate the treatment of affiliate relationships that is foundational to California privacy law.**

Under the proposed regulations, any business that independently meets the definition of a “data broker” must register with the CPPA, regardless of its status as a co-branded parent or subsidiary of another business.<sup>9</sup> This regulation would create significant consumer confusion. For many companies with diverse business models, parent companies and subsidiaries would need to separately register under the proposed rule, even if they are co-branded. This requirement would create undesirable results, as one company a consumer knows and recognizes may have several different registration entries depending on the number of affiliates it has. This proposed rule would also add a significant number of entities to the registration list, thereby diluting the meaning and utility of the list.

In addition, the proposed rule contrasts with the approach to businesses and parents/subsidiaries in the CCPA. The CCPA states that a “business” includes any for-profit entity that does business in California and meets certain data processing or revenue thresholds.<sup>10</sup> Any entity that controls or is controlled by a business and has common branding with the business may qualify as the same “business” for the purposes of the CCPA.<sup>11</sup> The proposed regulations would inject operational inefficiencies and would fail to reflect the realities of the marketplace. Under the proposed rule requiring parents and subsidiaries to register, “businesses” under the CCPA must be deconstructed as separate data brokers in the registration context. This would result in significant consumer confusion and unnecessary compliance burdens for businesses. The CPPA should not require parents and subsidiaries to register separately and should instead require any “business”—as defined by CCPA—that is also a “data broker” to register.

**III. The proposed requirements to disclose products and services covered by certain laws and the percentage of an entity’s data broker activities are unclear and will provide no consumer benefit.**

California law requires data brokers to disclose “whether and to what extent” they are regulated by the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, Insurance Information and Privacy Protection Act, the Confidentiality of Medical Information Act, or the privacy, security, and

<sup>9</sup> Cal. Code Regs. tit. 11, § 7602(a) (proposed).

<sup>10</sup> Cal. Civ. Code § 1798.140(d).

<sup>11</sup> *Id.*

breach notification rules established pursuant to the Health Insurance Portability and Accountability Act.<sup>12</sup> The draft regulations would also require entities to disclose “specific products or services covered by the enumerated state or federal law.”<sup>13</sup> Many of the listed laws apply to certain data types or certain entities rather than product offerings. As a result, a requirement to disclose products “covered by” each listed law could force data brokers to provide information to consumers that may be devoid of context necessary to explain the scope of coverage. A data broker’s list of products “covered” by applicable laws may change from time to time, requiring data brokers to constantly update their disclosures to the CPPA and causing significant confusion for consumers trying to make sense of the disclosures. The CPPA should reconsider this requirement, as it would mandate confusing disclosures to consumers without providing them with any clear benefits.

The proposed regulations would require data brokers to also disclose the “approximate proportion” of data collected and sold that is subject to those enumerated laws in comparison with their total data and collection and sales activities.<sup>14</sup> Requiring an “approximate proportion” of data collected and sold is vague and provides no clear standard by which data brokers are to understand what is required of them. If this proposed regulation is finalized, data brokers will have no common set of metrics to provide such disclosures to consumers; consumers will encounter a dynamic and fluid set of percentages that may change from time to time; and the CPPA will likely need to engage in further rulemaking to define a clear approach to disclosing such proportions. This would not be a desirable outcome for consumers, the CPPA, or businesses.

The Initial Statement of Reasons for the proposed rule states that this regulation is “necessary” because “consumers need to know how much of their data they can expect to be able to delete from the respective data broker” once the CPPA stands up an accessible deletion mechanism under the California Delete Act.<sup>15</sup> The CPPA should take steps to explain the scope of the deletion mechanism to consumers, including its relevant exemptions, rather than requiring data brokers to provide consumers with a non-standardized metric for information they can “expect” to be able to delete from a data broker. Consumers should be made aware of the fact that exemptions apply to requests made through the accessible deletion mechanism instead of being forced to interpret a percentage without context. The CPPA should remove the requirement to disclose an “approximate proportion” of data collected and sold from the proposed regulations.

\* \* \*

<sup>12</sup> *Id.* at § 1798.99.82(b)(2)(H).

<sup>13</sup> Cal. Code Regs. tit. 11, § 7603(d)(2) (proposed).

<sup>14</sup> *Id.* at § 7603(d)(3) (proposed).

<sup>15</sup> CPPA, Initial Statement of Reasons for Data Broker Registration Regulations at 13, located [here](#).



Thank you in advance for your consideration of these comments.

Sincerely,

Christopher Oswald  
EVP for Law, Ethics & Govt. Relations  
Association of National Advertisers  
[REDACTED]

Alison Pepper  
EVP, Government Relations & Sustainability  
American Association of Advertising Agencies, 4A's  
[REDACTED]

Lartease Tiffith  
Executive Vice President, 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  
Allaire Monticollo, Venable LLP

---

**From:** Julie Sweet [REDACTED]  
**Sent:** Tuesday, August 20, 2024 7:44 AM  
**To:** Regulations@CPPA  
**Subject:** AAPC Comment on Data Broker Registration Regulations  
**Attachments:** AAPC Letter on Draft California Data Broker Regulations.pdf

---

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Please find attached AAPC's Comment on Data Broker Registration Regulations. Please contact me at [REDACTED] for questions or for additional information.

Respectfully,

Julie C. Sweet  
Director, Advocacy & Industry Relations  
American Association of Political Consultants  
1750 Tysons Blvd. Ste 1500 | McLean, VA 22102

[www.theapc.org](http://www.theapc.org)



August 20, 2024

*Via Email ([regulations@cvpa.ca.gov](mailto:regulations@cvpa.ca.gov))*

California Privacy Protection Agency  
Attn: Elizabeth Allen  
2101 Arena Boulevard  
Sacramento, CA 95834

**Re: Public Comment on Data Broker Registration Regulations**

Dear Ms. Allen:

The American Association of Political Consultants (AAPC) welcomes the opportunity to submit comments on the California Privacy Protection Agency's proposed Data Broker Registration Regulations.

The AAPC is a bipartisan professional organization of political and public affairs professionals dedicated to advancing the field of political consulting and promoting ethical practices within the industry. The AAPC has over 1,800 members who rely on data to reach, educate, and engage voters in our democratic processes. We respect individuals' rights to control how their data is used and support well-defined privacy regulations and mechanisms to ensure that companies are following all state and federal laws.

The AAPC appreciates the Agency's diligent efforts in drafting the proposed regulations and accompanying draft initial statement of reasons. The AAPC respectfully offers two proposed revisions to the draft regulations.

**I. Definition of Direct Relationship**

First, the AAPC requests that the Agency revise the definition of "direct relationship" by deleting the final sentence of the proposed definition. The proposed definition is inconsistent with the legislative history of the law and, in combination with Attorney General Opinion No. 20-303, may inadvertently encompass processing activities that are not intended to be covered by the data broker law and the California Consumer Privacy Act (CCPA).

By way of background, the data broker law defines "data broker" as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship."<sup>1</sup> The law incorporates by reference the CCPA's definitions of "business," "third parties," "personal information," and "consumer." Although the law does not define "direct relationship," the original data broker law (AB 1202) contains legislative guidance indicating what the Legislature intended by that phrase. Specifically, Section 1 of AB 1202 states, in relevant part:

---

<sup>1</sup> Cal. Civ. Code § 1798.99.50(c).

There are important differences between data brokers and businesses with whom consumers have a direct relationship. Consumers who have a direct relationship with traditional and e-commerce businesses, which could have formed in a variety of ways such as by visiting a business' premises or internet website, or by affirmatively and intentionally interacting with a business' online advertisements, may have some level of knowledge about and control over the collection of data by those businesses, including: the choice to use the business' products or services, the ability to review and consider data collection policies, the ability to opt out of certain data collection practices, the ability to identify and contact customer representatives, and the knowledge necessary to complain to law enforcement.

By contrast, consumers are generally not aware that data brokers possess their personal information, how to exercise their right to opt out, and whether they can have their information deleted, as provided by California law.

Accordingly, the above legislative statements stand for the proposition that data brokers are entities that consumers have no interaction with and that consumers are not even aware have their personal information. In contrast, the Agency's proposed definition of direct relationship states that a "business is still a data broker if it has a direct relationship with a consumer but also sells personal information about the consumer that the business did not collect directly from the consumer." The draft initial statement of reasons further explains that the proposed definition "clarifies that a business can simultaneously have a direct relationship with a consumer related to the information it collects during an intentional interaction with that consumer and still be a data broker with respect to the personal information it independently collects from third parties and sells (i.e. personal information not acquired from a direct relationship."

The Agency's proposed "dual role" definition of direct relationship is not supported by the law's legislative history and, to the contrary, contradicts the Legislature's statements that data brokers are entities that consumers are "not aware" exist. Indeed, the harm the Legislature sought to solve is that consumers have no relationship with data brokers such that they do not even know that data brokers have their personal information and, therefore, are not in a position to exercise their privacy rights. That is a much different situation than instances in which a consumer does have a direct relationship, but a business collects personal information from other sources. Ultimately, because the final sentence of the proposed definition conflicts with the legislative intent, it should be stricken.

In addition, the final sentence of the definition could be interpreted to improperly require businesses to register as data brokers if they collect publicly available information that they then combine with personal information they collect directly from consumers. To explain, the CCPA's definition of "personal information" excludes "publicly available information or lawfully obtained, truthful information that is a matter of public concern."<sup>2</sup> The CCPA defines "publicly available" to include, among other things, "information that is made available from federal, state, or local government records."<sup>3</sup> The exclusion of publicly available information from the CCPA's

---

<sup>2</sup> Cal. Civ. Code § 1798.140(v)(2).

<sup>3</sup> *Id.*

definition of personal information is significant because it recognizes that there are First Amendment protections for publicly available information and, thereby, protects the CCPA from violating the First Amendment.

Nonetheless, in Attorney General Opinion No. 20-303, the Attorney General’s Office (interpreting the CCPA before CPRA amendments) blurred the lines between what is and is not publicly available information. Specifically, the Office reasoned that “[a] business might draw an inference about a consumer based in whole or in part on publicly available information, such as government identification numbers, vital records, or tax rolls. Under the CCPA, the inference must be disclosed to the consumer, even if the public information itself need not be disclosed in response to a request for personal information.”<sup>4</sup>

The conclusion that inferences based on publicly available information are subject to the CCPA is concerning and, at a minimum, raises First Amendment implications. In fact, the initial draft Colorado Privacy Act Rules took a similar approach, stating that the Colorado law’s definition of publicly available information does not include “[i]nferences made *exclusively* from multiple independent sources of publicly available information.”<sup>5</sup> The initial draft rules also sought to exclude from the definition “Publicly Available Information that has been combined with non-publicly available Personal Data.”<sup>6</sup> After commentors raised First Amendment concerns with these provisions,<sup>7</sup> the final rules removed them.

Ultimately, while the Agency’s current rulemaking does not include the CCPA’s publicly available information definition, the Agency’s rulemaking is not being done on a blank page and must be viewed in light of the prior Attorney General opinion. Therefore, the Agency should avoid creating potential First Amendment issues by deleting the last sentence of its “direct relationship” definition.

## II. Applicability of CCPA Regulation § 7301(b)

CCPA Regulation § 7301(b) provides: “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.”<sup>8</sup>

Given that the data broker regulations will be placed in a different chapter of the CCPA Regulations than § 7301(b), the AAPC respectfully requests that the Agency clarify that § 7301(b) also applies to any enforcement proceedings under the data broker law and regulations.

---

<sup>4</sup> Office of the Attorney General, Opinion No. 20-303 (Mar. 10, 2022) at 12.

<sup>5</sup> See Colorado Privacy Act Rules, Official Redline (emphasis added), *available at* <https://coag.gov/app/uploads/2023/03/FINAL-REDLINE-2023.03.09-Official-CPA-Rules.pdf>.

<sup>6</sup> *Id.*

<sup>7</sup> See, e.g., SIIA Comments at 2-4, *available at*

<https://coag.my.salesforce.com/sfc/p/#t00000004XX8/a/t0000001SORu/BQgSHixEtcxUkY2SkFaRx43Rz8AaQVoqMPj.mjTJrNI>.

<sup>8</sup> Cal. Code Regs., tit. 11, § 7301(b).

The protections afforded to businesses in § 7301(b) are crucial not only because the data broker regulations will be new but also because businesses are operating in a once-in-a-lifetime regulatory environment in which states are rapidly enacting new data privacy laws and regulations. Even the most well-funded and well-intentioned businesses will struggle with the avalanche of new state privacy laws. Clarifying that the protections in § 7301(b) apply to alleged violations of the data broker law and regulations will reward good actors who are making good-faith efforts to comply with these new laws and regulations.

The AAPC appreciates the opportunity to provide comments on the Agency's proposed Data Broker Registration Regulations and would be pleased to discuss these comments in greater detail. If you have any questions or would like to schedule a meeting, please feel free to contact us.

Respectfully submitted,



Alana Joyce  
Executive Director  
American Association of Political Consultants



[www.theaapc.org](http://www.theaapc.org)

---

**From:** Sara Geoghegan [REDACTED]  
**Sent:** Tuesday, August 20, 2024 8:26 AM  
**To:** Regulations@CPPA  
**Cc:** John Davisson  
**Subject:** EPIC submission to Public Comment on Data Broker Registration Regulations  
**Attachments:** EPIC - Data Broker Registry Comments 8.20.24.pdf

---

**This Message Is From an External Sender**

WARNING: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

---

[Report Suspicious](#)

---

Hello,

Please see attached the Electronic Privacy Information Center's (EPIC) comments regarding the Data Brokers Registration Regulations. Thank you.

Sara Geoghegan  
EPIC Counsel  
Electronic Privacy Information Center  
[REDACTED]

<https://www.epic.org/>

## COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

CALIFORNIA PRIVACY PROTECTION AGENCY

on

Proposed Rulemaking Regarding Data Broker Registration Regulations

August 20, 2024

---

The Electronic Privacy Information Center (EPIC) submits these comments<sup>1</sup> in response to the California Privacy Protection Agency (CPPA)'s invitation for public input concerning the Agency's development of regulations under Senate Bill 362, the Delete Act. We commend the Agency for ensuring more transparency into the opaque data broker industry and providing Californians with more information so that they can meaningfully exercise their rights under the California Consumer Privacy Act (CCPA).

EPIC is a public interest research center based in Washington, D.C., that 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.<sup>2</sup> EPIC has a long history of advocating for safeguards and rules to limit the harms caused by data brokers.<sup>3</sup> EPIC has

---

<sup>1</sup> EPIC Clerk Vaishali Nambiar contributed to these comments.

<sup>2</sup> EPIC, *About EPIC* (2022), <https://epic.org/about/>.

<sup>3</sup> EPIC, *FCRA Rulemaking: A Path to Reining in Data Brokers*, (2024) <https://epic.org/documents/fcra-rulemaking-a-path-to-reining-in-data-brokers/>; EPIC Comments to DOJ Regarding ANPRM on Access to Americans' Bulk Sensitive Personal Data and Government Related Data by Countries of Concern (Apr. 19, 2022), <https://epic.org/documents/epic-comments-to-doj-regarding-anprm-on-access-to-americans-bulk-sensitive-personal-data-and-government-related-data-by-countries-of-concern/>; EPIC, *Data Broker Threats: National Security* (2024), <https://epic.org/wp-content/uploads/2024/05/Data-Broker-One-Page-National-Security-2.pdf>; EPIC, *CFPB Fair Credit Reporting Act Rulemaking* (2024), <https://epic.org/cfpb-fair-credit-reporting-act-rulemaking>.



previously provided comments on the CCPA,<sup>4</sup> published a detailed analysis of the California Privacy Rights Act before its approval by California voters,<sup>5</sup> and regularly presents oral testimony to the Agency to encourage the strongest protections for Californians.

EPIC supports the Agency's efforts to rein in the largely opaque data broker industry. Although safeguarding the privacy of consumers requires far more than granting individual rights, providing Californians with transparency and choice is an important step in the right direction. EPIC supports the proposed regulations,<sup>6</sup> which will strengthen the data broker registry and ensure more meaningful compliance. The proposed regulations provide that the \$400 registration fee plus processing fees can be paid via a standardized electronic payment method including debit card, check, or wire transfer if the business cannot pay by credit card. The proposed regulations also provide more clarity on the requirements for registration completion; explain that each data broker business is required to uniquely register regardless of its status as a parent company or subsidiary to another business; and require that businesses must provide

---

<sup>4</sup> Comments of Consumer Reports, Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC) and Privacy Rights Clearinghouse (PRC) In Response to the California Privacy Protection Agency's Invitation for Preliminary Comments On Proposed Rulemaking Under Senate Bill 362 (June 25, 2024), <https://advocacy.consumenepoints.org/wp-content/uploads/2024/06/Comments-of-Consumer-Reports-In-Response-to-the-California-Privacy-Protection-Agency's-Invitation-for-Preliminary-Comments-On-Proposed-Rulemaking-Under-Senate-Bill-362.pdf>; Comments Of The Electronic Privacy Information Center, Center For Digital Democracy, and Consumer Federation Of America, to the California Privacy Protection Agency (Mar. 27, 2023), <https://epic.org/documents/comments-of-the-electronic-privacy-information-center-center-for-digital-democracy-and-consumer-federation-of-america-to-the-california-privacy-protection-agency/>; Comments of EPIC to Cal. Privacy Prot. Agency (Nov. 20, 2022), <https://epic.org/wp-content/uploads/2022/11/EPIC-CPPA-Comments-Nov-20.pdf>; Comments of EPIC et al. to Cal. Privacy Prot. Agency (Aug. 23, 2022), <https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf>; Comments of EPIC et al to Cal Privacy Prot. Agency (Nov. 8, 2021), <https://epic.org/wp-content/uploads/2021/11/PRO-01-21-Comments-EPIC-CA-CFA-OTI.pdf>; 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>.

<sup>5</sup> EPIC, *California's Proposition 24* (2020), <https://epic.org/californias-proposition-24/>.

<sup>6</sup> Data Broker Registration Proposed Text (Express Terms), CPPA (July 5, 2024) [https://cppa.ca.gov/regulations/pdf/data\\_broker\\_reg\\_prop\\_text.pdf](https://cppa.ca.gov/regulations/pdf/data_broker_reg_prop_text.pdf).

accurate and functional website links and email addresses to the Agency. These regulations will improve the efficacy of the data broker registry by promoting clarity, accuracy, and completeness.

We support the proposed regulations' broad definition of "reproductive health care data." Under the proposed rules, data brokers will be required to disclose whether they collect consumers' reproductive health care data, which will now be defined to include a wide array of reproductive and sexual information and inferences derived therefrom. The definition covers any information about a consumer searching for, accessing, procuring, using, or interacting with goods or services associated with the human reproductive system. Examples of goods include contraception, pre-natal and fertility supplements, menstrual-tracking apps, hormone-replacement therapy. Examples of services include sperm- and egg-freezing, in vitro fertilization, abortion care, vasectomies, sexual health counseling, treatment or counseling for STIs, erectile dysfunction, and reproductive tract infections; and precise geolocation information about such treatments. The definition also captures information about the consumer's sexual history, health, and family planning (including information that the consumer puts on a dating app), and it specifically covers inferences derived from both reproductive and sexual information. EPIC supports this broad definition to fully protect the reproductive privacy of California consumers. As EPIC has previously explained, much of this information falls outside of the scope of HIPAA and is not adequately protected. When data brokers can collect and use this information to profile consumers, it can reveal pregnancy status and pregnancy outcomes, violating consumers' privacy

and exposing them to serious harm.<sup>7</sup> The Agency's broad definition will help protect the reproductive privacy of California consumers from the invasive practices of data brokers.

While the proposed regulations will shed new light into the opaque data broker industry, the Agency should also require data brokers to provide an individual point of contact to be made publicly available on the registry—not just a URL and faceless email address. This change would increase data broker accountability and further the Agency's goal of providing consumers with more information to help them exercise their privacy rights. Public contact information could be valuable to a consumer who seeks to get in touch with a data broker to clarify and exercise their rights under California law. This measure has been successfully implemented in other regulatory settings. For example, the Federal Communications Commission requires all voice service providers to furnish a designated contact person (name, department, contact number) for its Robocall Mitigation Database, and all of this information is publicly available.

EPIC supports the Agency's efforts to enhance its data broker registry and rein in the privacy harms caused by the industry. EPIC supports the proposed regulatory clarifications and definitions and urges the Agency to require that data brokers supply an individual point of contact to be published on the registry.<sup>8</sup> We thank the Agency for the opportunity to comment on its proposed regulations and are eager to continue working with the CPPA to protect the privacy of all Californians.

---

<sup>7</sup> Sara Geoghegan and Dana Khabbaz, *Reproductive Privacy in the Age of Surveillance Capitalism*, EPIC (July 7, 2022) <https://epic.org/reproductive-privacy-in-the-age-of-surveillance-capitalism/>.

<sup>8</sup> *Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, FCC 20-136, at 46, para. 84-85 (Sept. 29, 2020), <https://docs.fcc.gov/public/attachments/FCC-20-136A1.pdf>.

Respectfully submitted,

*Isl John Davisson*

Director of Litigation and EPIC Senior Counsel

*Isl Sara Geoghegan*

EPIC Counsel

ELECTRONIC PRIVACY  
INFORMATION CENTER (EPIC)  
1519 New Hampshire Ave. NW  
Washington, DC 20036



---

**From:** Dani Kanda-Kaiser [REDACTED]  
**Sent:** Tuesday, August 20, 2024 11:02 AM  
**To:** Regulations@CPPA  
**Cc:** [REDACTED] Meghan Land  
**Subject:** Public Comment on Data Broker Registration Regulations: Support  
**Attachments:** 2024-08-19 - Comments to CPPA on Delete Act Implementing Regulations\_PRC.pdf

---

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Hello Ms. Allen,

Please see the attached letter from the sponsors of SB362 (Becker), the Privacy Rights Clearinghouse. Thank you for the opportunity to provide public comment. If you have any questions, please reach out to Emory Roane or myself.

Best,

**Dani Kando-Kaiser**

(she/heɪ·/heɪ·s)

---

1121 LStreet, Suite 602  
[Sacramento, CA](#) 95814



August 19, 2024

California Privacy Protection Agency  
Attn: Elizabeth Allen  
2101 Arena Blvd.  
Sacramento, CA 95834

**Re: Public Comment on Data Broker Registration Regulations: Support**

Dear Ms. Allen and Members of the California Privacy Protection Agency:

We are Privacy Rights Clearinghouse, a nonprofit organization dedicated to improving privacy for all through advocacy and education, writing to express our strong support for the proposed regulations implementing the Delete Act (SB 362). As co-sponsors of this legislation, we commend the Agency for drafting regulations that effectuate the Delete Act's purpose and enhance Californians' privacy rights.

*"Direct Relationship"*

We strongly support the proposed definition of "direct relationship" in Section 7601(a). This definition is essential as it determines which businesses must comply with the Delete Act's data broker obligations. Specifically:

1. The three-year limitation on the length "direct relationship" (§ 7601(a)) without subsequent intentional interaction acknowledges that consumers may be unaware of ongoing data collection and sales by businesses they interacted with in the distant past. This provision ensures that businesses cannot claim an indefinite exemption based on long-past interactions. This is particularly important given that data brokers often retain information for extended periods. The Federal Trade Commission's 2014 report "Data Brokers: A Call for Transparency and

Accountability" found that "Some of the data brokers store all data indefinitely, even if it is later updated, unless otherwise prohibited by contract."<sup>1</sup>

2. The requirement for intentional interaction (§ 7601(a)) prevents businesses from claiming a "direct relationship" based on incidental or unwitting consumer engagements. In today's digital ecosystem, consumers may unknowingly interact with numerous entities through a single website visit or app use. For instance, simply visiting a website could potentially expose a consumer's data to multiple third-party trackers, analytics providers, and advertising networks. The Delete Act must not permit data brokers to claim a "direct relationship" based on these passive, often invisible interactions. This provision ensures that only when a consumer knowingly and purposefully engages with a business can that business claim a direct relationship, thereby preventing data brokers from exploiting casual or inadvertent online activities to avoid the Act's obligations.
3. The clarification that a business is still considered a data broker if it sells personal information that it did not collect directly from the consumer, even if it also has a direct relationship (§ 7601(a)), is crucial. This prevents businesses from exploiting the "direct relationship" exemption while engaging in typical data broker activities. Consider Equifax: registered with the CPPA as a data broker selling reproductive healthcare data, minors' data, and geolocation information, while simultaneously offering identity theft protection services and ironically, currently providing free credit monitoring to countless affected consumers due to its own 2017 security breach of 147 million Americans' data. Without this provision, Equifax could potentially claim exemption from data broker regulations based on its credit monitoring relationships, while continuing to sell sensitive data through other business lines. This clarification ensures that even large, multifaceted organizations cannot use one arm of their business to shield their data broker activities.

### *"Reproductive health care data"*

We particularly appreciate the Agency's focus on reproductive healthcare and privacy and the comprehensive definition of "reproductive health care data" in Section 7601(e). This definition, which includes information consumers input into dating apps about their sexual history and family planning and, crucially, inferences about consumers' reproductive healthcare data, reflects the Delete Act's strong emphasis on protecting sensitive

---

<sup>1</sup> Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability" (2014), p. vi, available at <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

reproductive health information and the concerns of the broad coalition that supported SB 362, which included organizations dedicated to reproductive healthcare and privacy. This definition will help ensure that data brokers are transparent about their collection and sale of this highly sensitive information, enabling consumers to make informed and safe decisions about their privacy.

### *Registration, Transparency and Accessibility Requirements*

The clear registration requirements outlined in Section 7602 will ensure the Agency has accurate, current information on data brokers operating in California. We support the requirement that each data broker business, regardless of its status as a subsidiary or parent company, must register independently (§ 7602(a)). This prevents potential evasion of the Act's requirements through corporate structuring.

The detailed information requirements in Section 7603 will provide consumers with valuable insights into data brokers' practices. We particularly support the requirement for data brokers to disclose the types of personal information, products and services, and the proportion of data collected and sold that are subject to other laws (§ 7603(d)). In concert with the detailed CCPA reporting obligations now required by the Delete Act, this level of granularity will significantly enhance transparency in the data broker industry.

We support the requirement in Section 7605 for website disclosures to comply with existing accessibility standards. This ensures that all Californians, regardless of ability, can access critical information about data broker practices, aligning with the Delete Act's goal of empowering all consumers to exercise their privacy rights effectively.

We do, however, recommend that the Agency additionally require these disclosures to be machine-readable as well when possible. Especially for metrics and reports containing complex data, machine-readable formats would allow for automated analysis, enabling tools that could help consumers understand the contextual relevance and implications of the disclosures. This would significantly enhance transparency and the accessibility of these disclosures, as it's often difficult for individuals to fully grasp the scope and meaning of human-readable disclosures alone, particularly when dealing with large volumes of data or technical information.

These regulations provide a solid framework for implementing the Delete Act, offering much-needed clarity on key definitions and establishing important disclosure requirements. We appreciate the opportunity to share our comments and thank the



California Privacy Protection Agency for its careful consideration and dedication to strengthening privacy protections for Californians.

Sincerely,



Emory Roane

Associate Director of Policy  
Privacy Rights Clearinghouse

**From:** Darren Chaker [REDACTED]  
**Sent:** Tuesday, August 20, 2024 11:20 AM  
**To:** Regulations@CPPA  
**Subject:** SB 362 - Time Sensitive

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

I am Danen Chaker, and as a protected person under Gov. Code 6205 et seq. (Safe at Home) I ask that my recommendations are embraced and considered in reference to Senate Bill No. 362 (Delete Act).

In viewing various aspects of the cmTent reading of the California Consumer Privacy Act of 2018 (CCPA), I would recommend amendments to include:

**Private Cause of Action:** Cunenlty, the statute does not allow for a private cause of action. A consumer must rely upon the California Attorney General. While reviewing the enforcement actions, only a handful of cases exist.ill However, for the colllllllon person, he or she has no option to pmsue claims. For example, numerous data brokers exist who have not registered as a data broker, do not have a California corporation, but freely sell personal infonnation without any oversight. See CheckPeople.com and InfoImentation.com. If one of these websites do not comply with the law, there is, literally, no statute which allows to file a lawsuit to protect his or her rights.

This is significant not only for a member ofthegeneral public but also for people the California Legislatme have found at high risk of haim. In paiticular members of Safe at Home, and judicial officers, police, and other public officialsill who shai·e such risk in colllllllon, and the options to suppress and bring a private cause of action via injunctive means and/or seeking damages:

**SAH Participant (Cal. Gov't Code§ 6208.1)**

**Cal. Gov't Code§ 6208.1(a)(1)**

"No person, business, association, or other entity shall knowingly and intentionally publicly post or publicly display on the internet or any other public space the home address, home telephone number, or image..."

**Cal. Gov't Code§ 6208.1(b)(1)**

"describing a reasonable fear for the safety of that individual or of any person residing at the individual's home address"

**Cal. Gov't Code§ 6208.1(b)(2)**

**Public Officials (Cal. Gov. Code § 7928.215)**

**Gov. Code§ 7928.215(a)**

"No person, business, association, or other entity shall knowingly and intentionally publicly post or publicly display on the internet or any other public space the home address, home telephone number, or image..."

**Cal. Gov't Code§ 7928.215**

"shall include a statement describing a threat to the safety of that individual or of any person residing at the official's home address."

**Gov. Code§ 7928.230(c)**

**SAH Participant (Cal. Gov't Code § 6208.1)**

“shall award damages to that individual in an amount up to a maximum of three times the actual damages, but in no case less than four thousand dollars (\$4,000).”

**Cal. Gov. Code § 6208.2(2)**

“A violation of this subdivision is a misdemeanor”

**Public Officials (Cal. Gov. Code § 7928.215)**

“shall award damages to that official in an amount up to a maximum of three times the actual damages but in no case less than four thousand dollars (\$4,000)”

**Cal. Gov. Code § 7928.210(b)**

“A violation of this section is a misdemeanor.”

I believe borrowing from the above statutes to allow a consumer to file a lawsuit could only result in websites fearing a lawsuit to comply with registration duties and compliance with the law. At this juncture, seeing only a handful of lawsuits by the state is a clear indicator the odds are in favor of those who violate the law will not be sued.

**Sanctions:** In addition, for those who are at high risk of harm as found in categories of people identified in as “victim” or “witness”, under state or federal law, those defined under 6205 et seq. and 7928.215, in the event a data broker does not comply with the law, it places these people at far higher risk of harm. The Legislative intent to protect Safe at Home participant’s information was clear, “Because program participants are endangered when their personal identifying information is publicized, they should be able to protect their personal identifying information.” [California Bill Analysis, S.B. 636 Sen., 4/14/2011]

It is no secret the Internet has been used to seek out, locate, and punish those, such as myself, who have cooperated with both state and federal matters.<sup>[3]</sup> Thus, for data brokers who ignore requests from high risk groups, then additional risk to the revenue to these companies should be available to the state, as well to individuals in those categories.

The dangers of the data brokers may be in *In re Fees in Connection with Unauthorized Arrangements with Xclaim, Inc.*, 647 B.R. 269, 287 (Bankr. S.D.N.Y. 2022), where the court stated in part, “Tragically, using the internet to compile an individual's PII was precisely the method used by the deranged and disgruntled attorney to locate and murder New Jersey District Judge Esther Salas’ son and seriously injure her husband in July 2020.” District Court Judge Santos’ horrific experience resulted in writing in the New York Times, in which the court recited in part,

“The free flow of information from the Internet allowed this sick and depraved human being to find all our personal information and target us .... Currently, federal judges’ addresses and other information is readily available on the Internet. In addition, there are companies that will sell your personal details that can be leveraged for nefarious purposes.”

It should be noted, as with California that protects witnesses and judges with virtually identical language, Congress did not see the risk reduced when it passed federal statutes criminalizing posting information for these people. Particularly, 18 U.S.C. § 119(a)(1) is criminalizes posting “Restricted Personal Information” about a specific high-risk group of people defined as a “**covered person**.” [§ 119 also covers “immediate family” to the “covered person.” ((b)(2)(4).] Thus, the coexistence of the statutes is laser focused to protect specific class of people who have a history of being targeted for harm. The statute illustrates the significant potential harm of not only judges, but so too witnesses by protecting them under the same statute as judges, federal agents, and are mentioned twice in its definition.

**Enforcement:** Since websites do not exist absent a hosting service, I believe the inclusion of language which would require a company who hosts an unregistered data broker site shall be required to cease hosting the site within 72 hours, unless the data broker provide proof it is registered to sell or otherwise distribute the personal information. Further, I believe extending the language to search engines to deindex the site and related URLs would be useful in the event the site is hosts its own content. Therefore, the unregistered data broker would be removed from search results. Allowing an individual to make such requests to the hosting company or search engine is key since, as with enforcement actions, the chances of a lone consumer getting the attention of the state to enforce the law is low.

Permission to publish this comment and to use my name, but **not** disclose my email, is granted.

---

<sup>[1]</sup> <https://oag.ca.gov/privacy/privacy-enforcement-actions>

<sup>[2]</sup> The statute was recently renumbered from Government Code Section 6254.21 to Gov. Code § 7928.215.

<sup>[3]</sup> See *United States v. Petrovic*, 701 F.3d 849, 852 (8th Cir. 2012) ("Petrovic used online search tools to locate [the victim's] address and initiated a campaign of harassment and threats across state lines."); *United States v. Sayer*, 748 F.3d 425, 430 (1st Cir. 2014) ("Sayer utilized various online people search engines to find [the victim's] personal information, which he then used to cyberstalk her."); *United States v. Cassidy*, 814 F. Supp. 2d 574, 577 (D. Md. 2011) ("Cassidy accessed social media platforms and people search websites to gather information about [the victim], leading to persistent harassment."); *United States v. Herring*, 955 F.2d 703, 705 (11th Cir. 1992) ("Herring used an online directory to find the victim's residence, which facilitated his subsequent criminal activities against her."); *United States v. Howard*, 245 F. Supp. 2d 24, 27 (D.D.C. 2003) ("Howard employed internet search engines to track down [the victim's] address, culminating in repeated acts of intimidation and threats."); *United States v. Bowen*, 437 F.3d 1009, 1013 (10th Cir. 2006) ("Bowen utilized online people search tools to locate the victim's workplace, leading to charges of stalking and harassment."); *United States v. Wilson-Bey*, 2:21-cr-00306-GMN-NJK, (D. Nev. Apr. 25, 2022) ("Defendant intimidated her victims by demonstrating knowledge of their private and personal information, such as the location of their residences, contact information, and the identities of their friends and families."); *United States v. Dodson*, No. 22-3998, 23-24 (6th Cir. Feb. 21, 2024) ("In imposing the internet restriction, the district court reasoned, "the internet restriction is because this is how - you got on the internet and threatened Ms. McNamara, so you can't get on and use the internet without prior written approval of your supervising officer" Sent'g Hr'g Tr., R. 48, Page ID #260. ")

---

**Confidentiality Notice:** This message, along with any attachments and/or replies thereto, are covered by the Electronic Communications Privacy Act, 18 U.S.C. Sections 2510-2521, and may be legally privileged. The information contained in this electronic e-mail and any accompanying attachment(s) is intended only for the use of the intended recipient and may be confidential and/or privileged. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, copying, or retransmission of this message is in violation of 18 U.S.C. 2511(1) of the ECPA and is strictly prohibited. If you have received this communication in error, please immediately notify the sender by return e-mail, and delete the original message and all copies from your system.

---

**From:** Bailey Sanchez [REDACTED]  
**Sent:** Tuesday, August 20, 2024 11:37 AM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on Data Broker Registration Regulations"  
**Attachments:** CPPA Rulemaking Comments (DELETE Act).pdf

---

**This Message Is From an External Sender**

WARNING: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Hi Elizabeth,

Future of Privacy Forum's public comment on the data broker registration regulations is attached.

Best,  
Bailey



**Bailey Sanchez (she/her)**  
Senior Counsel, US Legislation  
Future of Privacy Forum  
[REDACTED] [www.fpf.org](http://www.fpf.org) 11350  
Eye Street NW, Suite 350,  
Washington, DC 20005



August 20, 2024

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

**RE: Public Comment on Data Broker Registration Regulations**

Dear Elizabeth Allen and Members of the California Privacy Protection Agency,

Thank you for your ongoing work and the opportunity to comment regarding the implementation of Senate Bill 362 (“the Delete Act” or “the Act”). The Future of Privacy Forum (“FPF”) is a non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies in the United States and globally. FPF seeks to support balanced, informed public policy and equip regulators with the resources and tools needed to craft effective regulation.<sup>1</sup> In response to the Agency’s public comment on data broker registration regulations, FPF recommends clarifying the definition of “direct relationship” to better align with user expectations on the forthcoming accessible deletion mechanism. Specifically, FPF encourages the Agency to consider:

- How the proposed definition may lead to unintentional data deletion requests, and
- Whether tying a “direct relationship” to recent user interactions may lead to the accessible deletion mechanism not operating as intended.

**Clarify the definition of “direct relationship”**

**A. The proposed definition may lead to unintentional data deletion requests.**

As currently drafted, the regulations define a covered data broker to include a business that sells personal information about a user that the business did not directly collect from the user, including instances where a business has a direct relationship with a user.<sup>2</sup> This proposed standard for when businesses qualify as covered data brokers may be an expansion from the plain text of the Delete Act, which is focused exclusively on businesses that lack a direct relationship with individuals.<sup>3</sup> Should the Agency proceed in expanding the scope of organizations subject to the Delete Act, it is crucial to consider potential consequences for

---

<sup>1</sup> The opinions expressed herein do not necessarily reflect the views of FPF’s supporters or Advisory Board.

<sup>2</sup> Data Broker Registration – Notice File Number Z2024-0625-02, § 7601, Cal. Priv. Prot. Agency (July 5, 2024), [https://coppa.ca.gov/regulations/pdf/data\\_broker\\_reg\\_prop\\_text.pdf](https://coppa.ca.gov/regulations/pdf/data_broker_reg_prop_text.pdf)

<sup>3</sup> Cal. Civ. Code, § 1798.99.87.

individual expectations and the exercise of consumer rights through the accessible deletion mechanism, or the Delete Requests and Opt-Out Platform (DROP) provided for under the Delete Act.<sup>4</sup>

The Delete Act calls for the development of an accessible deletion mechanism that requires covered data brokers to, upon request, delete **any** personal information about an individual, not just information collected from third-party sources.<sup>5</sup> Given that the accessible deletion mechanism intends to serve as a ‘one-stop shop’ to enable individuals to issue bulk deletion requests, it is important to ensure that both the organizations and personal data subject to such requests are aligned with individual expectations and are not over- or under-inclusive. If the impact of a bulk deletion request covers less data than users expect, individuals may have a false sense of their online privacy. If the request implicates more information than expected, individuals may lose personal data or access to desired products and services. The scope of entities required to register for the data broker list is therefore critical to the success of the Delete Act and the DROP.

An individual who issues a bulk request through the DROP that is transmitted to organizations with whom they have a direct relationship could result in the deletion of not just third-party data collected about users, such as clickstream data used for targeting ads, but also first-party data affirmatively provided to the business, potentially including entire accounts and their storage contents. As a result, individuals could inadvertently delete their social media profiles, email accounts, or online photo and file storage. While the Delete Act contains an exception for a data broker to deny a deletion request if maintaining the personal information is “reasonably necessary” to fulfill a purpose described in subsection (d) of Section 1798.105 of the California Consumer Privacy Act, this exclusion may not encompass all of an entity’s first-party data and businesses may find it easier to comply broadly with a request to delete data than rely on an exception.<sup>6</sup>

FPF notes that the Agency’s Initial Statement of Reasons provides an illustrative example of a scenario where a business that offers a widely used service may also buy and sell data about a user unrelated to information directly collected by the user.<sup>7</sup> FPF finds this to be a helpful explanation of the Agency’s reasoning for this proposed definition and demonstrates that a

---

<sup>4</sup> Cal. Civ. Code, § 1798.99.86.

<sup>5</sup> Cal. Civ. Code, § 1798.99.86(a)(2).

<sup>6</sup> Cal. Civ. Code, § 1798.99.86(c)(2)(A).

<sup>7</sup> “For example, a business that offers a widely used service, such as a video game that can be used on a mobile phone, may also buy and sell data about a consumer completely unrelated to the game purchase or use, such as information about their menstrual cycle. Thus, the business would not be considered a data broker with respect to the personal information collected directly from the consumer for the video game but would be considered a data broker for purposes of the personal information about the consumer’s menstrual cycle that it independently bought and sold to third parties.” California Privacy Protection Agency, *Initial Statement of Reasons*, p. 7

[https://www.cppa.ca.gov/regulations/pdf/data\\_broker\\_reg\\_isor.pdf](https://www.cppa.ca.gov/regulations/pdf/data_broker_reg_isor.pdf)

business may function as a data broker only with respect to certain sources of data or certain customers. We recommend that the proposed definition of “direct relationship” could be strengthened and further aligned with the Initial Statement of Reasons by explicitly stating that deletion requests apply specifically to brokered data and not any personal data associated with an individual. The Agency could clarify either in these regulations or in a future process, but it should be an essential consideration as the Agency develops the DROP.

#### **B. Considerations in tying a "direct relationship" to recent user interactions**

The draft regulations propose that there must be an interaction between a user and a business within the preceding three years for a “direct relationship” to exist. The Agency explains this is intended to prevent businesses from claiming an indefinite direct relationship and avoiding registration requirements.<sup>8</sup> FPF is agnostic as to whether three years is the appropriate timeframe but encourages the Agency to consider how creating a definition dependent on user interactions with a business will interact with exercising individual rights through the DROP.

The intended purpose of the DROP is to be a one-stop mechanism for individuals to quickly delete data from businesses with whom they do not have a direct relationship. A requirement that a user must have interacted with a business in the preceding three years could lead to many infrequently used websites and services being on the list that a user might not expect to encounter. Broadening the types of businesses considered data brokers would result in a user needing to more closely inspect the list of companies they would be requesting to delete their data from or risk losing desired data, thus diminishing the value of this one-stop mechanism.

Additionally, it is unclear how the proposed three-year requirement for holding a “direct relationship” would impact other customers of a business. Whether a user has interacted with a business within the preceding three years is unique *to each individual*. Would a business need to register for the data broker list and respond to DROP requests for its entire customer base if more than three years have lapsed for merely one user? If so, businesses could be required to respond to DROP requests from individuals they routinely interact with. The proposed definition may incentivize businesses to prematurely delete their customers' data solely to avoid needing to register as a data broker rather than when it is most prudent to delete it in line with data retention best practices. In the alternative, the regulations could specify that a business may only be a data broker with respect to the data of individuals with whom they have not interacted in the previous three years. Still, the appearance of such organizations on the data broker registry could also confuse individuals using the DROP.

One approach to the issue of indefinite relationships is the concept of “refreshing consent” developed through the Colorado Privacy Act’s implementing regulations.<sup>9</sup> Under the regulations,

---

<sup>8</sup> California Privacy Protection Agency, *Initial Statement of Reasons*, p. 7 [https://www.cppa.ca.gov/regulations/pdf/data\\_broker\\_reg\\_isor.pdf](https://www.cppa.ca.gov/regulations/pdf/data_broker_reg_isor.pdf).

<sup>9</sup> 4 CCR 904-3, Rule 7.08 “Refreshing Consent.”



a controller must refresh consent after 24 months of inactivity to continue processing sensitive data or personal data for a secondary use. While Colorado’s refreshing consent concept applies in a different context than the Delete Act’s “direct relationship” definition, FPF encourages the Agency to continue exploring how mitigating its concern with “indefinite direct relationships” can better align with user expectations and the goals of the DROP.

\* \* \*

Thank you for this opportunity to provide comment on these proposed regulations. We welcome any further opportunities to provide resources or information to assist in this important effort. If you have any questions regarding these comments and recommendations, please contact Bailey Sanchez at [REDACTED]

Sincerely,

Bailey Sanchez  
Senior Counsel, U.S. Legislation

---

**From:** Tany Ficarrotta [REDACTED]  
**Sent:** Tuesday, August 20, 2024 12:28 PM  
**To:** Regulations@CPPA  
**Cc:** David LeDuc; Leigh Freund; Allen, Elizabeth@CPPA  
**Subject:** Public Comment on Data Broker Registration Regulations -- NAI Comments  
**Attachments:** NAI Delete Act NPRM Comments (8.20.2024).docx.pdf

---

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

To the California Privacy Protection Agency,

The NAI is submitting comments in response to the Agency's Notice of Proposed Rulemaking of July 5, 2025 concerning data broker registration requirements. Please see the attached pdf for our comments. If you have any questions or would like to discuss further, please do not hesitate to reach out.

Thank you,  
-Tony Ficarrotta

Tony Ficarrotta  
Vice President, General Counsel  
[The NAI](#)  
409 7th Street, NW, Suite 250, Washington, DC 20004





409 7th Street, NW Suite 250  
Washington, DC 20004

Submitted via electronic mail to: [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

August 20, 2024

California Privacy Protection Agency  
Attn: Elizabeth Allen  
2101 Arena Blvd  
Sacramento, CA 95834

**Re: NAI Comments on Proposed Data Broker Registration Regulations**

To the California Privacy Protection Agency:

On behalf of the Network Advertising Initiative (the “NAI”), thank you for the opportunity to provide comments in response to the notice of proposed rulemaking on data broker registration (the “NPRM”)<sup>1</sup> issued by the California Privacy Protection Agency (the “Agency”) under SB 362 (the “Delete Act”).<sup>2</sup>

Founded in 2000, the NAI is the leading non-profit, self-regulatory association for advertising-technology companies. For over 20 years, the NAI has promoted strong consumer privacy protections, a free and open internet, and a robust digital advertising industry by maintaining the highest industry standards for the responsible collection and use of consumer data for advertising. Our member companies range from large multinational corporations to smaller startups and represent a significant portion of the digital advertising technology ecosystem, all committed to strong self-regulation and enhancing consumer trust.

Our comments below are organized into two sections.

---

<sup>1</sup> 27-Z Cal. Regulatory Notice Reg. 844 (July 5, 2024), [https://coppa.ca.gov/regulations/pdf/data\\_broker\\_reg\\_nopa.pdf](https://coppa.ca.gov/regulations/pdf/data_broker_reg_nopa.pdf).

<sup>2</sup> See CAL. CIV. CODE §§ 1798.99.80 *et seq.*

In Section I, we focus on the Agency’s proposed definition of reproductive health care data (“RHCD”) and recommend that the Agency specify that RHCD is sensitive personal information under the California Consumer Privacy Act (“CCPA”).<sup>3</sup> Doing so will promote clarity and consistency both for consumers seeking to exercise their CCPA rights with businesses that collect RHCD as shown on California’s data broker registry page (the “Registry”),<sup>4</sup> and for businesses seeking to provide the information required by the Delete Act.

In Section II we address the fact that in some cases businesses process RHCD and/or precise geolocation solely for short-term, transient uses such as de-identifying, aggregating, deleting, or rendering it non-sensitive. Based on this fact, we recommend that the Agency distinguish this type of data minimization from other types of processing undertaken for commercial purposes and use the distinction to clarify which businesses must report that they collect RHCD and/or precise geolocation. Doing so will help consumers identify which businesses on the Registry use these categories of information for commercial purposes and facilitate their exercise of CCPA rights; and will incentivize businesses to minimize their processing of those categories of data.

I. Comments regarding the proposed definition of reproductive health care data

- A. *The Agency should update the proposed definition of “reproductive health care data” to better align with the CCPA by specifying that it is “sensitive personal information” under the CCPA.*

As discussed in more detail below, the definition of RHCD proposed by the Agency does not specify that RHCD is “sensitive personal information” under the CCPA.<sup>5</sup> The Agency should amend the proposed definition of RHCD to make this specification because doing so will promote clarity and consistency both for consumers seeking to exercise their CCPA rights with businesses shown to collect RHCD on the Registry, and for businesses seeking to report the information required by the Delete Act.

The Delete Act uses the term RHCD to specify a type of data businesses must report when registering with the Agency, but does not define the term.<sup>6</sup> One of the goals set by the Agency in the Initial Statement of Reasons (ISOR) accompanying the NPRM is to define certain terms

---

<sup>3</sup> CAL. CIV. CODE §§ 1798.100 *et seq.*

<sup>4</sup> See *Data Broker Registry*, CAL. PRIV. PROT. AGENCY, [https://cppa.ca.gov/data\\_broker\\_registry/](https://cppa.ca.gov/data_broker_registry/) (last visited Aug. 15, 2024).

<sup>5</sup> See CAL. CIV. CODE § 1798.140(ae) (defining sensitive personal information).

<sup>6</sup> See *id.* § 1798.99.82(b)(2)(E).

used in the Delete Act that are not otherwise defined by the CCPA, including RHCD.<sup>7</sup> To meet that goal, the Agency proposed the following definition for RHCD:<sup>8</sup>

*“Reproductive health care data” means any of the following:*

*(1) Information about a consumer searching for, accessing, procuring, using, or otherwise interacting with goods or services associated with the human reproductive system, which includes goods such as contraception (e.g., condoms, birth-control pills), pre-natal and fertility vitamins and supplements, menstrual-tracking apps, and hormone-replacement therapy. It also includes, but is not limited to, services such as sperm- and egg-freezing, In Vitro Fertilization, abortion care, vasectomies, sexual health counseling; treatment or counseling for sexually transmitted infections, erectile dysfunction, and reproductive tract infections; and precise geolocation information about such treatments.*

*(2) Information about the consumer’s sexual history and family planning, which includes information a consumer inputs into a dating app about their history of sexually transmitted infections or desire to have children is considered sexual history and family planning information.*

*(3) Inferences about the consumer with respect to (1) or (2).*

Although the proposed definition does state that RHCD is information “about” a consumer, it does not explicitly state that such information is sensitive personal information under the CCPA. In evaluating the NAI’s recommendation for updating the proposed definition to state this explicitly, the Agency should consider both (1) the role of the defined term RHCD within the Delete Act; as well as (2) the overall purpose of the proposed regulations and how the defined term RHCD works to serve that purpose.

Regarding the first point, the role of the defined term RHCD in the proposed regulations is to clarify when a business must indicate that it “collects consumers’ reproductive health care data” when completing its annual registration as a data broker with the Agency.<sup>9</sup> After a business provides this information to the Agency, the Agency publishes it on the Registry and enables the public to view the list of businesses on the Registry based on whether those

---

<sup>7</sup> See CAL. PRIV. PROT. AGENCY, Initial Statement of Reasons at 1-2 (July 5, 2024), [https://cppa.ca.gov/regulations/pdf/data\\_broker\\_reg\\_isor.pdf](https://cppa.ca.gov/regulations/pdf/data_broker_reg_isor.pdf) (hereinafter “ISOR”); CAL. CIV. CODE § 1798.99.80(a) (stating that CCPA definitions apply to the Delete Act unless otherwise specified).

<sup>8</sup> CAL. CODE REGS. tit. 11, § 7601 (proposed), [https://cppa.ca.gov/regulations/pdf/data\\_broker\\_reg\\_prop\\_text.pdf](https://cppa.ca.gov/regulations/pdf/data_broker_reg_prop_text.pdf).

<sup>9</sup> See CAL. CIV. CODE § 1798.99.82(b)(2)(E); ISOR at 8.

businesses collect reproductive health care data.<sup>10</sup> The way the Agency presents this information on the Registry suggests that the Agency views the Delete Act’s reporting requirement as working primarily in service of transparency for consumers, because the incorporation of the reported information on the Registry allows consumers to more easily identify which businesses may collect RHCD about them.

As to the second point, the Agency has indicated that the overall objectives of the proposed rulemaking – which should cover its definition of RHCD – include:<sup>11</sup>

*“ensur[ing] that data brokers provide accurate and adequate information to support the statute’s goals of consumer protection through transparency and informed decision-making when exercising the California Consumer Privacy Act (CCPA) privacy rights.”*

Reading these two points together, the NAI understands the main purpose of defining RHCD in the proposed regulations to be clarifying when a business must report to the Agency that it collects RHCD, which in turn empowers the Agency to give consumers transparency into which businesses on the Registry collect RHCD. But this transparency is not an end in itself – the added transparency should also support “informed decision-making”<sup>12</sup> for consumers when exercising their CCPA privacy rights. In other words, transparency into the collection of RHCD should enable consumers to more easily exercise their CCPA rights with businesses who collect it.

To help achieve this purpose, the NAI recommends that the Agency harmonize the proposed definition of RHCD with the CCPA by specifying that RHCD is “sensitive personal information.”<sup>13</sup> Doing so will clarify for both consumers and businesses that RHCD is subject to the consumer rights and business responsibilities set forth in the CCPA, including the rights to delete, to opt out of sales and sharing, as well as the right to limit the use of sensitive personal information.<sup>14</sup>

---

<sup>10</sup> See *Data Broker Registry*, CAL. PRIV. PROT. AGENCY, <https://cppa.ca.gov/data-broker-registry/> (last visited Aug. 15, 2024).

<sup>11</sup> ISOR at 1.

<sup>12</sup> *Id.*

<sup>13</sup> See CAL. CIV. CODE § 1798.140(ae). As a practical matter, specifying that RHCD is sensitive personal information also guarantees that it will be treated as “personal information,” because sensitive personal information is a subset of personal information under the CCPA; see *id.* § 1798.140(v)(1)(L) (specifying that personal information includes sensitive personal information); *id.* § 1798.140(ae) (including the term personal information in every enumerated type of sensitive personal information).

<sup>14</sup> See *id.* § 1798.105 (establishing the consumers’ right to delete); *id.* § 1798.120 (establishing the consumers’ right to opt out of the sale or sharing of personal information); *id.* § 1798.121 (establishing the consumers’ right to limit use and disclosure of sensitive personal information).

If the Agency does not make this clarification, businesses will be in the position of determining on an individual basis whether data they collect that does *not* meet the CCPA definition of personal information (*i.e.*, data that is publicly available, is lawfully made available to the general public, or is deidentified or aggregated)<sup>15</sup> may nevertheless be RHCD under the Delete Act, which could lead to inconsistencies and additional compliance burdens. Further, without this clarification, consumers may be misled into believing that a business is collecting personal information about them that relates to their reproductive health care even if that business only processes, *e.g.*, de-identified or aggregate data relating to reproductive health care. The result could be that consumers seeking to exercise their CCPA rights after learning which businesses collect RHCD through the Registry would not have their expectations met – because under the current proposed definition, it would be possible that no CCPA rights relate to certain RHCD.

Similar issues could arise when considering whether RHCD is not only personal information, but also *sensitive* personal information. The definition of RHCD should not require businesses to determine individually whether personal information they process that is *not* classified as sensitive personal information under the CCPA may nevertheless be RHCD under the Delete Act. Instead, the Agency should define RHCD as a type of sensitive personal information, because RHCD should always be a subset of personal information that is “collected and analyzed concerning a consumer’s health” and/or their “sex life.”<sup>16</sup> Defining RHCD as a type of sensitive personal information will also assist consumers in exercising their privacy rights when they visit the Registry and learn that a business collects RHCD. For example, a consumer may identify that a business on the Registry collects RHCD and seek to exercise their right to limit the use of sensitive personal information with that business under the CCPA.<sup>17</sup> The consumer is sure to have their expectation met (*i.e.*, that the use of RHCD relating to them will be limited) if the Agency specifies by definition that RHCD is sensitive personal information.

The NAI appreciates the care demonstrated by the Agency in seeking to align the definition of RHCD with other aspects of California law that address information related to reproductive health care;<sup>18</sup> but the proposed definition should also address the more fundamental issue of RHCD’s status as sensitive personal information under the CCPA. As discussed above, this will promote clarity and consistency both for consumers who are seeking to exercise their CCPA

---

<sup>15</sup> See *id.* § 1798.140(v)(2)-(3).

<sup>16</sup> See *id.* § 1798.140(ae)(2) (including personal information collected and analyzed relating to a consumer’s health and relating to a consumer’s sex life as types of sensitive personal information).

<sup>17</sup> See *id.* § 1798.121(a).

<sup>18</sup> See ISOR at 9 (explaining the proposed definition of RHCD is consistent with the definitions of similar terms in other areas of California law); see also CAL. HEALTH & SAFETY CODE § 128560(b) (defining “reproductive health”); CAL. CIV. CODE § 1798.300(e) (defining “reproductive health care services”); CAL. CIV. CODE § 56.05(q) (defining “reproductive or sexual health application information”).

rights based on the additional transparency into the collection of RHCD provided through the Registry as well as for businesses seeking to report the information required by the Delete Act.

*B. Recommended amendments to the proposed definition of RHCD*

The NAI recommends that the Agency amend its proposed definition of RHCD as set forth below to state explicitly that RCHD is sensitive personal information:

*“Reproductive health care data” means [sensitive personal information \(as defined by Cal. Civ. Code § 1798.140\(ae\)\) collected and analyzed concerning](#) any of the following:*

*(1) ~~Information about~~ a consumer searching for, accessing, procuring, using, or otherwise interacting with goods or services associated with the human reproductive system, which includes goods such as contraception (e.g., condoms, birth-control pills), pre-natal and fertility vitamins and supplements, menstrual-tracking apps, and hormone-replacement therapy. It also includes, but is not limited to, services such as sperm- and egg-freezing, In Vitro Fertilization, abortion care, vasectomies, sexual health counseling; treatment or counseling for sexually transmitted infections, erectile dysfunction, and reproductive tract infections; and precise geolocation information about such treatments.*

*(2) ~~Information about~~ the consumer’s sexual history and family planning, which includes information a consumer inputs into a dating app about their history of sexually transmitted infections or desire to have children is considered sexual history and family planning information.*

*(3) Inferences about the consumer with respect to (1) or (2).*

Adopting these changes to the proposed definition of RHCD would align the additional transparency the Delete Act provides into the processing of RHCD with the CCPA’s definition of sensitive personal information, which furthers consumers’ ability to exercise their privacy rights with businesses based on what they learn from the Registry. Further, it would promote consistency and administrability for businesses complying with both the CCPA and the Delete Act.



II. Comments regarding the scope of the reporting requirements for precise geolocation and reproductive health care data.

- A. *The Agency should not require business to report that they collect RHCD or precise geolocation if they process those types of information solely for the purpose of deleting, de-identifying, aggregating, or rendering them non-sensitive.*

Businesses collect information about consumers from a variety of sources that may include both sensitive and non-sensitive information. Some businesses incorporate more sensitive types of data directly into their commercial data products while taking the steps necessary to process those data types in a way that respects consumer privacy and complies with the law. Other businesses do not directly commercialize those types of data and instead take steps to avoid or minimize their processing of them by processing them only for purposes of deleting, de-identifying, aggregating, or rendering them non-sensitive (collectively, by “Minimizing” their processing of these data types).

For example, while some companies collect precise geolocation and incorporate precise geolocation directly into their data products, other businesses immediately “uplevel” precise geolocation information they collect by truncating latitude/longitude coordinates in a way that renders that information non-precise (*i.e.*, incapable of locating a consumer within a circle with a radius of 1,850 feet).<sup>19</sup> Similarly, for companies that do incorporate precise geolocation directly into their data products, some choose to take additional steps to minimize information related to reproductive healthcare by maintaining a directory of known reproductive healthcare facilities and suppressing any consumer precise geolocation that is associated with those facilities.<sup>20</sup>

As discussed in more detail below, the Agency should in its reporting requirements under the Delete Act<sup>21</sup> distinguish between businesses that Minimize their processing of RHCD or precise geolocation and businesses that collect RHCD and precise geolocation for other commercial purposes.

---

<sup>19</sup> See CAL. CIV. CODE § 1798.140(w). The NAI has also published guidance on rendering location information imprecise. See generally GUIDANCE FOR NAI MEMBERS: DETERMINING WHETHER LOCATION IS IMPRECISE (2020), [https://thenai.org/wp-content/uploads/2021/07/nai\\_impreciselocation2.pdf](https://thenai.org/wp-content/uploads/2021/07/nai_impreciselocation2.pdf)

<sup>20</sup> See generally NAI Precise Location Information Solution Provider Voluntary Enhanced Standards, NETWORK ADVERT. INITIATIVE (June 22, 2022), <https://thenai.org/accountability/precise-location-information-solution-provider-voluntary-enhanced-standards/>.

<sup>21</sup> See CAL. CIV. CODE § 1798.99.82(b)(2)

The Delete Act requires a business registering with the Agency as a data broker to indicate whether the business collects certain types of information, including precise geolocation and RHCD.<sup>22</sup> As discussed in more detail above<sup>23</sup> – and consistent with the Agency’s statements in the ISOR<sup>24</sup> – the NAI understands the main purpose of these disclosures to be in service of transparency to consumers who review the list of businesses on the Registry, which in turn helps those consumers in exercising their CCPA rights with those businesses.

However, the reporting requirements in the Delete Act do not explicitly account for the fact that some businesses take proactive steps to Minimize information that may otherwise qualify as RHCD or precise geolocation (or both). If a business that Minimizes its processing of these data types is nonetheless required to report to the Agency that it collects RHCD and/or precise geolocation – and is subsequently identified to the public on the Registry as a business that collects those types of information – that result does not increase transparency for consumers or assist them in exercising their CCPA rights. Instead, it is more likely to mislead consumers toward the conclusion that businesses Minimizing their processing of potentially sensitive information are the same as companies that collect and process such information directly for commercial purposes.

To prevent this outcome, the Agency should distinguish in the Delete Act’s reporting requirements between businesses that Minimize RHCD and/or precise geolocation from businesses that collect those types of data for other commercial purposes. There is strong precedent for making this type of distinction, both in industry self-regulatory practices as well as in FTC enforcement actions.

As to industry self-regulation, the NAI’s Precise Location Information Solution Provider Voluntary Enhanced Standards (the “VES”) led the way in 2022 by requiring VES signatories to proactively identify and suppress sensitive points of interest, including locations associated with reproductive health care such as fertility or abortion clinics.<sup>25</sup> This includes an obligation for VES signatories to never use, allow the use of, sell, or share any information about device or user activity correlated to a known sensitive point of interest such as a reproductive health care facility.<sup>26</sup> But the NAI recognized that in order for signatories to meet this obligation, they may need to undertake certain limited processing of data associated with sensitive points of interest

---

<sup>22</sup> See *id.* § 1798.99.82(b)(2)(D)-(E).

<sup>23</sup> See *supra* section I.

<sup>24</sup> See ISOR at 1.

<sup>25</sup> See generally NAI Precise Location Information Solution Provider Voluntary Enhanced Standards, NETWORK ADVERT. INITIATIVE (June 22, 2022), <https://thenai.org/accountability/precise-location-information-solution-provider-voluntary-enhanced-standards/>.

<sup>26</sup> *Id.* § I(C).

– for example, transferring that information to a service provider to the extent doing so is necessary to facilitate compliance with the VES.<sup>27</sup>

Recent enforcement actions from the FTC – which largely track the principles underlying the NAI’s VES – also focused on the processing of information associated with sensitive points of interest such as reproductive health care facilities.<sup>28</sup> However, in the settlement agreements associated with those enforcement actions, the FTC also allowed for certain limited processing of information associated with sensitive points of interest for compliance purposes, including to render the information non-sensitive. Specifically, although the respondent in one settlement agreement was prohibited from selling, licensing, transferring, sharing, disclosing, or otherwise using sensitive location data;<sup>29</sup> the respondent was also required to process that same information in order to comply by “deleting or rendering non-sensitive” the sensitive location data at issue.<sup>30</sup> In another settlement agreement, the respondent agreed to delete certain sensitive location data it had already collected by ensuring such data were “deleted, de-identified or rendered non-sensitive.”<sup>31</sup> In both cases, the FTC recognized that the respondents, in order to minimize processing of sensitive information already collected, would need to conduct limited further processing solely to delete, de-identify, or render non-sensitive the information at issue.

By making a similar distinction in the Delete Act’s reporting requirements and allowing businesses to indicate that they do not collect RHCD and/or precise geolocation if their processing is limited to Minimizing those data types, the Agency can create an incentive for data brokers to minimize their processing of those categories of sensitive information while preserving consumers’ ability to understand which registered data brokers processes those categories directly for commercial purposes.

---

<sup>27</sup> See *id.* at 3 (setting forth in commentary limited exceptions for processing sensitive points of interest for compliance purposes).

<sup>28</sup> See In the Matter of X-Mode Social, Inc., FTC C-4802 Complaint at ¶44 (Apr. 11, 2024), [https://www.ftc.gov/system/files/ftc\\_gov/pdf/X-ModeSocialComplaint.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialComplaint.pdf) (alleging that X-Mode data could be used to “track consumers who have visited women’s reproductive health clinics[.]”); In the Matter of InMarket Media, LLC, FTC C-4803 Complaint at ¶6, [https://www.ftc.gov/system/files/ftc\\_gov/pdf/InMarketMedia-Complaint.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/InMarketMedia-Complaint.pdf) (alleging that InMarket “collects sensitive information from consumers, including . . . where they receive medical treatment[.]”).

<sup>29</sup> In the Matter of X-Mode Social, Inc., FTC C-4802 Decision and Order at § II (Apr. 11, 2024), [https://www.ftc.gov/system/files/ftc\\_gov/pdf/X-ModeSocialDecisionandOrder.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf).

<sup>30</sup> See *id.* § III.G; *id.* § XIII(B) (referring to processing certain location data to delete, deidentify, or render non-sensitive).

<sup>31</sup> In the Matter of InMarket Media, LLC, FTC C-4803 Decision and Order at § XII. (Apr. 29, 2024), [https://www.ftc.gov/system/files/ftc\\_gov/pdf/InMarketMedia-Complaint.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/InMarketMedia-Complaint.pdf).

*B. Recommended amendments to the proposed regulations to address disclosure obligations related to limited processing of RHCD and precise geolocation.*

To address the issues discussed above, the NAI recommends that the Agency add a new subsection (e) to section 7603 of the proposed regulations to distinguish between businesses that process RHCD and/or precise geolocation only to Minimize it and those that process those data types for other commercial purposes, as follows:

*§ 7603. Registration Information Requirements.*

*(a) A data broker must provide only true and correct responses when submitting the registration information required by Civil Code section 1798.99.82.*

*(b) All website links and email addresses provided in the registration must be accurate and functioning.*

*(c) In addition to the information required by Civil Code section 1798.99.82, a data broker must include the business's trade name (i.e., "DBA"), if applicable, and provide the Agency with a point of contact, including name, email, and phone number. The point of contact information will not be posted on the public data broker registry.*

*(d) When reporting the extent to which the data broker is regulated by the other laws described in Civil Code section 1798.99.82(b)(2)(H), a data broker must describe:*

*(1) The types of personal information the data broker collects and sells that are subject to the enumerated laws;*

*(2) The specific product(s) or services covered by the enumerated state or federal law;*

*(3) The approximate proportion of data collected and sold that is subject to the enumerated laws in comparison with their total annual data collection and sales (i.e., percentage of their general data broker activities).*

*(e) When submitting the registration information required by Civil Code section 1798.99.82(b)(2), a data broker is not required to indicate to that it collects the following types of data if its collection and processing of such data is limited solely to the short-term, transient use of such data for purposes of deleting, de-identifying, aggregating, or*

*rending non-sensitive the relevant data type(s), and the data broker does not use such data directly for any other commercial purpose:*

*(1) Reproductive health care data;*

*(2) Precise geolocation.*

Adopting these changes to the proposed regulations would improve transparency for consumers by highlighting only those businesses on the Registry that directly commercialize RHCD and/or precise geolocation and would create a clear incentive for businesses to minimize their processing of those data types by easing a reporting requirement.

III. Conclusion

The NAI appreciates the opportunity to submit comments to the Agency on the proposed data broker registration regulations. If we can provide any additional information, or otherwise assist your office as it continues to engage in the rulemaking process, please do not hesitate to contact me at [REDACTED], or David LeDuc, Vice President, Public Policy, at [REDACTED]

\*\*\*\*\*

Respectfully Submitted,

[REDACTED]  
**Tony Ficarrotta**  
Vice President & General Counsel  
Network Advertising Initiative (NAI)

---

**From:** Shapiro, Tracy [REDACTED]  
**Sent:** Tuesday, August 20, 2024 12:52 PM  
**To:** Regulations@CPPA  
**Cc:** Holman, Eddie; Lee, Doo  
**Subject:** Public Comment on Data Broker Registration Regulations  
**Attachments:** 2024-08-20 CPPA Delete Act Proposed Regulations Public Comment.pdf

---

**This Message Is From an Untrusted Sender**

**Warning:** This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Dear Board Members and Staff of the California Privacy Protection Agency:  
Please find attached our comments in response to the California Privacy Protection Agency's invitation for comments on the Data Broker Registration Regulations.  
Thank you,  
Tracy Shapiro

[REDACTED] Shapiro | Partner, Privacy & Cybersecurity | Wilson Sonsini Goodrich & Rosati  
[REDACTED] Street | San Francisco, CA 94105 | [REDACTED]

This email and any attachments thereto may contain private, confidential, and privileged material for the sole use of the intended recipient. Any review, copying, or distribution of this email (or any attachments thereto) by others is strictly prohibited. If you are not the intended recipient, please contact the sender immediately and permanently delete the original and any copies of this email and any attachments thereto.



TRACY SHAPIRO

Internet

Direct dial:

August 20, 2024

Attn: Elizabeth Allen  
California Privacy Protection Agency  
2101 Arena Boulevard  
Sacramento, CA 95834  
[regulations@cpha.ca.gov](mailto:regulations@cpha.ca.gov)

Re: Public Comment on Data Broker Registration (“Delete Act”) Regulations

Dear Board Members and Staff of the California Privacy Protection Agency:

Wilson Sonsini Goodrich & Rosati appreciates the opportunity to submit these comments in response to the California Privacy Protection Agency’s (“CPPA”) invitation for comments on the Data Broker Registration Regulations, also known as the “Delete Act” regulations, Cal. Code Regs. tit. 11, §§ 7600 7605 (“Proposed Regulations”). We submit these comments on behalf of certain of our clients, though to be clear, these comments do not necessarily reflect the views of all of our clients. These companies appreciate the importance of consumer privacy and data protection, and we submit these comments with the aim of encouraging the CCPA to issue regulations that will protect the privacy of consumers in a manner that is effective, practical, and allows companies to continue to provide consumers with valuable services.

## I Introduction

The Delete Act, which built on California’s existing data broker registration law, applies to “data brokers” businesses that knowingly collect and sell to third parties the personal information of a consumer with whom the business *does not* have a direct relationship. The Proposed Regulations seek to modify and drastically expand the term “data broker” to cover companies that *do* have direct relationships with consumers. This proposed expansion contradicts the statutory definition and enlarges its scope in violation of the California Administrative Procedures Act (the “Cal APA”). It also runs afoul of the California legislature’s clear intent to limit the Delete Act to businesses that do not have direct relationships with consumers, and is inconsistent with the legislature’s stated policy goals. To avoid a violation of the Cal APA, we respectfully request that the CCPA revise Section 7601(a) to remove the following sentence from the Proposed Regulations: “A business is still a data broker if it has a direct relationship with a consumer but also sells personal information about the consumer that the business did not collect directly from the consumer.”

## II. Regulations Promulgated by California Agencies are Invalid under the Cal APA to the Extent They Conflict with or Enlarge the Scope of a Statute

The Cal APA governs the adoption of regulations by California state agencies, including the CPPA. *See* Cal. Gov. Code § 11340 et seq. For regulations to be effective, they must fall “within the scope of authority conferred and in accordance with standards prescribed by other provisions of law.” Cal. Gov. Code § 11342.1. Further, “no regulation adopted is valid or effective unless consistent and not in conflict with the [authorizing] statute and reasonably necessary to effectuate the purpose of the statute.” *Cal. Gov. Code* § 11342.2.

Any substantial failure to comply with the Cal APA in adopting regulations may be the basis for a judicial declaration that the regulations are invalid. Cal. Gov. Code § 11350(a). In fact, courts have held that “administrative regulations that *alter or amend the statute or enlarge or impair its scope* are void and courts not only may, but it is their obligation, to strike down such regulations.” *Ontario Community Foundation, Inc. v. State Board of Equalization*, 35 Cal. 3d 811, 817 (Cal. Sup. Ct. 1984). “No protestations that [regulations] are merely an exercise of administrative discretion can sanctify them.” *Id.*

On this basis, California courts have repeatedly struck down California agency regulations that have overstepped their statutory authority in violation of Cal APA. *See, e.g., Citizens to Save California v. California Fair Political Practices Commission*, 145 Cal. App. 4th 736 (Cal. Ct. App. 2006) (striking down the California Fair Political Practices Commission’s regulations because “whatever the wisdom of the FPPC’s effort to plug loopholes in California’s campaign regulatory scheme” the regulation “conflict[ed] with multiple provisions of the Political Reform Act,” was “at odds with the language of the [statute]” and therefore “exceed[ed] the FPPC’s authority.”); *Slocum v. State Bd. of Equalization*, 134 Cal.App.4th 969, 974 (Cal. Ct. App. 2005) (holding that the California State BOE’s effort to expand calamity reassessment relief beyond the requirement of direct physicality embedded in the Revenue and Taxation Code was invalid because “agencies do not have discretion to promulgate regulations that are inconsistent with the governing statute, or that alter or amend the statute or enlarge its scope.”); *West Coast Chapter of the Institute of Scrap Recycling Industries. v. Smithline*, (Sup. Ct. Case No. 2019 00257463, ruling dated October 22, 2021) (declaring that the California Department of Resources’ “solid waste” regulations were invalid under the Cal APA to the extent the agency applied them scrap recycler’s recyclable materials, because the legislature’s amendments did not expand the statute’s definitions to include “recyclables” that had not been discarded as “solid waste” and legislative intent was to only apply the materials to solid waste, “which by definition is discarded material.”); *Ontario Community Foundation, Inc. v. State Board of Equalization*, 35 Cal. 3d 811 (Cal. Sup. Ct. 1984) (holding the California State BOE’s regulation invalid where the legislature had exempted “occasional sales” from a tax imposed on “retail sales” but the BOE’s regulation withheld the exemption if the seller of the “occasional sale” was a “unitary business” also engaged in other sales which are not tax exempt, and explaining that “there is no agency discretion to promulgate a regulation which is inconsistent with the governing statute” and “our function is to inquire into the legality of the regulations, not their wisdom.”); *Woods v. Superior Court*, 28 Cal. 3d 668, 679 (Cal. 1981) (stating “administrative regulations which exceed the scope of the enabling statute are invalid and have no force or life” and upholding the Department of Social Services Director’s



Elizabeth Allen  
August 20, 2024  
Page 3

refusal to apply an invalid regulation); *Morris v. Williams*, 67 Cal. 2d 733, 748 (Cal. 1967) (striking down regulations by the Health and Welfare Agency that reduced Medi Cal benefits because they “contravene[d] the legislative intent expressed in [the statute]” by reducing services for both “recipients” and the “medically indigent” when the statute clearly establishes a “mandatory order of priorities” that prescribed reducing coverage for the “medically indigent” before “recipients”).

### III. The Proposed Regulations Conflict with and Enlarge the Delete Act’s “Data Broker” Definition in Violation of the Cal APA

The Delete Act authorizes but does not require the CPPA to adopt regulations pursuant to the Cal APA to implement and administer the statute. Cal. Civ. Code § 1798.99.87(a). Similar to the cases above, the Proposed Regulation if adopted, would alter and enlarge the scope of the statute. Specifically, the scope of companies covered by the Delete Act would be substantially broadened by redefining what is means to be a “data broker.”

The relevant definition of a “data broker” was first set forth in AB 1202, enacted by the California legislature in 2019 to require “data brokers” to register annually with the California Attorney General. In 2023, the legislature enacted the Delete Act, SB 362, thereby amending AB 1202 and augmenting California residents’ ability to exercise their personal deletion rights. The Delete Act did not, however, change or expand the definition of “data broker” i.e., “a business that knowingly collects and sells to third parties the personal information of a consumer *with whom the business does not have a direct relationship.*” To the contrary, the legislature considered the scope of the term and further *narrowed* it by adding a new exemption for HIPAA covered entities and business associates

Nevertheless, the CPPA now proposes to alter the definition of “data broker” in a way that directly conflicts with the Delete Act’s definition and drastically expand the scope of companies covered by the law. The CPPA does this not by explicitly revising the definition of data broker. Rather, in defining a “direct relationship,” it adds the following commentary after the proposed definition: “A business is still a data broker if it has a direct relationship with a consumer but also sells personal information about the consumer that the business did not collect directly from the consumer.”

The proposed change contradicts the statute’s text, which prescribes that a “data broker” is a business that “does not have a direct relationship” with a consumer, and is not supported by legislative history or intent, as further discussed below. This change would erase the important, statutorily recognized distinction between those businesses with whom consumers knowingly and intentionally engage (and thus are aware of how to exercise their rights directly) and those

---

Cal. Civ. Code 1798.99.87(b) provides for a narrow exemption from the Cal APA for any regulations adopted to establish data broker registration fees but not other regulations adopted pursuant to the Delete Act.

businesses with whom consumers do not engage with directly (for which the data broker registry was created).

#### IV. The Proposed Regulations are Contrary to Legislative Intent and Purpose

In addition to the text contained in the statute, the legislative history of AB 1202 and SB 362 also makes clear that the California legislature intended the data broker registration requirements to exclude all companies that have a direct relationship with consumers. The legislative findings for AB 1202 emphasize that “there are important differences between data brokers and businesses with whom consumers have a direct relationship,” making clear that the legislature saw these as binary concepts.<sup>3</sup> The key difference, the legislature explained, is that where consumers have a direct relationship with a business, consumers “have some level of knowledge about and control over the collection of data by those businesses, including: the choice to use the business’ products or services, the ability to review and consider data collection policies, the ability to opt out of certain data collection practices, the ability to identify and contact customer representatives, and the knowledge necessary to complain to law enforcement.”<sup>4</sup> This is equally true where a business has a direct relationship with consumers and collects data from sources other than the consumer.

Consistent with these legislative findings, Senator Becker, the author of the Delete Act, stated that the purpose of the bill was to “empower consumers to control their own data from *unknown* third party data brokers.”<sup>5</sup> He described data brokers as entities that “spend their days and nights building dossiers with millions of people’s [sensitive information] so they can sell it to the highest bidder.”<sup>6</sup> He further explained that “it’s disturbing to see how much information is out there on each one of us that some people just don’t know about. Part of the goal [with the Delete

---

<sup>2</sup> [https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill\\_id=201920200AB1202](https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1202)

<sup>3</sup> While AB 1202 did not define “direct relationship,” the legislative findings describe consumers forming direct relationships by, for example, visiting a business’ premises or internet website or by affirmatively and intentionally interacting with a business’ online advertisements. The legislative findings draw no distinction between whether a business collected data directly from a consumer vs. from a third party.

<sup>4</sup> [https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill\\_id=201920200AB1202](https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1202)

<sup>5</sup> [https://sd13.senate.ca.gov/news/press\\_release/september\\_2023/senator\\_beckers\\_delete\\_act\\_clears\\_assembly\\_appropriations](https://sd13.senate.ca.gov/news/press_release/september_2023/senator_beckers_delete_act_clears_assembly_appropriations)

<sup>6</sup> [https://sd13.senate.ca.gov/news/press\\_release/may\\_3\\_2023/senator\\_beckers\\_delete\\_act\\_advances\\_senate\\_floor](https://sd13.senate.ca.gov/news/press_release/may_3_2023/senator_beckers_delete_act_advances_senate_floor)

Elizabeth Allen  
August 20, 2024  
Page 5

Act] is to just bring it out of the shadows... [the dossier is] quite extensive.”<sup>7</sup> Senator Becker’s statements further support that the statute was not intended to cover companies that may tangentially collect and sell non direct consumer data as part of an already existing and intentional consumer business relationship.

Many businesses wear multiple hats by collecting some personal information directly from consumers while also utilizing other personal information obtained from third parties (e.g., from third party apps and services that consumers connect to the business’s service, from ad calls in the ad tech ecosystem, or from data providers). There is simply no evidence in the legislative record to suggest that the legislature intended businesses that have direct relationships with consumers to be covered by the Delete Act on the basis that they collect some data about a consumer from sources other than the consumer.

#### **V. The Proposed Regulations Do Not Further the Policy Goal of Encouraging Consumers to Exercise their Deletion Rights**

Forcing companies with direct consumer relationships to register as data brokers will result in consumers unwittingly having their accounts on various services deleted if they sign up for the accessible deletion mechanism. This is because the Delete Act says that the mechanism “shall allow a consumer to request the deletion of *all personal information related to that consumer* through a single deletion request” (emphasis added). Since the deletion mechanism would apply to companies with which the consumer has directly and intentionally established business relationships, forcing these companies to delete the consumer’s account would result in a terrible consumer experience and discourage consumers from using the deletion mechanism.

Further, the Proposed Regulations risk creating an unreasonable interpretation where if a business creates internally generated inferences about a consumer using information it collected from the consumer and then discloses that data, for example, to a third party ad tech partner to facilitate advertising (which the [California Attorney General’s enforcement action against Sephora](#)) makes clear may constitute a “sale”), that business could be considered a “data broker” because the business created those inferences rather than collecting them “directly from the consumer.” At a minimum, the CPPA should clarify that a business does not become a data broker merely by “selling” internally generated inferences about consumers with whom it has a direct relationship.

#### **VI. Conclusion**

In summary, we respectfully request that the CPPA revise Section 7601(a) of the Proposed Regulations as follows to remove the language that conflicts with the Delete Act, its legislative purpose and intent, and its policy goals:

---

<sup>7</sup> California State Senator Josh Becker on privacy, data brokers and why he’s sponsoring the Delete Act (September 7, 2023) available at <https://digiday.com/marketing/california-state-senator-josh-becker-privacy-data-brokers-and-why-hes-sponsoring-the-delete-act/>

Elizabeth Allen  
August 20, 2024  
Page 6

**§ 7601. Definitions.**

In addition to the definitions set forth in Civil Code section 1798.99.80:

(a) "Direct relationship" means that a consumer intentionally interacts with a business for the purpose of obtaining information about, accessing, purchasing, using, or requesting the business's products or services within the preceding three years. A consumer does not have a "direct relationship" with a business if the purpose of their engagement is to exercise any right described under Title 1.81.5 of Part 4 of Division 3 of the Civil Code, or for the business to verify the consumer's identity. A business is still a data broker if it has a direct relationship with a consumer but also sells personal information about the consumer that the business did not collect directly from the consumer.

Sincerely,

WILSON SONSINI GOODRICH & ROSATI  
Professional Corporation

[Redacted Signature]

Tracy Shapiro

[Redacted Signature]

Eddie Holman

---

**From:** Tim Lynch [REDACTED]  
**Sent:** Tuesday, August 20, 2024 1:02 PM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on Data Broker Registration Regulations  
**Attachments:** Yahoo\_Public Comment on Data Broker Registration Regs.pdf

---

**This Message Is From an External Sender**

WARNING: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

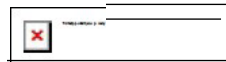
[Report Suspicious](#)

To whom it may concern:

Attached please find Yahoo's comments with regard to the July 5, 2024 Notice of Proposed Rulemaking concerning Data Broker Registration requirements.

Best,

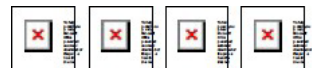
Tim



**Tim Lynch**

Head of US Federal Affairs  
Public Policy Team

**M** [REDACTED]  
**E** [REDACTED]  
Washington, D.C.



By email

Subject Line: Public Comment on Data Broker Registration Regulations

August 20, 2024

California Privacy Protection Agency

Attn: Elizabeth Allen

2101 Arena Blvd.

Sacramento, CA 95834

[regulations@ccpa.ca.gov](mailto:regulations@ccpa.ca.gov)

To Whom It May Concern:

Please find below comments from Yahoo, Inc. with respect to the July 5, 2024 Notice of Proposed Rulemaking concerning Data Broker Registration requirements. Yahoo thanks the California Privacy Protection Agency ("Agency") for the opportunity to provide feedback on the proposed regulations under the Delete Act and for considering these comments.

As a medium-sized legacy technology company that prides itself on being a trusted first-party provider of email and search services, Yahoo supports the Delete Act and similar legislative efforts to bring transparency to, and ready controls over, the activities of companies whose practices and even identities are otherwise invisible to consumers. In that same vein, Yahoo appreciates the Agency's effort to clarify provisions of the Delete Act, including with respect to what it means for a business to have a "direct relationship" with a consumer as that term is used in the Delete Act's definition of "data broker." Cal. Civ. Code § 1798.S0(c).

The first two sentences of the proposed definition of "direct relationship" reflected in the Agency's proposed regulations help achieve this clarity, first by setting reasonable timelines and boundaries over how these first-party relationships operate, and second by ensuring companies may not exploit a consumer making a rights request as a loophole to assert a "direct relationship." The third sentence of the proposed "direct relationship" definition, however, redefines what it means to be a data broker rather than clarifying what it means to have a direct relationship with a consumer. The result would be to sweep in companies that do have direct and established relationships with consumers in the event they (however incidentally) collect personal information about them from other sources. For the reasons below, including this sentence would exceed the Agency's authority, be contrary to legislative intent, conflict with similar regimes adopted in other states, and frustrate and confuse consumers rather than serve them.

- 1. The Proposed Definition Exceeds the Bounds of Mere Clarification - and the Agency's Rulemaking Authority- and Would Significantly Expand the Scope of the Delete Act*



The Delete Act defines data broker as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." Cal. Civ. Code § 1798.80(c). This statutory definition clearly establishes that the "direct" qualifier speaks to the business's relationship with the consumer, rather than the context in which personal information is collected and puts businesses that collect personal information directly from consumers outside of the bounds of the Delete Act.

The final sentence in the definition of "direct relationship" reflected in the proposed regulations would impermissibly expand this clear, statutorily-defined, concept of what it means to be a "data broker": "A business is still a data broker if it has a direct relationship with a consumer but also sells personal information about the consumer that the business did not collect directly from the consumer." By inserting a new "direct" requirement that is tied to the *personal information* collected and sold rather than the relationship between the consumer and the business, this sentence would fundamentally alter the Delete Act. Beyond being unnecessary to "implement and administer" the Delete Act, Cal Civ. Code § 1798.99.81(a), it would expand the statutory definition of data broker to include companies that have deep and established direct relationships with *consumers* merely because some personal information such companies "sell" - however incidentally - was not collected directly from the consumer.

Such a fundamental expansion of the statute's scope exceeds the Agency's rulemaking authority.<sup>1</sup> It is also impractical and inconsistent with consumer expectations. Particularly given how broadly California authorities have interpreted the term "sell,"<sup>2</sup> the inclusion of this sentence would potentially require thousands of companies that have direct relationships with consumers, do not "sell" personal information in the way consumers understand that word, and do not meet the Delete Act's definition of "data broker" to nevertheless register as such and to process centralized deletion requests. Such companies are likely to include a wide range of companies that no reasonable consumer will expect to delete their data when they employ a centralized deletion mechanism meant to control shadowy third parties. For example, a retailer might be forced to register as a data broker, and thus receive deletion requests from a centralized deletion mechanism, simply because they allow consumers to provide other people's personal information in order to send them a gift. Publishers and gaming and entertainment apps may similarly be pulled in, for instance if they offer "refer a friend" type functionality.

*2. The Draft Regulations Would Depart from the Scope of Entities Contemplated by Legislators And Similar Laws Adopted in Other States.*

California lawmakers adopted the Delete Act to address risks associated with businesses that fit within the common understanding of the term "data broker" shared by the Federal Trade Commission and the drafters of California's existing Data Broker Registration Law

---

<sup>1</sup> See, e.g., *Morris v. Williams*, 433 P.2d 697, 748 (Cal. 1967) ("Administrative regulations that alter or amend the statute or enlarge or impair its scope are void.").

<sup>2</sup> See, e.g. Compl. [People v. Sephora USA, Inc.](#), at 4.



alike - i.e., "companies whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analyzing, and sharing that information, or information derived from it, for purposes such as marketing products, verifying an individual's identity, or detecting fraud."<sup>3</sup> In such traditional data broker relationships, the Assembly Committee on Privacy and Consumer Protection noted, "there is no direct relationship between a *consumer* and any data broker that has information about the consumer.....[and t]he key point to understand is that no consumer chooses to have a relationship with a data broker."<sup>4</sup> This commentary illustrates a focus on the consumer/business relationship rather than concern with the source of personal information. Indeed, two hallmarks of first-party relationships are the consumer's choice to interact with the business and the business's identity being front-and-center to the consumer. If adopted without modification, the draft regulations would depart and distract from the statutory goal of addressing companies that operate out of sight from the consumer and without such a direct relationship, and instead bring in countless companies that have direct, first-party relationships with consumers and with whom consumers choose to interact to obtain products and services.

Adopting the regulations without adjustment would also represent a stark departure from how the term "data broker" is defined under other state data broker laws in force today, contrary to the Agency's stated goal of achieving consistency across privacy regimes,<sup>5</sup> and contrary to the law on which it was modeled. AB 1202, which established California's data broker registry and the definition of "data broker" codified at California Civil Code Section 1798.80(c), was modeled off of Vermont's Data Broker Registration Law.<sup>6</sup> That law, and the laws enacted in three other states that now regulate data brokers, apply only to companies that do not have direct relationships with consumers or whose primary source of revenue is monetizing personal information.<sup>7</sup> None of these laws would deem retailers, publishers, or gaming or entertainment services that may incidentally disclose data they may not have collected directly from the consumer to be "data brokers." Adopting through regulation a definition of "data broker" that differs radically from parallel definitions in other states would likely result in California having potentially thousands more companies registered as data brokers than are registered in other states, leading to consumer confusion and undercutting legislative intent.

---

<sup>3</sup> *Analysis of S.B. 362 by Assem. Comm. on Priv. & Consumer Protection*, 2023-2024 Leg., Reg. Sess. 10 (Cal. 2023), [https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill\\_id=202320240SB362#](https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=202320240SB362#).

<sup>4</sup> *Id.* at 11 (emphasis added).

<sup>5</sup> See Cal. Priv. Prot. Agency, California Consumer Privacy Act Regulations Draft Initial Statement of Reasons (July 2024), [https://cppa.ca.gov/meetings/materials/20240716\\_item8\\_draft\\_omnibus\\_isor.pdf](https://cppa.ca.gov/meetings/materials/20240716_item8_draft_omnibus_isor.pdf) (noting efforts to harmonize its regulations with those adopted in other states); [CPRA § 3.C.8](#) (mandating that "[t]o the extent it advances consumer privacy and business compliance, the law should be compatible with privacy laws in other jurisdictions").

<sup>6</sup> *Analysis of S.B. 362 by S. Judiciary Comm.*, 2023-2024 Leg., Reg. Sess. 10 (Cal. 2023), [https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill\\_id=202320240SB362#](https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=202320240SB362#).

<sup>7</sup> See Vt. Stat. Ann. tit. 9, § 2430(4)(A)-(B); Or. Rev. Stat. Ann. § 646A.593(1)(c)(A)-(B); Nev. Rev. Stat. Ann. § 603A.323; Tex. Bus. & Com. Code Ann. § 509.001(4).





### 3. *The Proposed Definition Undermines Rather than Enhances the Delete Act's Overarching Goals Regarding Transparency and Consumer Control*

The statutory definition of "data broker" in the Delete Act maintains focus on companies that do not have a direct relationship with consumers, a scope that aligns with the problems California lawmakers sought to address through its adoption. Namely, the Delete Act's author and the Legislature alike were troubled by the "the emergence of data brokers that collect and profit from this data *without having any direct relationship with the consumers* whose information they amass"<sup>8</sup> and from whom such consumers "do not directly consume any products or services."<sup>9</sup>

The Delete Act was intended to address the impracticality of requiring consumers to make individual deletion requests with more than five hundred registered data brokers, particularly where such companies' identities are not well-known given the absence of a first-party relationship.<sup>10</sup> The Delete Act helps solve this problem by providing a mechanism for consumers to request deletion of their personal information from these invisible entities in, essentially, one click.<sup>11</sup> Yahoo supports these legislative goals and the Delete Act's effort to bring needed transparency into, and convenient controls over, the practices of companies with which consumers do not intentionally interact.

There is no similar policy justification for bringing companies with established, direct relationships with consumers within the scope of the universal deletion mechanism merely because certain - and often incidental - elements of personal information they process may have been collected from a source other than the consumer. Indeed, doing so would frustrate, rather than serve, consumers. Consumers are already well-aware that first parties hold their data. Moreover, thanks to California's leadership in enacting the nation's first omnibus consumer privacy law, such companies have already spent nearly five years and significant investment enabling consumers to exercise the important rights, including deletion, conferred by the California Consumer Privacy Act (including its amendments and regulations) directly with them. Thus, consumers already have the tools that they need to selectively exercise their deletion rights with respect to any companies that lose their trust or with whom they no longer choose to do business.

Including companies with first-party relationships in the universal deletion mechanism would also lead to confusion and potentially frustration. The point of a one-stop-shop mechanism is to request that companies with which consumers have no direct relationship, from which they receive no benefits or functionality, and the identities of which they do not know, delete

---

<sup>8</sup> *Analysis of S.B. 362 by S. Judiciary Comm.*, 2023-2024 Leg., Reg. Sess. 1, 11-12 (Cal. 2023), [https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill\\_id=202320240S8362#](https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=202320240S8362#) (emphasis added).

<sup>9</sup> *Analysis of S.B. 362 by Assem. Comm. on Priv. & Consumer Protection*, 2023-2024 Leg., Reg. Sess. 10-11 (Cal. 2023), [https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill\\_id=202320240S8362#](https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=202320240S8362#).

<sup>10</sup> *Analysis of S.B. 362 by S. Judiciary Comm.*, 2023-2024 Leg., Reg. Sess. 1, 11-14 (Cal. 2023), [https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill\\_id=202320240S8362#](https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=202320240S8362#).

<sup>11</sup> *Id.*



their personal information. Forcing companies that *have* direct relationships to participate in this deletion mechanism will mean that consumers are (best case) bombarded with questions regarding their intent or (worst case) find themselves unable to login to their accounts or learning that the company they had no reason to view as a data broker has disabled functionality the consumer relies upon, such as email service or photo storage, or deleted information such as shopping history.

\* \* \*

In order to stay within the confines of the Delete Act, serve legislative intent, maintain consistency with other data broker laws, and avoid the unintended consequences for consumers and first-party businesses alike, we urge the Agency to modify the draft regulations by deleting the final sentence of the proposed definition of "direct relationship," as shown below:

(a) "Direct relationship" means that a consumer intentionally interacts with a business for the purpose of obtaining information about, accessing, purchasing, using, or requesting the business's products or services within the preceding three years. A consumer does not have a "direct relationship" with a business if the purpose of their engagement is to exercise any right described under Title 1.81.5 of Part 4 of Division 3 of the Civil Code, or for the business to verify the consumer's identity. A business is still a data broker if it has a direct relationship with a consumer but also sells personal information about the consumer that the business did not collect directly from the consumer.

Yahoo appreciates the opportunity to submit comments on the proposed regulations for the Delete Act.

Sincerely,



Tim Lynch  
Head of US Federal Affairs  
Public Policy Team  
Yahoo, Inc.



---

**From:** Tracy Rosenberg [REDACTED]  
**Sent:** Tuesday, August 20, 2024 1:24 PM  
**To:** Regulations@CPPA  
**Subject:** Oakland Privacy Comments - Data Broker Rule Making  
**Attachments:** Oakland Privacy Public Comments - Data Broker Regulations Rule Making.pdf

---

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Please find enclosed these brief comments on the proposed regulations submitted on behalf of Oakland Privacy.

Thank you,

Tracy Rosenberg  
On behalf of Oakland Privacy

Tracy Rosenberg  
Executive Director  
Media Alliance  
2830 20th Street Suite 201  
San Francisco, CA 94110  
<https://media-alliance.org>

Email: [REDACTED]

Encrypted email at [REDACTED]

Text via Signal

Pronouns: She/Her/Hers



August 20, 2024

California Privacy Protection Agency  
2101 Arena Boulevard  
Sacramento, CA 95834

TITLE 11. LAW DIVISION 6. CALIFORNIA PRIVACY PROTECTION AGENCY  
CHAPTER 3. Data Broker Registration. NOTICE OF PROPOSED RULEMAKING Notice  
published July 5, 2024

### **Public Comments from Oakland Privacy**

Thank you for the opportunity to make comments to the Agency as you embark on your rule-making and enforcement duties granted under Senate Bill 362, The Delete Act.

Oakland Privacy is a citizen's coalition that works statewide to defend the right to privacy, enhance public transparency, and increase oversight. We were instrumental in the creation of the first standing municipal citizens' privacy advisory commission in the City of Oakland, and we have engaged in privacy enhancing legislative efforts with several California cities, regional entities and the State Assembly and Senate. As experts on municipal privacy reform, we have written use policies and impact reports for a variety of surveillance technologies, conducted research and investigations, and developed frameworks for the implementation of equipment with respect for civil rights, privacy protections and community consent.

Firstly, we would like to emphasize that the section (1798.99.86(d)(1) that requires data brokers to not only comply with consumers' DROP requests through the CPPA's page, but to **do so every 45 days on an ongoing basis**, is a very strong part of this bill. Where consumer privacy is concerned, the relationship between someone's personal data and a broker's pecuniary interest in monetizing that data is often deeply skewed in favor of the brokers. This requirement shifts the balance back toward individuals and away from corporations.

Other sections of the proposed regulations that we wanted to highlight as effective and that should remain in the finalized regulations:

Section 179.88.82(b)(2)(A) contains a strong **list of requirements** that data brokers must comply with in supplying information to consumers, including the steps and easy access to the processes for deleting/requesting removal of their data.

Section 1798.88.84 focuses on ensuring that the “**accessibility**” called for in the legislative language is delivered to users.

Section 1798.99.85(b) requires data brokers to reveal the number of requests they denied in whole or in part based on 4 reasons. Those are (1) The request was not verifiable, (2) the request was not made by a consumer, (3) the request called for information exempt from deletion, (4) the request was denied on other grounds. These transparency requirements will provide useful **data** going forward on how the system is working and what improvements or refinements may be needed at a later date, if any. We caution the Commission that fixes for problems with paid agents that the industry fears should, and appropriately so, wait for evidence from the transparency disclosures if there is a problem, and what the scale of the problem is. The Commission should desist from trying to fix future/anticipated problems until meaningful data is available.

There is also some room for improvement. In the introductory text to the Delete Act is this phrase: *“This bill would prohibit an administrative action pursuant to these provisions from being commenced more than 5 years after the date on which a violation occurred.”* Given that this is directly related to the effectiveness of the DROP portal, we believe it is important to consider how the timeline is measured. The CPPA ought to consider whether the date the violation occurred is the right start clock or whether it should be the date consumers, affected parties, and/or regulators were presumptively notified. To start the clock on the date of a violation—even if it is for five years—focuses the attention on the actions of the corporations. The focus of the rest of the bill, the implementation of the DROP portal, and much of the focus of the CPPA itself is on protecting consumers from harm. This perspective shift is not insignificant: it mirrors a recent shift in the American social concept of privacy and personal identity away from an industry-specific approach, which is largely dictated by the needs and desires of the commercial voices in those industries, towards something more closely resembling a European model, which places the attention on and centers decision making around the locus of harm to the consumer. Following this important shift in perspective, the CPPA might consider altering the timeline from 5 years after the violation occurred to 5 years after affected parties were **presumptively notified** of the violation.

Section 1798.99.82(c)(2) says *“A data broker that fails to register as required by this section is liable for administrative fines and costs in an administrative action brought by the [CPPA] as follows: An amount equal to the fees that were due during the period it failed to register.”* The fees are low. It's \$400/year to register as a data broker. It's \$200/day for each day they don't register after January 31st, which has a maximum of \$66,800 annually. The businesses in the CA data broker registry and in the sector as a whole range from fairly small to quite large. We have some concerns that for the largest of these, the failure to register fee is a literal drop in the bucket. The CPPA might want to

consider a sliding scale for civil penalties based on annual revenues (which nominally would correlate to the amount of consumer information the company handles) to ensure that civil penalties are an **effective deterrent** to noncompliance for all of the regulated entities.

The draft regulations contain no definition of the term "**dark patterns**," and the CPPA could clarify by providing statutory citation. One possible citation is in Cal. Civ. Code § 58.18(b)(4): *"Dark Pattern' means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice."*

A month ago during the previous public comment period a woman asked an important question that we would like to underline: what is the actual harm to consumers from companies who erroneously remove someone's information from their databases? The European model of consumer privacy protects the individual based on their expectation of privacy, rather than allow that expectation to differ wildly between industries. The CPPA's previous analyses within this European model of the relationship between individuals, their private data, and the companies who have created an industry around aggregating, analyzing, and commercializing those data should continue to follow this person-first trend. Data brokers will try to paint the risk of removing someone's data without properly verifying their identity as profound; it is not.

Thank you for your time and consideration of this matter-the data brokerage industry has not existed for very long at all, and the importance of ensuring people are treated with the dignity and respect we deserve as our behaviors themselves are commodified cannot be overstated. This is an important piece of legislation and an important rule making process that holds great promise for making Californians lives better.

Respectfully submitted,



Tracy Rosenberg  
Advocacy Director  
Oakland Privacy  
P.O. Box 3003  
Oakland CA 94609  
<https://oaklandprivacy.org>

with Saoirse Grace  
2024 Privacy Rights Fellow at Oakland Privacy

---

**From:** Craig Erickson [REDACTED]  
**Sent:** Tuesday, August 20, 2024 2:33 PM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on Data Broker Registration Regulations  
**Attachments:** Public Comment - Data Broker Registration.pdf; ADT Risk Assessment - Accenture.pdf

---

**This Message Is From an External Sender**

**WARNING:** This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

To the Agency:  
My public comment is attached for the public record.

I have also taken the liberty to test my recommendations by conducting Risk Assessments for the use of AI and Automated Decisionmaking Technologies on my personal vendors, and their suppliers, which includes all registered data broker listings prior to 7/1/2024. This risk assessment on *just one unregistered data broker* supports my recommendations, and will be disseminated to relevant stakeholders who can offer additional evidence in support of, or in contradicting claims made by this particular "high-risk processor".

I sincerely wish the Agency success between now and 2026 or 2028. My need as a California Consumer is immediate, therefore I have no time for filing complaints against companies who violate laws and suffer no consequences.

Craig Erickson, a California Consumer

To: regulations@coppa.ca.gov

Subject: "Public Comment on Data Broker Registration Regulations"

Date: August 19, 2024

My name is Craig Erickson, a California Consumer who voted for the CCPA and has participated in the rule-making process since 2019.

I exercise my privacy rights to gain transparency into the business practices of companies I have a relationship with and companies I might want to have a relationship with. The majority of these companies I call "my vendors" are using or planning to use AI for Automated Decisionmaking, aka "Automated Decisionmaking Technologies" (ADT).

One of the sets of processing activities the Agency (CPPA) included in its Draft Regulations on mandatory risk assessments is Access / Opt-out rights. Decisions about whether to fulfill or deny my CCPA Right to KNOW, CORRECT, LIMIT, DELETE, or OPT-OUT from the Sale or Sharing of my personal information are being made automatically using data sets from data brokers.

I use the Data Broker Registry for its intended purpose: to seek transparency about what personal information data brokers collect, process, and share with non-direct business entities. I try to achieve this by submitting KNOW requests to every data broker listing in the registry.

Based on data I've collected through this legal discovery process for consumers, I am disappointed to report that there is very little benefit to me personally and to taxpayers from privacy laws like the CCPA, the CPRA, and SB 362 aka "The Delete Act".

I am opposed to finalizing the proposed regulations for Data Broker Registration, because the majority of registered data brokers and the businesses using their data products and services state they are not obliged to comply with these laws.

Until the Agency convinces stakeholders it can enforce existing regulations effectively and fairly, the Agency is harming taxpayers and consumers by its lack of transparency regarding enforcement actions. Businesses are also harmed: those which do comply are at an unfair competitive disadvantage to non-compliant businesses. Without established case law on compliant and non-compliant practices, stakeholders are dependent upon lawyers, privacy technology companies, and other advisory firms which market themselves as experts or providers of CCPA-compliant solutions for guidance.

Although I oppose the proposed regulations on Data Broker Registration, SB 362 was passed into law, and the CPPA is obligated to finalize regulations for its authorized rulemaking activities.

Therefore I am making the following recommendations regarding the draft regulations, based on reports I have published and disseminated to academic researchers, policymakers, investors, employees, businesses, enforcement agencies, and professional associations that represent certified audit, cybersecurity, privacy, legal, and Responsible AI professionals. These reports and the data sets of evidence which supports them are available to the public at no cost.



## **Recommendation #1:**

**The Agency should not waste taxpayer funds trying to perfect formal rule-making activities of pending regulations without first enforcing final regulations on existing statutes.**

**Rationale:** It is difficult to enforce statutes and regulations which are poorly understood. With the commendable exception of ENFORCEMENT ADVISORY NO. 2024-01 issued April 2, 2024, the Agency has provided very little guidance to businesses or consumers on which specific business practices most likely violate the CCPA or other laws under its authority. This includes incentives for compliance, such as how to become compliant with these laws; and which issues businesses should focus their resources on, based on the Agency's enforcement priorities.

### **Relevant proposed rules:**

Recommendation #1 SUPPORTS **Anticipated Benefits of the Proposed Regulations:** The proposed regulations also facilitate increased compliance with CCPA... [which] advances the state's goal of transparency, supports the consumer's ability to make informed choices about their personal information, and provides the consumer with realistic expectations regarding the extent to which they can expect their personal information to be deleted.

Recommendation #1 CONTRADICTS **Determination of Inconsistency / Incompatibility with Existing State Regulations:** "The Agency has determined that these proposed regulations are not inconsistent or incompatible with existing state regulations. After conducting a review for any regulations that would relate to or affect this area, the Agency has concluded these are the only regulations that concern the data broker registration requirements of SB 362."

Recommendation #1 CONTRADICTS **CONSIDERATION OF ALTERNATIVES:** In accordance with Government Code section 11346.5 subdivision (a)(13), the Agency must determine that no reasonable alternative considered by the Agency or has otherwise been identified and brought to the attention of the Agency would be more effective in carrying out the purpose for which the action is proposed or would be as effective and less burdensome to affected private persons than the proposed action or would be more cost-effective to affected private persons and equally effective in implementing the statutory policy or other provision of law.

"The Agency has determined that the proposed regulations are the most effective way to operationalize the data broker registry requirement of SB 362 to balance the benefits to consumers, burdens to data brokers, and the purpose of the law itself."

Recommendation #1 CONTRADICTS **(2) The proposal would not benefit worker safety as the provisions do not pertain to, nor impact, worker safety:** Public officials, victims of domestic violence, and other individuals protected in Address Confidentiality and Safe-at-Home Programs often includes government employees and military personnel whose personal information is publicly-available and are at risk of leaking secret intelligence and losing their jobs, or worry about the safety of their loved ones.

## Recommendation #2:

**Data brokers who are EXEMPT from the CCPA should NOT be accepted in the Data Broker Registry.**

### Rationale:

The Agency does not tell consumers or businesses whether any particular company is covered under the CCPA, CPRA, or SB 362. Consumers who reasonably expect that every registered data broker is required to comply with the Agency's regulations should not expect the Agency to protect their rights when filing complaints against these companies.

As of July 1, 2024:

**22** registered data broker listings are outside the US, which is clearly outside the Agency's jurisdiction.

**At least one** registered data broker listing is a not-for-profit trade association, which "serves as a trusted advocate for the safe and secure growth of small businesses by providing a central repository for aggregating credit payment performance data".

**96** of registered data broker listings claim partial if not total exemption from the CCPA, using their own creative interpretations of the statutes, regulations, and guidance.

**79** of registered data broker listings only provide fabricated rights as substitutes for CCPA rights such as, "Opting out from targeted advertising" (**31**), "adding your name to a 'Suppression List' (**12**), and treating KNOW requests as requests to Delete and/or Opt-out (**36**).

Additionally, **144** registered data brokers have committed **at least 274** obvious violations of the CCPA which obstructs or discourages consumers from exercising their rights under the CCPA and SB 362.

Out of the **19** registered data brokers I call "Laggards", who waited until 30 days to 44+ days to respond to my CCPA Request to KNOW:

**4** asked questions I could not answer;

**3** redirected me to another endpoint to resubmit my request;

**2** sent acknowledgements yet provided no subsequent responses;

**1** demanded I verify my identity, **1** sent me a Frequently Asked Question, and **1** inappropriately said they deleted my data;

The vast majority, **9**, ultimately fulfilled my request claiming they had no data. This is a statistical outlier: out of all fulfilled access requests, (**50**) included my personal data, while (**60**) returned no data.

And what kind of company does this? When the Responders are ANONYMOUS (**9**), with the remainder (**10**) claiming to be from Privacy, Compliance, and DPO but are nameless -- unlike many compliant companies having 'responsible humans-in-the-loop' i.e. legal counsels and privacy professionals who identify themselves by name.

When the Agency took ownership of the data broker registration process in January 2024, data brokers reached out with questions about their registration requirements and expressed confusion due to a lack of clarity in the statute around undefined terms, common questions and occasional obstacles about SB

362's registration requirements, but did not mention similar concerns coming from California consumers or CCPA-covered entities conducting due diligence on third-party data providers.

My concern as a California consumer is that the Data Broker Registry is being used as a quasi-compliance certification condoning the data broker's data practices.

The Agency's definition of a "data broker" includes "high-risk processors" which intersects with qualification criteria for mandatory cybersecurity audits and ADT risk assessments. Rather than survey data brokers and allow them to self-report what, if any part of their business, is exempt from CCPA or SB 362, the Agency should establish a baseline by conducting a Privacy Threshold Assessment as part of the data broker registration process. This allows the Agency to do the minimum amount of discovery needed to identify the personal data processed and in particular, the identifiers used for searches and verification of identity, along with other metadata related to an entity's legal obligations.

*I use the CCPA Request to KNOW test, to positively identify which data brokers are covered entities under the CCPA, based on their fulfillment of my requests. **The CCPA Request to KNOW test is also the only legal method I know of, for verifying whether or not personal data was in fact deleted and/or limited from specific types of processing / sharing (opt-out); and the CCPA Request to Opt-in to the Sale or Sharing of my personal information is the only legal method I know of, for discovering the purpose for disclosing my personal information to third parties.***

I also used the Data Broker Registry listings as a basis for the metadata used to build profiles of these data brokers, supplemented with identifiers the Agency requested from them in its Accessible Deletion Mechanism 2024 Questionnaire to document the business' PII data inventory. This information is compatible with the *Privacy Threshold Assessment (PTA)* used by the Office of Information Security for determining if a Privacy Impact Assessment is required for California state agencies after consultation with the California Department of Technology which assesses the use of Generative AI.

Recommendation #3:

**The Data Broker Registry listings should be tested daily to evaluate whether it is effective in achieving its stated purpose, from the consumer's point-of-view.**

Rationale:

Many of the proposed rules referenced below abdicates the Agency's oversight of registered data brokers by disproportionately transferring responsibility to these data brokers to police themselves, such as:

- Requiring employee or agent for the data broker to register on behalf of the data broker and to have sufficient knowledge of their practices to provide accurate information under penalty of perjury. (Proposed § 7602 (b).)
- Preventing amendments or withdrawals to registration information after the registration period, subject to exceptions. (Proposed § 7602 (c).)
- Requiring true and correct responses be submitted by the data broker. (Proposed § 7603 (a).)
- Requiring accurate and functional website links and email addresses be provided to the Agency. (Proposed § 7603 (b).)
- Requiring disclosure of business's alternative names and requiring contact information to facilitate communication from the Agency as necessary. (Proposed § 7603.)
- Requiring disclosure of the types of personal information, products and services, and the proportion of data collected and sold that are subject to other laws. (Proposed § 7603 (d).)
- Allowing updates to certain types of registration information. (Proposed § 7604 (b).)
- Requiring that a data broker's disclosure of metrics must comply with section 7330, where applicable and technically feasible. (Proposed § 7605.)

The Agency should publish tests and tools that data brokers and consumers could use to determine compliance.

For example, in my *SB 362 DELETE ACT Compliance Report* published on July 1, 2024: only 143 of 495 data broker listings tested had published privacy policies dated later than 12/31/2023. The Federal Trade Commission disseminated an advisory to businesses regarding 'silent updates' of published privacy policies, yet many registered data brokers 'silently updated' their "CCPA Request Metrics" in this manner, which invalidates audits, investigations, and consumer complaints filed under penalty of perjury.

Recommendation #4:

**The schema, or data model for the Data Broker Registry listings should be refitted to support the complexity of data broker metadata.**

Rationale:

As it exists now, a comma-delimited flat file is insufficient for operationalizing the purpose of the law itself, for businesses conducting due diligence on their vendors registered as data brokers, as well as for consumers who want to know what personal information is used to make decisions that impact them.

Data brokers provide information and services to my personal vendors, helping them make automated decisions about which financial and employment opportunities I might be interested in, and whether or not my security and privacy rights are fulfilled.

I conduct risk assessments on my personal vendors' use of AI for making automated decisions (ADT), which requires establishing a baseline of their personal data inventory, and identifying vendors involved in processing this information – which includes registered data brokers who use AI to provide their data products and services.

The current data broker registry is not operationalized for consumers who want to use it to exercise their privacy rights. Aside from providing an email address for a designated contact, consumers need to know how to exercise their rights according to the data held and which instructions must be followed according to their applicable privacy policies. I do not use automated means to manage my privacy rights requests due to the complexity of resolving entities involved in the digital supply chain, and identifying which PI elements are used for each purpose, and relevant to the contextual relationship of each entity. In my risk assessments on the use of ADT I must rely on my own enriched data broker metadata model for managing my privacy rights requests.

I understand the Agency has its reasons for NOT considering the Accessible Delete Mechanism (“DROP”) for these proposed regulations. Maintaining an informational website that won't be needed for consumers who exercise their rights to delete and opt-out may waste of taxpayer funds. Perhaps the Agency is reconsidering whether the stated purposes of these proposed regulations for the Data Broker Registry are still valid when a 'one-stop' Accessible Deletion Mechanism exists.

Recommendation #5:

**There should be only one Data Broker Registry listing for each unique Privacy Policy governing CCPA and DELETE ACT rights rather than having multiple listings for the same data broker business entity or affiliate which shares a common Privacy Policy.**

Rationale:

**Recommendation #5 SUPPORTS: • Establish a rule requiring disclosure of business’s alternative names and requiring contact information to facilitate communication from the Agency as necessary. (Proposed § 7603.)**

When multiple companies reference the same privacy policy without disclosing the relationship between these entities, duplicative and contradictory privacy rights requests confuse consumers when responses come from unexpected companies or internet domains, and can invalidate their privacy rights requests in unanticipated ways. Therefore, although Recommendation #5 supports this draft proposal, it should strike “to facilitate communication with the Agency” in its Final Regulations submitted to OIS if its objective also includes providing transparency to consumers.

Recommendation #6:

**The Agency should protect its enforcement authority from being impeded by future litigation of disproportionate and unfair regulation of registered versus non-registered data brokers through greater transparent about its enforcement activities.**

Rationale:

The California Chamber of Commerce successfully delayed the Agency’s authority to enforce the CCPA for years, which harmed consumers and businesses that did comply with the CCPA. As a result, high-risk processors of personal information meeting the number of records threshold under the CCPA includes data brokers, authorized agents, and data privacy rights management portal platforms based within and outside the United States. Many of these high-risk processors either are exempt from the CCPA, are partially-exempt, make misleading claims about its exemption status, or imply they are compliant with a law they are exempted from. Some of these companies act in all three roles simultaneously or are orchestrated through affiliates which obscures conflicts of interest and/or deceptive business practices.

In 2020, I published the results of Experiment #2: the Data Broker Oracle I built as a model for using statistical learning techniques to predict classification status of businesses who should register or pay a \$200 per day fine. In 2023, I updated these results to evaluate the performance of my model which failed, according to the relatively small number of entries added during that period.

## Recommendation #7:

**The Agency should require every registered data broker and every non-registered data broker identified as service providers, contractors, and third parties to CCPA-covered entities to submit a mandatory cybersecurity assessment and risk assessment on its use of Automated Decisionmaking Technologies.**

## Rationale:

Many data brokers are using AI to process personal information currently and are on pace to become a majority before these regulations go into effect. While the industry is still 'wet behind the ears' in terms of technical assessments of AI-powered products and services, the Agency has a short window of opportunity now to collect baseline assessments of business practices, data and supplier inventories, data breaches, and histories of non-compliance with laws it has the authority and responsibility to enforce now.

In support of Recommendation #7, I am submitting a risk assessment to the Agency on behalf of Accenture, Inc. which has declined to answer any questions about its "Expanded Data & AI practice to offer new industry solutions and pre-built models that will help companies across 19 industries drive value" and the "more than 1,450 patents and pending patent applications worldwide and hundreds of client solutions at scale, ranging from marketing to retail and security to manufacturing" in which "Accenture has embedded AI across its service delivery approach".

Accenture is named as one of several companies the FTC is currently investigating for "Surveillance Pricing", even though I could not find any products or services Accenture offers to consumers. Accenture, which is described by the FTC as "an intermediary" is not registered as a data broker, and claims it has no obligation for reporting its metrics on privacy requests it processes. This is clearly a red flag for employees and prospective employees worried about being displaced by Accenture's "AI-Ready Workforce".

The Agency has admitted during its public hearing on finalizing its draft of mandatory risk assessments that it does not have the capacity to review all the abridged assessments it receives. Therefore, because I cannot rely on the Agency protecting my rights as a California Consumer, I am publishing my assessment so that policymakers, researchers, the public, and other interested stakeholders can determine the validity of my assessments, and possibly benefit from them.

## References:

[Enforcement Updates and Priorities](#), March 8, 2024, Michael S. Macko, Deputy Director, CPPA

[Enforcement Update and Priorities](#), July 16, 2024, Michael S. Macko, Deputy Director, CPPA

[Experiment #11: Activity Log](#), Craig S. Erickson, California Consumer

[Experiment #11: Complaint Log](#), Craig S. Erickson, California Consumer

[Experiment #12: Activity Log](#), Craig S. Erickson, California Consumer

[Experiment #12: Complaint Log](#), Craig S. Erickson, California Consumer

[SB 362 DELETE ACT Compliance Report - July 1 2024](#), Craig S. Erickson, California Consumer

[CCPA Regulations to NIST Privacy Framework and 800-53r5 Control Set Crosswalk](#), Craig Erickson, CIPT

[Everyone's Guide to the CCPA](#), Craig Erickson, CIPT

[Women In Security & Privacy \(WISP\) Privacy Red-Team – AI Risk Assessment](#), Craig Erickson, CIPT

[PTA / PIA SIMM 5310-C](#), State of California Department of Technology, Office of Information Security

[Generative Artificial Intelligence Risk Assessment SIMM 5305-F](#), State of California Department of Technology, Office of Information Security

[AI Risk Management Framework](#), NIST

[Accessible Deletion Mechanism 2024 Questionnaire](#), California Privacy Protection Agency

[Data Broker Delete Requests and Opt-Out Platform \(DROP\) Virtual Preliminary Stakeholder Session \(ca.gov\)](#)

[Draft Regulations on Mandatory Risk Assessments for ADT](#), California Privacy Protection Agency

[Experiment #2: Data Broker Oracle](#), Craig Erickson, CIPT

(The Risk Assessment I conducted on Accenture is only available to relevant stakeholders for additional input and verification purposes.)



## Privacy Threshold Assessment

The Office of Information Security SIMM 5310-C form is used by all California state agencies for conducting a Privacy Threshold Assessment (PTA). After consultation with the California Department of Technology, the PTA helps determine if a Privacy Impact Assessment (PIA) is required.

### Office of Information Security SIMM 5310-C

All California state agencies are required to conduct a PTA, and a PIA when certain criteria are met, which often depends upon the volume and type of personal information processed by the agencies.

No such equivalent criteria exists for which businesses are legally obligated to submit a risk assessment to the California Privacy Protection Agency. Businesses have the responsibility to self-classify their own legal obligations and submit the mandated risk assessment if the business' criteria is met.

Consumers have a right and a legitimate need to protect themselves from harm due to AI used for Automated Decisionmaking. Transparency is not only a key factor in assessing risk, it is a necessary prerequisite.

This risk assessment is intended for use by government agencies, businesses, consumers, regulators, and academic researchers.

This format was designed for compatability with PTA/PIAs for California state agencies, the CPPA's Draft Regulations for Mandatory Risk Assessments on the Use of AI for ADT, and TrustArc's Certification Program for Responsible AI.

When exercising my privacy rights as a California consumer, I conduct a Risk Assessment if:

- 1) The company claims it has or uses AI or has plans to build, acquire, use, or sell services or products (including information); and
- 2) The AI involves consumers in some way; and
- 3) The AI is used to make Automated Decisions about consumers in some way; and
- 4) The AI uses Personal information of consumers in some way; and
- 5) The company is legally obligated to comply with the CCPA and CPRA; and
- 6) The company meets the definition of a 'high-risk processor' of California Consumers' personal information; or
- 7) The company has violated the CCPA or other state and federal privacy-related laws.

Privacy Threshold Assessment			
<p>The California Privacy Protection Agency (CPPA, aka the "Agency"), uses its Formal Regulations to define legal requirements for businesses to submit a risk assessment on their use of Automated Decisionmaking Technologies (ADT), in which Automated Decisionmaking refers to the processing activity being assessed, and Artificial Intelligence (AI) is a technological component of the processing activity. These formal regulations have not been finalized, and the Agency has not published a standard format for businesses to submit. § 7150. When a Business Shall Conduct a Risk Assessment is the section that determines if a business is legally obligated to submit a Privacy Impact Assessment (PIA), aka "Risk Assessment" to the Agency. For the purpose of submitting my own risk assessments to the Agency, on behalf of businesses which have declined to answer questions about their use of AI, this questionnaire was designed using requirements from the draft rulemaking and formatted as a tool for evaluating risks of harm to consumers like me.</p>			
AI and Automated Decisionmaking Technologies (ADT) Risk Assessment Questionnaire			
Questions	Your Response to Consumers	Your Public Claims	How Other Entities Evaluate Your Business
I. Does your company use or plan to use Artificial Intelligence (AI) or Automated Decisionmaking Technologies (ADT) for any purpose?	Dear Craig Erickson, Thank you for writing to Accenture on October 10, 2023. In regards to your request, rest assured that Accenture processes personal information in	June 13, 2023 Accenture to Invest \$3 Billion in AI to Accelerate Clients' Reinvention	Accenture ai-RETAIL is listed as one of the Top 100 AI companies according to eWeek, prominently promotes its "Artificial Intelligence (AI) Services &amp; Solutions   Accenture" services on
II. Will your company's use of ADT data processing potentially present significant risk to consumers' privacy?	"If you choose to exercise your rights, we will not charge you different prices or provide different quality of services unless those differences are related to your personal information or otherwise permitted by law."	"We also know that numerous critical AI systems currently being used in industries like banking, insurance, healthcare, life sciences and many more will be affected. These systems will be classified as "high risk"	According to FTC Matter No. #P246202 RESOLUTION DIRECTING THE USE OF COMPULSORY PROCESS REGARDING SURVEILLANCE PRICING INVOLVING INTERMEDIARY
III. How did your company determine its use of ADT data processing potentially presents significant risk to consumers' privacy?	Perhaps Accenture responded to my KNOW request by 'Opting me out' because there is a significant risk to me, but offered me no explanation for this action. So I exercised my right to "Opt-in" to discover what I'm "Opting-in to"	The company's AI expertise spans more than 1,450 patents and pending patent applications worldwide and hundreds of client solutions at scale, ranging from marketing to retail and security to manufacturing.	According to <a href="https://insights.greym.com/accenture-patents/">https://insights.greym.com/accenture-patents/</a> , Accenture is blocking 7,061 patent applications. The majority of personal information collected on consumers according to
1. Did you determine your company's use of ADT presents significant risk to consumers' privacy based on how the business collects, uses, discloses, and retains personal information?	It is based on our Privacy Policy, and Binding Corporate Rules.	According to our published Privacy Statement and principles for Responsible AI, the answer can be found in our regular privacy reviews or by checking with the Chief A.I. Officer, Global Lead - Data and AI, or the	[no source found]
2. Did you determine your company's use of ADT presents significant risk based on categories of personal information to be processed, as disclosed in your Privacy Policy or	[declined]	6/2/2023	[no source found]
3. Does your company's use of ADT present significant risk to consumers' privacy when processing sensitive personal information?	[declined]	Accenture may collect certain types of sensitive information when permitted by local law or with your consent, such as health/medical information [including disability status], trade union membership	According to Accenture's statement regarding the ransomware data breach it suffered in 2021, "We have completed a thorough forensic review of documents on the attacked Accenture systems.
4. Is your company using or planning to use ADT for processing access / opt-out rights?	Dear Craig Erickson, Thank you for writing to Accenture on October 10, 2023. In regards to your request, rest assured that Accenture processes personal information in	"If you choose to exercise your rights, we will not charge you different prices or provide different quality of services unless those differences are related to your personal information or otherwise permitted by law."	According to Craig S. Erickson, a California Consumer who exercised his CCPA Right to Opt-In to the Sale of Personal Information, Accenture verified his identity and honored his request using a
5. Please approximate the number of consumers whose personal information your company plans to process during the next fiscal year.	[not requested]	With over 45,000 professionals dedicated to Data & AI, Accenture's Data & AI organization will double AI talent to 80,000 people through hiring, acquisitions and training: We are a talent and innovation led company	According to Accenture's Privacy Statement, the company has no Reporting Requirements for disclosing how many requests it receives, fulfills, and denies.

1. Project / Process / System / Program and Data / Information	
Questions	Answers
New Project Name:	CPPA - Mandatory AI and Automated Decisionmaking Technologies (ADT) Risk Assessment
Brief description of the project/process/system/program (if a project includes the system and business process(es) being developed within the scope of the project).	Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to: (B) Submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.
Data Classification: (Per SIMM 5305-A) * Check all that apply	X-Confidential X-Sensitive X-Public
Security Categorization: (NIST 800-53) (Per FIPS 199) *Select only one	X-High X-Moderate X-Low
Has a system security plan been completed for the project?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> X-No <input type="checkbox"/> N/A If No or N/A is selected, please explain why it is not completed and when it will be completed (e.g., before procurement). <b>The FTC's order against Accenture re: Surveillance Pricing does not include this requirement, and Accenture did not share one with me.</b>
Is there a Generative Artificial Intelligence (GenAI) component or byproduct to this project, regardless of whether it is intentional or incidental?	X-Yes <input type="checkbox"/> No If "YES," attach the completed mandatory GenAI Risk Assessment (SIMM 5305-F) and outcome of CDT consultation

1. Project / Process / System / Program and Data / Information			
Questions	Answers	Questions	Answers
6. Where is your company located?	<input checked="" type="checkbox"/> United States <input checked="" type="checkbox"/> International	12. How does your company process deletion requests from California consumers?	[ write your response here ]
7. Approximately how many employees does your company have?	<input type="checkbox"/> 1 - 10 <input type="checkbox"/> 10 - 100 <input type="checkbox"/> 100 - 1000 <input checked="" type="checkbox"/> 1000+	13. After processing a delete request for a California consumer, how does the company document that data was deleted in accordance with Cal. Civ. Code 1798.105(c)(2)?	[ write your response here ]
8. What is your company's gross annual revenue?	<input type="checkbox"/> \$0 - 100,000 <input type="checkbox"/> \$100,000 - \$1 million <input type="checkbox"/> \$1 million - \$5 million <input type="checkbox"/> \$5 million - \$25 million <input checked="" type="checkbox"/> \$25 million +	14. What APIs or other mechanisms does your company currently maintain for processing deletion requests from	[ write your response here ]
9. How many individual consumer records did you sell and / or share during the last calendar year?	<input type="checkbox"/> 0 - 100,000 <input checked="" type="checkbox"/> 100,000 - 10 million <input type="checkbox"/> 10 million - 100 million <input type="checkbox"/> 100 million - 500 million <input type="checkbox"/> 500 million +	15. Please identify all processing activities and personal data which the company or any of its subsidiaries claim is partially or completely exempt from the CCPA or CPRA or SB	[ write your response here ]
10. Approximately how many individual records of California consumers are maintained by your company?	<input type="checkbox"/> 0 - 100,000 <input type="checkbox"/> 100,000 - 250,000 <input type="checkbox"/> 250,000 - 1 million <input type="checkbox"/> 1 million - 10 million <input type="checkbox"/> 10 million - 20 million <input type="checkbox"/> 20 million+	16. Please specify all patents, certifications, and AI Registries where technical information can be used for assessments by external stakeholders.	[ write your response here ]
11. Which industries best represent your company's line of business? (specify SAIC codes on corporate filings for the company and all affiliated entities)	[ write your response here ]	17. Please specify any data breaches, legal settlements, or pending investigations by enforcement authorities pertaining to your company within the past calendar year.	1) "During the fourth quarter of fiscal 2021, we identified irregular activity in one of our environments, which included the extraction of proprietary information by a third party, some of which was made available to the public by the third party." Even though Accenture

Stakeholder Groups		
18. This section includes other stakeholders which may review this assessment and make comments.		
Group	Name	Comment
The business being assessed:	Accenture, Inc.	[ write your response here ]
"Recipient businesses":	[ write your response here ]	[ write your response here ]
Industry consortium:	[ write your response here ]	[ write your response here ]
Investors:	[ write your response here ]	[ write your response here ]
Experts:	[ write your response here ]	[ write your response here ]
Consumers:	[ write your response here ]	[ write your response here ]
The public:	[ write your response here ]	[ write your response here ]
Enforcement authorities:	[ write your response here ]	[ write your response here ]

AI and Automated Decisionmaking Technologies (ADT) Stakeholders				
19. For businesses consulting with external parties in its preparation or review of the risk assessment, please identify them by name and contact information, along with their role, responsibilities and qualifications:				
Name	Contact Information	Role	Responsibilities	Qualifications
[ write your response here ]	[ write your response here ]	example: How does the responsible human influence decisions on business use of ADT and its output(s)?	example: How does the responsible human evaluate the appropriateness of the personal information processed by, and the logic and output(s) of, the ADT for the company's proposed use(s)?	example: What qualifications does this responsible human have for understanding the business's use of the ADT, including the personal information processed by, the logic and output(s) of, the Technology?
[ write your response here ]	[ write your response here ]	[ write your response here ]	[ write your response here ]	[ write your response here ]
[ write your response here ]	[ write your response here ]	[ write your response here ]	[ write your response here ]	[ write your response here ]
20. Who is responsible for human involvement in your company's use of ADT for deciding if and how rights requests will be fulfilled?				
Name	Contact Information	Role	Responsibilities	Qualifications
[ write your response here ]	[ write your response here ]	example: How does the responsible human influence decisions on business use of ADT and its output(s)?	example: How does the responsible human evaluate the appropriateness of the personal information processed by, and the logic and output(s) of, the ADT for the company's proposed use(s)?	example: What qualifications does this responsible human have for understanding the business's use of the ADT, including the personal information processed by, the logic and output(s) of, the Technology?
[ write your response here ]	[ write your response here ]	[ write your response here ]	[ write your response here ]	[ write your response here ]
[ write your response here ]	[ write your response here ]	[ write your response here ]	[ write your response here ]	[ write your response here ]

2. Project Contact Information	
Project Manager	Fillable Information
Name	Craig Erickson, CIPT
Title	Data Protection Officer
Contact Number	[REDACTED]
E-mail Address	[REDACTED]
Organization Unit/Office	PrivacyPortfolio / Authorized Agent
Data Owner	Fillable Information
Name	Craig Erickson
Title	Data Custodian
Contact Number	[REDACTED]
E-mail Address	[REDACTED]
Organization Unit/Office	California Consumer
Business Process Owner	Fillable Information
Name	Senthil Ramani
Title	Global Lead - Data and AI
Contact Number	[REDACTED]
E-mail Address	[REDACTED]
Organization Unit/Office	Global Lead - Data and AI
IT Manager/Data Custodian	Fillable Information
Name	Kris Timmermans
Title	IT Manager
Contact Number	[REDACTED]
E-mail Address	[REDACTED]
Organization Unit/Office	[REDACTED]
Privacy Officer/Manager	Fillable Information
Name	Lan Guan
Title	Chief A.I. Officer
Contact Number	[REDACTED]
E-mail Address	[REDACTED]
Organization Unit/Office	[not known]

21. Privacy Threshold / Impact Assessment Authorization and Acceptance	
I have reviewed this assessment and resolved any inaccuracies and / or omissions:	
Privacy Threshold Assessment	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Privacy Impact Assessment	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Print Name	Craig Erickson, CIPT, dba PrivacyPortfolio, authorized agent for Craig S. Erickson
Signature Name	Craig Erickson, CIPT (digital signature)
Signature Date	8/19/2024
I have reviewed this assessment and resolved any inaccuracies and / or omissions:	
Privacy Threshold Assessment	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Privacy Impact Assessment	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Print Name	Craig S. Erickson
Signature Name	Craig S. Erickson (digital signature)
Signature Date	8/19/2024
I have reviewed this assessment and resolved any inaccuracies and / or omissions:	
Privacy Threshold Assessment	<input type="checkbox"/> Yes <input type="checkbox"/> No
Privacy Impact Assessment	<input type="checkbox"/> Yes <input type="checkbox"/> No
Print Name	
Signature Name	
Signature Date	
I have reviewed this assessment and resolved any inaccuracies and / or omissions:	
Privacy Threshold Assessment	<input type="checkbox"/> Yes <input type="checkbox"/> No
Privacy Impact Assessment	<input type="checkbox"/> Yes <input type="checkbox"/> No
Print Name	
Signature Name	
Signature Date	
I have reviewed this assessment and resolved any inaccuracies and / or omissions:	
Privacy Threshold Assessment	<input type="checkbox"/> Yes <input type="checkbox"/> No
Privacy Impact Assessment	<input type="checkbox"/> Yes <input type="checkbox"/> No
Print Name	
Signature Name	
Signature Date	

Data Inventory			Accessible Deletion Mechanism Questionnaire 2024	
<p>Office of Information Security SIMM 5310-C</p> <p>The CPPA Risk Assessment for Automated Decisionmaking Technologies lacks a Data Inventory.</p> <p>The Accessible Deletion Mechanism Questionnaire 2024, sent out to all registered data brokers does include specific personal data elements which correspond to this data inventory.</p>			<p>Beginning August 1, 2026, registered data brokers must access the accessible deletion mechanism at least once every 45 days and process all deletion requests, subject to limited exceptions. The accessible deletion mechanism allows a consumer, through a single verifiable request, to request that every data broker that maintains any personal information delete any personal information related to that consumer held by the data broker or associated service provider or contractor.</p>	
<p>Will the system collect, use, maintain, or share any of the following types of personally identifiable information as it relates to an individual?</p>	Yes	No	<p>22. Which specific pieces of personal information do you collect? [select all that apply]</p>	Your response
Name, Former Name, or Alias	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full name	YES
Date of Birth	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Birthdate	YES
Social Security Number (SSN)	<input type="checkbox"/>	<input type="checkbox"/>	SSN	[no response]
Truncated SSN	<input type="checkbox"/>	<input type="checkbox"/>	[not requested]	[no response required]
Driver's License Number or State Identification Card Number	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Driver's license / Passport	YES
Financial Data (e.g., account number, credit/debit card numbers, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	[not requested]	[no response required]
Health Insurance Information (e.g., including policy number, subscriber identifier, medical ID, or any information in an individual's application or claims history, including appeals records, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	[not requested]	[no response required]
Medical Information (e.g., medical history, mental and physical condition, or medical treatment or diagnosis, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	[not requested]	[no response required]
Username/ID, email address, password, or security question and answer	<input type="checkbox"/>	<input type="checkbox"/>	Email	YES
Physical Description (including height, weight, etc., please specify) Specify: [specify here]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	[not requested]	[no response required]
Biometric Data (e.g., fingerprints, iris scans, DNA, photographic facial images, etc.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Fingerprint / Faceprint	YES

Employment History	<input checked="" type="checkbox"/>	<input type="checkbox"/>	[not requested]	[no response required]
Education History	<input checked="" type="checkbox"/>	<input type="checkbox"/>	[not requested]	[no response required]
Criminal History	<input type="checkbox"/>	<input type="checkbox"/>	[not requested]	[no response required]
Information or data collected through the use or operation of the automated license plate recognition system.	<input type="checkbox"/>	<input type="checkbox"/>	[not requested]	[no response required]
Genetic Data	<input type="checkbox"/>	<input type="checkbox"/>	[not requested]	[no response required]
Other personal information (e.g., home address, email address, mother's maiden name, home phone number, personal cell phone number, place of birth, etc.). Specify [specify here]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Phone	YES
[not requested]	<input type="checkbox"/>	<input type="checkbox"/>	Another data broker's proprietary identification number	[no response]

( The PIA also has a Risk Assessment Questionnaire based on Draft Regulations from the CPPA, which correspond to questions on the SIMM 5310-C form used by California State Agencies.)

<b>4. Privacy Impact Assessment</b>		
<p>The Privacy Impact Assessment will consist of questions in six sections: Privacy Program Administration, Collection, Use, Maintenance and Storage, Disclose / Share, and Destruction/Disposal. Each section includes questions to be completed. At the end of each section, an analysis related to that section will identify and address privacy risks, mitigations, and, if necessary, a correction plan. Multiple privacy risks may be identified in each section; each of these risks must be identified and documented.</p>		
<b>4.1 Privacy Program Administration</b>		
<b>1. Project/Process/System/Program and Data/Information</b>		
<b>No.</b>	<b>Questions</b>	<b>Responses</b>
4.1.1	Does the organization document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection,	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
	<i>[not requested]</i>	<i>[no response required]</i>
	<i>[not requested]</i>	<i>[no response required]</i>
	<i>[not requested]</i>	<i>[no response required]</i>
4.1.2	Will contractors or service providers have access to PII?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No If "NO," skip to question #4.1.5
4.1.3	Describe the privacy roles, responsibilities, and access requirements for contractors and service providers.	[no information available]
4.1.4	Are the privacy and GenAI disclosure notification requirements included in contracts and other acquisition related documents?	<input type="checkbox"/> Yes <input type="checkbox"/> No
	<i>[not requested]</i>	<i>[no response required]</i>

4.15	Describe how individuals who have access to PII are trained to handle the PII appropriately.	<b>[Generative AI and LLM Center of Excellence and YouTube videos]</b>
4.16	Describe what controls are in place to ensure system users have completed training relevant to the project or program. Tip: Each project or program may offer training specific to the project or program, including GenAI, which touches on information handling procedures and the sensitivity of information.	[no information available]
4.17	Does your organization issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information?	<b>X Yes</b> <input type="checkbox"/> No If "YES," describe: <b>Accenture provides this guidance for its customers.</b>
4.18	Does the organization provide a means for individuals to authorize collection, use, maintenance, and sharing of PII prior to its collection?	Collection: <b>X Yes</b> <input type="checkbox"/> No Use: <b>X Yes</b> <input type="checkbox"/> No Maintenance: <b>X Yes</b> <input type="checkbox"/> No Sharing: <b>X Yes</b> <input type="checkbox"/> No If "YES," describe all applicable means: <b>[Consumers may contact our Data Privacy Officer if they have a general question about how Accenture protects your personal information.]</b>
4.18	Does the organization provide a means for individuals to authorize collection, use, maintenance, and sharing of PII prior to its collection?	Collection: <b>X Yes</b> <input type="checkbox"/> No Use: <b>X Yes</b> <input type="checkbox"/> No Maintenance: <b>X Yes</b> <input type="checkbox"/> No Sharing: <b>X Yes</b> <input type="checkbox"/> No If "YES," describe all applicable means: <b>[Consumers may contact our Data Privacy Officer if they have a general question about how Accenture protects your personal information.]</b>
4.19	Describe any procedures your organization has in place that allow an individual access to information collected by the project / process / system / program and/or to an accounting of disclosures of that information.	<b>[Contact us first if you wish to make a complaint about Accenture's use of your data.]</b>



4.1.10	Describe the procedures for individuals to address possibly inaccurate or erroneous information. Tip: If the correction procedures are the same as those given in question above, state as much. If the system has been exempted from the provisions of the IPA, explain why individuals may not access their records.	<b>If you would like to exercise your erasure, rectification, or access rights in reference to your data as a job applicant, you may also click here. Any other rights can be exercised by contacting us.</b>
4.1.11	Does your company require notice to affected individuals when their personal information is requested, sold, or released to third parties?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If "NO," explain: <b>[This notice is not required when a consumer exercises the right to 'Opt back in to the sale of my personal information']</b>
4.1.12	Are the company privacy practices publicly available through the organizational website?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No If "NO," explain: [insert response here]
4.1.13	Is the privacy incident response plan incorporated into your entity's Incident Response Plan?	<input type="checkbox"/> Yes <input type="checkbox"/> No If "NO," explain why not; if "YES," describe where it is located.
4.1.14	Does your organization's online privacy notice or statement to the public and individuals include the following: a) Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII) b) Authority for collecting PII c) The choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices d) The ability to access and have PII amended or corrected if necessary	a) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No b) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No c) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No d) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
	<i>[not requested]</i>	<i>[no response required]</i>
4.1.15	Does the organization evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized?	<input type="checkbox"/> Yes <input type="checkbox"/> No If "YES," provide a brief description: [no information available]
4.1.16	Does the privacy notice provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Provide copies of the applicable privacy notices.
4.1.17	Analysis: Related to Privacy Program Administration This portion of the PIA is for details about information provided in this Privacy Program Administration section. Identify privacy risks, mitigation strategies and, if necessary, provide a corrective action plan.	Privacy Risk: <b>[No audit trail for Sharing PI with third parties;]</b> Mitigation: <b>[Implement AC-20: Use of External Systems to monitor and govern sharing through access controls;]</b> Corrective Action Plan: <b>[Require password-protected accounts for third parties Accenture shares PI with;]</b>

#### 4.2 Collection

The following section pertains to the collection of personally identifiable information by the company.

No.	Questions	Responses
4.2.1	List all statutory and regulatory authority to collect the personally identifiable information (PII) listed in the Privacy Threshold Assessment. Tip: Explain how the statutory and regulatory authority permits the collection, use, maintenance, and sharing of the information. A simple citation without more information will not be sufficient for the purposes of this document and will result in the rejection of this Privacy Impact Assessment. You must explain how the statutory and regulatory authority permits the collection of the subject information.	<b>[“Accenture processes personal information in accordance with our Privacy Statement, all obligations in our Binding Corporate Rules, and applicable state and federal laws.”]</b>
4.2.2	Does the system collect Social Security Numbers?	<b>X</b> Yes <input type="checkbox"/> No If “YES,” identify the specific authority allowing such collection. If you are relying on another federal or state agency, list their legal authorities. <b>[All employers collect social security numbers on employees and contractors]</b>
4.2.3	Is PII received from another governmental agency or entity under an agreement?	<b>X</b> Yes <input type="checkbox"/> No If “YES,” cite the agreement and where it can be found. <b>[Accenture provides a wide range of services to the US federal government through its subsidiary, Accenture Federal Services. They work with various federal agencies, including those in national security, defense, public safety, civilian, and military health sectors. Their services include cloud computing, data and AI, cybersecurity, human capital management, and more. <a href="https://www.accenture.com/us-en/support/us-federal-government/3pao">https://www.accenture.com/us-en/support/us-federal-government/3pao</a>]</b>

4.2.4	Describe the purpose(s) for which PII is collected, used, and maintained.	<b>[For the business purpose of serving our customers]</b>
	<i>[not requested]</i>	<i>[no response required]</i>
4.2.5	Is the above purpose also stated in your 'notice on collection'?	<b>X Yes</b> <input type="checkbox"/> No Tip: 'Notice on collection' means clearly communicating to individuals the purpose of collecting their personal information.
4.2.6	Is the reason information is being collected displayed in clear, simple language that can be easily understood by the data subject?	<input type="checkbox"/> Yes <b>X No</b>
4.2.7	a) Does this project / process / system / program collect PII directly from the individual to the greatest extent possible?  b) Identify the sources from which the information may be collected.	a) <input type="checkbox"/> Yes <b>X No</b> ; b) <b>X Individuals</b> <b>X Another Entity</b> <b>X Business Partner/Vendors</b> <b>X Internally – please describe:</b> <b>[Avanade gets PII from the Workday third party job portal, which is a shared resource of Accenture and Avanade, an undisclosed partner or subsidiary of Accenture.]</b>
4.2.8	Will the system ingest or output information, such as images, videos, audio clips, or text that has been significantly altered or generated by algorithms, including by AI, known as "synthetic data"?	<b>X Yes</b> <input type="checkbox"/> No
4.2.9	Is there a probability that the synthetic data will impact information integrity, increase fraud, or cause intellectual property and/or copyright issues?	<b>X Yes</b> <input type="checkbox"/> No If "YES, please describe how: <b>[Accenture is in the business of transforming companies through Responsible AI, which necessitates rigorous system testing for bias and inaccuracies, while also ensuring that unauthorized / non-consensual Personal Information and Intellectual Property are not used.]</b>

4.2.10	Will the data output be reviewed/audited by an individual/team to mitigate against hallucinations and bias to ensure that data outputs are accurate and factual?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If "NO," describe here and document it as a risk. Provide a mitigation plan in the Analysis: Collection section. <b>[The company's AI expertise spans more than 1,450 patents and pending patent applications worldwide and hundreds of client solutions at scale, ranging from marketing to retail and security to manufacturing. Accenture has embedded AI across its service delivery approach, driving efficiency, insights, and accelerating value for thousands of clients through its market leading platforms such as myWizard, SynOps, and MyNav. Six years ago, Accenture pioneered its responsible AI framework, which is now part of how Accenture delivers its work for clients, is included in the company's code of ethics and underlies its rigorous responsible AI compliance program. Accenture is currently working with many clients on generative AI projects, such as helping a hotel group manage customer queries or a judicial system synthesize judicial process information across hundreds of thousands of complex documents.]</b>
4.2.11	How will PII be collected? Select all applicable items:	<input type="checkbox"/> Paper <input checked="" type="checkbox"/> Electronically <input type="checkbox"/> Verbally <input checked="" type="checkbox"/> Other - please specify: <b>[publicly available sources (registers or the internet), Accenture employees, contractors, (prospective) members of board of directors, shareholders, Accenture's affiliates, subsidiaries and newly acquired businesses, employers of our contractors, our clients, public authorities, public websites and social media, previous employers, educational institutions, suppliers and vendors (including third party data providers); What are the sources of marketing data?</b> <b>The bulk of the personal information we collect and use for marketing purposes relates to individual employees of our clients and other companies with which we have an existing business relationship. We may also obtain contact information from public sources, including content made public at social media websites, to make an initial contact with a relevant individual at a client or other company;]</b>

4.2.12	<p>Are Social Security Numbers extracted from any other source?  Tip: For example, is an SSN match made and extracted via other information provided by the claimant, employer, or provider, or verified with SSA, etc.?</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No If "YES", describe the source: [no information available]
4.2.13	<p>a) Does the system or manual process use information from commercial sources, including GenAI or publicly available data?   b) If GenAI data is used, answer the following questions:  What data sets are being pulled, and where are they pulled from?   c) Why is the data set being pulled, and what is it used for?   d) How will you ensure that publicly available data, in combination with other data, does not create/output PII data?  Tip: Example: The commercial data is used as a primary source of information regarding the individual. Alternatively, commercial data is used to verify information already provided by or about the individual.</p>	<p>a) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No  If "YES," explain why and how this information is used. Indicate whether the commercial or public source data is marked within the system.  <b>[There are too many AI-powered services, applications, and patents to respond within this format.]</b>   b) <b>[The majority of references generated by Microsoft Copilot are sourced from Accenture's website.]</b>   c) <b>[All personal data is used for business purposes disclosed in our privacy statement.]</b>   d) <b>[All personal data is used for business purposes disclosed in our privacy statement.]</b></p>
	<i>[not requested]</i>	<i>[no response required]</i>
4.2.14	<p>Does the system receive or send data to another system or third party outside of the organization?  Tip: For example, is data received through an application programming interface (API) or other data transfer protocols, e.g., a response to a background check?</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No  If "YES," describe the system, entity, and data sharing agreement, including what information is used and how it is used.  System Name: <b>[Avanade Recruitment]</b>  Data elements: <b>[name, email]</b>  How the information is used: <b>[to send unsolicited recruitment pitches]</b>  Name of the entity: <b>[Avanade]</b>  Original source or data owner of the data: <b>[Craig S. Erickson, a California Consumer]</b></p>

	<i>[not requested]</i>	<i>[no response required]</i>
	<i>[not requested]</i>	<i>[no response required]</i>
	<i>[not requested]</i>	<i>[no response required]</i>
	<i>[not requested]</i>	<i>[no response required]</i>
4.2.15	Does the organization identify the minimum PII elements required by the information system or activity to accomplish the legally authorized purpose of collection?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
4.2.16	<p><b>Analysis: Related to Collection</b></p> <p>This portion of the PIA is to provide details about information related to PII collection. Identify privacy risks, including GenAI risks, mitigation, and, if necessary, provide a corrective action plan.</p>	<p><u>Privacy Risk:</u>  <b>[With more than 1,450 AI patents and pending AI patent applications worldwide and hundreds of client solutions at scale, anything less than disclosing to the public a complete and current registry of all Accenture AI-powered solutions represents a significant risk to consumers with no direct relationship to Accenture and to employees of Accenture clients who are listed as sources of PI in Accenture's Privacy Statement.]</b></p> <p><u>Mitigation:</u>  <b>[Submit to the CPPA a complete and current registry of all Accenture AI-powered solutions and patents];  [Implement PT-2: Authority to Process Personally Identifiable Information; PT-3: Personally Identifiable Information Processing Purposes, PT-5: Privacy Notice]</b></p> <p><u>Corrective Action Plan:</u>  <b>[to be determined by the CPPA]</b></p>

**4.3 Use**

The following information relates to how the use of personally identifiable information is controlled and managed within the company.

No.	Questions	Responses
4.3.1	Who is authorized to receive and have access to the PII within the project/system? Tip: Describe the different roles in general terms that have been created to provide access to the information. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.	<b>Accenture does not identify specific individuals and the permissions they have to access PII, which includes all staff who process privacy rights requests.</b>
4.3.2	Is the use of the PII collected limited to the stated purpose for which the individual has provided consent?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> <b>No</b> If "NO," please provide further information. <b>[When I registered my online account at Workday, and before I applied for a job with Accenture, I received a recruitment email from Avanade saying I was a good fit for them. I did not consent to sharing my PI with Avanade, but I did opt-in to the Sale of my PI prior to creating an online account at Workday.]</b>
4.3.3	Will PII be used in testing, training, and or research?	<input checked="" type="checkbox"/> <b>Yes</b> <input type="checkbox"/> No If "Yes," please describe: <b>[When I opted in to the sale of my PI at Accenture, there was no disclosure regarding use of my PI, or the option to restrict use, so my reasonable expectation is Accenture can do what it wants. Data, tools, and talent are the main products of Accenture and I suspect that both my data and my intellectual property is used to test, train, or research AI when applying for patents or providing automated decisions for its clients.]</b> If "NO," go to 4.3.6.

4.3.4	Are there policies and/or procedures to minimize the use of PII in testing, training, GenAI training models and/or research?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No If "YES," describe and provide the name and location of the policies/procedures: <b>[I assume so because Accenture advises businesses worldwide about Responsible AI, but I cannot find any and must rely on "Forward-looking Statements" in Accenture's marketing content.]</b>
4.3.5	If PII is used in testing, training, GenAI training models, or research, what controls will be implemented to protect PII from unauthorized use and disclosure?	<b>["Accenture processes personal information in accordance with our Privacy Statement, all obligations in our Binding Corporate Rules, and applicable state and federal laws."]</b>
4.3.6	Is the use of PII internally only for the authorized purpose(s) identified in the privacy policy or notice on the collection?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
4.3.7	Can other entities (including contractors or service providers) access the data in this system?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No If "YES," What laws or regulations authorize access? <b>[All applicable state and federal laws]</b>
4.3.8	<p>a) Describe how you ensure that only the employees authorized to access the PII data have access to it.</p> <p>b) Describe how the organization will monitor and audit privacy controls for this project / process / system.</p> <p>c) Do the audit measures discussed above include the ability to identify specific records each user can access?</p> <p>d) Describe the different roles that have been created to provide access to the project information. Use general terms.          Tip: Certain users may have "read-only" access, while others may be permitted to make certain amendments or changes to the information.          Example: If certain celebrity records are accessed, a supervisor is notified and reviews to ensure that the records were properly used.</p>	<p>a) <b>[By relying on AI service accounts, subsidiaries, partners, vendors and customers to access the PII instead of using Accenture employees to access it.]</b></p> <p>b) <b>[By reviewing consumer complaints filed with relevant enforcement agencies and investigation findings by enforcement agencies.]</b></p> <p>c) <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No          If "NO," explain why:  <b>[AI services run on machine-accounts which are not auditable or accessible, and in LLM there is no such thing as specific records in a searchable format. ]</b></p> <p>d) <b>[Some tools such as ChatGPT have no such controls we can configure for our users.]</b></p>



4.3.9	Does the project have human verification on GenAI outputs and perform self-audits or third-party audits and/or reviews by other entities?	<b>X Yes</b> <input type="checkbox"/> No <input type="checkbox"/> N/A If "NO," explain why [insert response here]
	<i>[not requested]</i>	<i>[no response required]</i>
	<i>[not requested]</i>	<i>[no response required]</i>
	<i>[not requested]</i>	<i>[no response required]</i>
	<i>[not requested]</i>	<i>[no response required]</i>
4.3.10	<p><b>Analysis: Related to Use</b></p> <p>This portion of the PIA is to provide details about information related to PII use. Identify privacy risks including GenAI risks, mitigation strategies and, if necessary, provide a corrective action plan.</p>	<p><u>Privacy Risk:</u>  <b>[Misrepresentation of CCPA Regulations by businesses harm consumers who lack access to legal guidance and resources.]</b></p> <p><u>Mitigation:</u>  <b>[Implement AT-3: Role-based Training;]</b></p> <p><u>Corrective Action Plan:</u>  <b>[The CPPA should audit training records and ensure that training content includes alleged violations of CCPA Regulations.]</b></p>

**4.4 Maintenance and Storage**

Please describe below how the business controls the maintenance and storage of personally identifiable information.

No.	Questions and Fillable Answers	Responses
4.4.1	Where will PII be stored? Select all applicable items:	<p><b>X Cloud</b>  <b>X Local Drive</b>  <b>X Shared Drive</b>  <b>X System/Database (including GenAI Training model)</b>  <b>X Third-Party storage</b>  <b>[Too many vendors to list in this format]</b>  <input type="checkbox"/> Physical paper filed                      [specify location here]</p>
4.4.2	Explain how the project checks for and corrects, as necessary, any inaccurate or outdated PII used by its programs or systems. How often? Tip: For example, the project or program does not utilize the inaccurate or outdated PII. It merely identifies to the state entity that it is visible when it should not be visible since it should be encrypted.	<b>[no information available]</b>
	<i>[not requested]</i>	<i>[no response required]</i>
4.4.3	Describe the process used for checking accuracy. If a commercial data aggregator is involved, describe the levels of accuracy required by the contract. Tip: Sometimes, information is assumed to be accurate, or in Research & Development, inaccurate information may not impact the individual or the system. If the system or program does not check for accuracy, including reviewing/auditing GenAI outputs, please explain why.	<b>[When we fulfill a consumer's request to KNOW and a request to CORRECT or check publicly-available records to verify information provided by the individual. ]</b>

	<i>[not requested]</i>	<i>[no response required]</i>
	<i>[not requested]</i>	<i>[no response required]</i>
	<i>[not requested]</i>	<i>[no response required]</i>
4.4.4	Describe any technical solutions, policies, or procedures focused on improving personally identifiable information accuracy and integrity within the system/project/process or program. Tip: Example: The system may check the information provided by the individual against any other source of information (within or outside your organization) before the project uses the information to make a decision about an individual.	<b>[no information available]</b>
4.4.5	How long will the information be stored? Tip: Example: The project manager, in consultation with the legal counsel and the component records management officer, must develop a records retention schedule early in the development process for the records contained in the system that considers the minimum amount of time necessary to retain information while meeting the program's needs. Consult with your records management office for assistance with this question if necessary.	<b>[no information available]</b>
4.4.6	Is all the information the project / process / system / program collects retained?	<b>X</b> Yes <input type="checkbox"/> No If "YES," Is there a specific subset of information retained? <b>X</b> Yes <input type="checkbox"/> No If "YES," describe: <b>[Accenture requires consumers exercising their right to KNOW and CORRECT to submit a copy of a Driver's License or Government-issued Identification Card and promises to delete it IMMEDIATELY.]</b>

4.4.7	Is there an automated purge process built into this system/program for all data housed within the system/program?	<input type="checkbox"/> Yes <input type="checkbox"/> No Provide the Business Use Case, which outlines the purge criteria. [no information available]
4.4.8	Are there any data elements within this system/program that do not adhere to an automated purge process?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No If "YES," is there an active data retention variance for this data? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Consider the following to assist in providing a response: • Does the project retain only the PII necessary for its purpose and only for as long as necessary and relevant to fulfill the specified purposes? • Has the PIA described policies and procedures for purging PII that is no longer relevant and necessary? <b>[Our system for verifying a consumer's identity asks consumers to redact some data elements from their government-issued id, which cannot be purged. The retention period is IMMEDIATELY which probably does not appear in the PIA or in any retention policy.]</b>
4.4.9	Can the synthetic data be tracked and audited for integrity and non-reputability?	<input type="checkbox"/> Yes <input type="checkbox"/> No If "YES," please describe how: <b>[no information available]</b>
4.4.10	Is there a mechanism to ensure consumers are notified when speaking to Artificial Intelligence and can opt out if they choose to do so?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
4.4.11	<b>Analysis: Related to Maintenance and Storage</b> This portion of the PIA is to provide details about information related to PII maintenance and storage. Identify privacy risks, mitigation strategies and, if necessary, provide a corrective action plan. Tip: Discuss the risks associated with the length of time personally identifiable information is maintained and stored. How were those risks mitigated? The proposed schedule should keep the minimum amount of PII for the minimum amount of time. The schedule should align with the stated purpose and mission of the system.	<u>Privacy Risk:</u> <b>[Consumers cannot exercise their Right to CORRECT when they are denied their Right to KNOW, and enforcement authorities cannot validate consumer complaints unless they request the inaccurate or missing personal information directly from consumers.]</b> <u>Mitigation:</u> <b>[Implement PM-22: Personally Identifiable Information Quality Management; ]</b> <u>Corrective Action Plan:</u> <b>[The CPPA should audit all Requests to Opt-In After Opting-out of the Sale or Sharing of Personal Information to discover and notify consumers exactly what processing activities are "high-risk".]</b>

#### 4.5 Disclose/Share

In the following section, describe whether the business discloses or shares the personally identifiable information under its purview with other entities.

No.	Questions and Fillable Answers	Responses
4.5.1	Does the project maintain an accurate accounting/record of disclosure of information held in the system?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> <b>No</b> Who is responsible for the accounting of disclosures? Title: <b>[Chief Responsible AI Officer]</b> Name: <b>[Arnab Chakraborty]</b>
4.5.2	What is the retention period for the accounting/record of disclosure of PII mentioned above?	<b>[for as long as necessary]</b>
	<i>[not requested]</i>	<i>[no response required]</i>
4.5.3	Is the disclosure of the PII collected limited to the stated purpose and for which the individual has provided consent?	<input type="checkbox"/> Yes <input type="checkbox"/> No If "NO," describe: [describe here]
4.5.4	Discuss information sharing between departments, subsidiaries and/or affiliates, and third party entities. • Identify and list the entities with which the information is shared. • What laws or statutes authorize disclosure? Tip: For example, certain systems regularly share information because of the crossover of the different parts of the state.	<b>[Our Binding Corporate Rules and all applicable state and federal laws.]</b>
4.5.5	The following questions are intended to describe the scope of the project / system / process / program information sharing external to the entity. External sharing encompasses sharing with separate business entities not disclosed in, and not sharing the same privacy policy. Is information shared externally as part of normal business operations?	<input checked="" type="checkbox"/> <b>Yes</b> <input type="checkbox"/> No If "YES," identify the external entities, how the information is accessed, and how it is to be used. <b>[Accenture does not divulge trade secrets or provide a list of customers. ]</b>

4.5.6	Does the project share PII with parties external to the company only for the authorized purposes identified in the privacy policy or notice on collection?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> <b>No</b> If "NO", explain. <b>[The purpose of Opting in to the Sale / Sharing of Personal Information is to sell or share it with anyone we want. Haven't seen a privacy notice saying our company monetizes your personal information as a revenue source or in consideration of something else of value to the company.]</b>
4.5.7	<p>a) If the organization shares PII collected within this project / system / process / program with external entities, describe how that sharing occurs:</p> <p>b) Are Memoranda of Understanding, Inter-Agency Agreement, Letters of Intent, or similar agreements executed?</p> <p>c) Is the PII specifically identified?</p> <p>d) Are the purposes for which it will be used detailed?</p> <p>e) Does the agreement (in whatever form) detail the responsibilities of the third parties to protect and secure the PII?</p> <p>f) Does the agreement require formal acknowledgment (i.e., the signature of authority, etc.)?</p> <p>g) Is the data captured for this system or the output of this system being used to train another AI model?</p>	<p>a) <b>[Someone applies for a job at Accenture and they are contacted by Avanade instead.]</b></p> <p>b) <input type="checkbox"/> Yes <input type="checkbox"/> No If "YES," provide a copy.</p> <p>c) <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>d) <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>e) <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>f) <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>g) <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If the response is "YES" to any of the above, describe: [insert response here]</p> <p>If the response is "No" to any of the above and data is being shared/exchanged, explain how this risk is mitigated in the analysis section.</p>
4.5.8	What is the process for the discovery of data subject to PII disclosure?	[no information available]
4.5.9	Will any of the following techniques be implemented to directly disclose how AI was used in the content creation?	Select all applicable items: <input type="checkbox"/> Content labels <input type="checkbox"/> Visible watermarks <input type="checkbox"/> Disclosures fields <input checked="" type="checkbox"/> <b>Other</b> - please specify: <b>[no information available]</b>

4.5.10	<p>Will any of the following techniques be implemented to indirectly disclose how AI was used in the content creation?</p>	<p>Select all applicable items:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Covert watermarks</li> <li><input type="checkbox"/> Digital fingerprints</li> <li><input type="checkbox"/> Embedded metadata</li> </ul> <p>Will the system host metadata information?  <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If "YES," will there be security controls to prevent privacy leakage through the visibility of sensitive metadata across the network?  <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> <b>Other</b> - please specify:  <b>[no information available]</b></p>
4.5.11	<p><b>Analysis: Related to Information Disclosure and Sharing</b>  This portion of the PIA is to provide details about information related to PII disclosure and sharing. Identify privacy risks, mitigation strategies and, if necessary, provide a corrective action plan.</p>	<p><u>Privacy Risk:</u>  <b>[Unknown Risks to Consumers and Known Risks to Government workers and military personnel due to lack of disclosure about Accenture's processing activities.]</b></p> <p><u>Mitigation:</u>  <b>[Implement SA-9: External System Services;]</b></p> <p><u>Corrective Action Plan:</u>  <b>[Accenture should have Requirements for Businesses Collecting Large Amounts of Personal Information. ( a ) ( 1 );]</b></p>

#### 4.6 Destruction/Disposal

Describe below how the company manages the destruction and/or disposal of personally identifiable information.

No.	Questions and Fillable Answers	Responses
4.6.1	How will information be disposed of (e.g., placed in a confidential bin, disposed of by a contractor, or electronically wiped/erased)?	<b>[no information available]</b> If done by a contractor, provide the name of the contractor and a copy of the agreement. [insert response here]
4.6.2	What method does the organization use for secure deletion/destruction of PII?	<b>[no information available]</b>
	<i>[not requested]</i>	<i>[no response required]</i>
4.6.3	Does the entity formally validate the secure destruction /disposal of PII?	<input type="checkbox"/> Yes <input type="checkbox"/> No <b>[no information available]</b>
4.6.4	<b>Analysis: Related to Destruction / Disposal</b> This portion of the PIA is to provide details about information related to PII destruction and/or disposal. Identify privacy risks, mitigation strategies and, if necessary, provide a corrective action plan.	<u>Privacy Risk:</u> <b>[A business that discloses a data breach only in its SEC filing harms consumers as members of the workforce by failing to provide transparency of controls intended for data protection.]</b> <u>Mitigation:</u> <b>(SI-12: Information Management and Retention; SI-18: Personally Identifiable Information Quality Operations; SI-19: De-identification)</b> <u>Corrective Action Plan:</u> <b>[CCPA should audit Accenture's Record-Keeping and based on the results of testing the specified NIST 800-53r5 controls, require public disclosure of its 'CCPA Metrics' and pay a \$200/day fine for not registering as a data broker]</b>



4. Privacy Impact Assessment				
The AI and Automated Decisionmaking Technologies (ADT) Risk Assessment drafted by the CPPA consists of 7 sections under ARTICLE 10. RISK ASSESSMENTS:				
The Privacy Impact Assessment will consist of questions in six sections: Privacy	1) § 7150. When a Business Shall Conduct a Risk Assessment; 2) § 7153. Additional Requirements for Businesses Using Automated Decisionmaking Technology; 3) § 7154. Additional Requirements for Businesses that Process Personal Information to Train Artificial Intelligence or Automated Decisionmaking Technology; 4) § 7155. Restriction on Processing If Risks to Consumers' Privacy Outweigh Benefits; 5) § 7156. Timing and Retention Requirements for Risk Assessments; 6) § 7157. Conducting Risk Assessments for a Comparable Set of Processing Activities or in Compliance with Other Laws or Regulations; 7) § 7158. Submission of Risk Assessments to the Agency.			
4.1 Privacy Proc	§ 7158. Submission of Risk Assessments to the Agency. (a) Upon request, businesses shall make risk assessments available to the Agency or the Attorney General.			
1. Project/Proc AI and Automated Decisionmaking Technologies (ADT) Risk Assessment Questionnaire				
No.	Questions	Your Response to Consumers	Your Public Claims	How Other Entities Evaluate Your Business
4.11	1. Is this risk assessment on your company's use of ADT based on a documented privacy risk management process?	[declined]	The company's AI expertise spans more than 1,450 patents and pending patent applications worldwide and hundreds of client solutions at scale, ranging from marketing to retail and security to manufacturing. Accenture has embedded AI across its service delivery approach, driving efficiency, insights, and accelerating value for thousands of clients through its market leading platforms such as myVizard, SynOps, and MyNav. Six years ago, Accenture pioneered its responsible AI framework, which is now part of how Accenture delivers its work for clients, is included in the company's code of ethics and underlies its rigorous responsible AI compliance program. Accenture is currently working with many clients on generative AI projects, such as helping a hotel group manage customer queries or a judicial system synthesize judicial process information across hundreds of thousands of complex documents.	TrustArc is one company that provides independent certification for Responsible AI, which Accenture has not have.
	2. Does this risk assessment on your company's use of ADT include all technology used in processing personal information?	[write your response here]	[no public statement found]	[no source found]
	3. If your company conducts and submits a single risk assessment for each "comparable set of processing activities", please identify each processing activity.	[write your response here]	[no public statement found]	[no source found]
	4. For companies planning to conduct and document a risk assessment in accordance with the requirements of this Article no sooner than 2028 (24 months of the effective date of these regulations), please explain your reasons, and identify how your use of ADT will be governed to protect the rights of consumers.	[write your response here]	[no public statement found]	[no source found]
4.12	5. Does this risk assessment on your company's use of ADT include an inventory of all service providers, contractors, or third parties involved in processing consumers' personal information?	[declined]	According to <a href="https://www.accenture.com/content/dam/accure/infinal/accenture-com/document-2/Accenture-PDV-From-Davos-2024-200-Level-GenAI-Sessions-Rethinking-Responsibility-With-GenAI.pdf">https://www.accenture.com/content/dam/accure/infinal/accenture-com/document-2/Accenture-PDV-From-Davos-2024-200-Level-GenAI-Sessions-Rethinking-Responsibility-With-GenAI.pdf</a> , Accenture acts as a "data broker". Accenture assists its customers with "Data Services" which includes making data "AI-ready", and Accenture discloses its customers as a source of collected personal information, like many data brokers registered in the State of California. By assigning an Accenture employee or contractor to work for the customer, or by training the customers' employees, Accenture is capable of exposing the personal information of hundreds of thousands of consumers as an implementation agent of an "AI-ready workforce" within their customer's domain.	According to <a href="https://www.bleepingcomputer.com/news/security/accenture-confirms-data-breach-after-august-ransomware-attack/">https://www.bleepingcomputer.com/news/security/accenture-confirms-data-breach-after-august-ransomware-attack/</a> , Accenture has confirmed that the attackers stole information from its systems and leaked it online, but has not yet publicly acknowledged the data breach outside SEC filings or filed data breach notification letters with relevant authorities.

4.13	6. For each service provider, contractor, or third party explicitly named in your inventory, please identify which grouped categories represent these entities according to your company's disclosures to consumers:	[declined]	Third parties include our affiliates, public authorities, public websites and social media, suppliers, clients and vendors.	[no source found]
4.14	7. For each service provider, contractor, or third party explicitly named in your inventory, please identify the disclosed purpose for sharing consumers' personal information for ADT processing by these entities:	[declined]	[no public statement found]	[no source found]
	8. For each service provider, contractor, or third party explicitly named in your inventory, please provide the effective date of the binding, written contract specifying data processing agreements with these entities:	[write your response here ]	[no public statement found]	[no source found]
4.15	[not requested]	[no response required]	We have a global Client Data Protection ("CDP") program in place which governs the stewardship of client information and systems entrusted to us.	[no source found]
4.16	[not requested]	[no response required]	[no public statement found]	[no source found]
4.17	9. What guidelines are disseminated to users about the company's use of the ADT for validity, reliability, and fairness?	[declined]	"If you choose to exercise your rights, we will not charge you different prices or provide different quality of services unless those differences are related to your personal information or otherwise permitted by law."	[no source found]
4.18	10. Will a risk assessment occur before initiating any ADT processing activity, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public?	[write your response here ]	[no public statement found]	[no source found]

4.18	11. Will the risk assessment be shared with the consumer before obtaining their consent to the ADT processing activity?	[declined]	The disclosed categories of personal data have been obtained either directly from you (for example, when you provide information to sign up for a newsletter or register to comment on a forum website) or indirectly from certain third parties (for example, through our website's technology). Your decision to provide any personal data to us is voluntary. We will not use your personal information for purposes that are incompatible with the purposes of which you have been informed, unless it is required or authorized by law, or it is in your own vital interest (e.g. in case of a medical emergency) to do so.	[no source found]
4.19	12. Which safeguards allow consumers access to processing records such as audit or event logs for assurance that control over how their personal information is processed?	[declined]	1) For this reporting period, Accenture does not qualify for the CCPA 11 CCR § 999.317(g) reporting requirement; 2) You have the right at all times to register a complaint directly with the relevant supervisory authority or to make a claim against Accenture with a competent court (either in the country where you live, the country where you work or the country where you deem that data privacy law has been infringed).	[Accenture, Inc. dba Accenture ai.RETAIL] violated I. § 7004. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent. These Methods for Submitting Requests to Delete, Requests to Correct, and Requests to Know provided by [Accenture, Inc. dba Accenture ai.RETAIL] are not (a) (1) Easy to understand, nor (a) (3) clearly indicate the consumer's choice. Because the nature of my CCPA Request to KNOW is misinterpreted by [Accenture, Inc. dba Accenture ai.RETAIL] as a Request to Opt-out of Sale/Sharing, the Choice of Request Methods Are Not Symmetric, which violates subsection (c) of Methods for Submitting Requests to Delete, Requests to Correct, and Requests to Know.
4.110	13. How does your company verify and maintain the quality of personal information processed by the ADT, and/or personal information used to train the ADT?	[declined]	[no public statement found]	According to Craig S. Erickson, a California Consumer, Accenture denied my CCPA Request to KNOW, which impedes my ability to make corrections to my personal information.
4.111	[not requested]	[no response required]	[no public statement found]	According to Craig S. Erickson, a California Consumer, Accenture has failed to notify me of the sale or sharing of my personal information to Avanade, which I opted in to, and have proof that Avanade received it within 24 hours of providing it to Accenture.

4.112	<i>[not requested]</i>	<i>[no response required]</i>	<a href="https://www.accenture.com/us-en/about/privacy-policy.html">https://www.accenture.com/us-en/about/privacy-policy.html</a>	<i>[no source found]</i>
4.113	<i>[not requested]</i>	<i>[no response required]</i>	We hold an ISO27001 certification, which indicates that we adhere to strict information security standards. This is a security standard	Regarding the most recent data breach, an Accenture spokesperson replied with the company's original statement: "As we have stated, there was no
4.114	<i>[not requested]</i>	<i>[no response required]</i>	<i>[no public statement found]</i>	<i>[no source found]</i>
	14. Overall, does the company's assessment of whether the negative impacts identified in this assessment, as mitigated by the associated	<i>[declined]</i>	<i>[no public statement found]</i>	<i>[no source found]</i>
4.115	<i>[not requested]</i>	<i>[no response required]</i>	<i>[no public statement found]</i>	<i>[no source found]</i>
4.116	15. Does your company's use of ADT include context of the processing activity? If so, please list and describe the contexts for this processing activity.	<i>[declined]</i>	Our Privacy Statement scope applies to all of Accenture's externally facing applications, services, games, tools, websites and other data processing activities where Accenture is acting as a data controller.	According to Craig S. Erickson, a California Consumer, without disclosing what personal information of mine that Accenture has, and declining to disclose what ADT uses my information, Accenture's Privacy Statement is irrelevant whether I understand it or not.
4.117	<p><b>Risk Assessment Summary:</b>  <b>Accenture more likely than not, violated these CCPA Regulations:</b></p> <p><b>General Rules Regarding Verification.</b> (a), (c)(1), (c)(3)(b); <b>Verification for Password-Protected Accounts.</b> (a),(b); <b>Verification for Non-Accountholders.</b> (b),(c); <b>Requests to Limit Use and Disclosure of Sensitive Personal Information.</b> (a),(m)(2),(m)(4),(m)(8); <b>Consumers Less Than Under 13 Years of Age.</b> (c); <b>Service Providers and Contractors.</b> (a)(5); <b>Contract Requirements for Service Providers and Contractors.</b> (a),(b),(c); <b>Contract Requirements for Third Parties.</b> (b); <b>Methods for Submitting Requests to Delete, Requests to Correct, and Requests to Know.</b> (c),(d); <b>Timelines for Responding to Requests to Delete, Requests to Correct, and Requests to Know.</b> (a),(b); <b>Authorized Agents.</b> (a),(c),(d); <b>Requests to Know.</b> (a),(b); <b>Requests to Correct.</b> (a),(k); <b>Requests to Delete.</b> (b)(3); <b>Notice at Collection of Personal Information.</b> (a),(b),(c),(g)(1),(g)(2); <b>Privacy Policy.</b> (e)(1)(i),(e)(1)(k),(e)(3)(D), (e)(3)(F),(e)(3)(J),(e)(5); <b>Record-Keeping.</b> (a); <b>Requirements for Businesses Collecting Large Amounts of Personal Information.</b> (a)(2); <b>Sworn Complaints Filed with the Agency.</b> (a),(b); <b>Personal Information Security Breaches</b> (a)(1),(a)(2);</p> <p><b>Evidence of these violations can be collected from California consumers, Accenture's employees, customers, and third parties. Evaluating the corresponding NIST 800-53r5 controls which are included in Accenture's ATO for FedRAMP, can provide critical evidence consumers need for assessing the probability of harm when exercising their privacy rights or by working for or with Accenture in any capacity.</b></p>			

<b>4.2 Collection</b>	§ 7158. Submission of Risk Assessments to the Agency. (a) Upon request, businesses shall make risk assessments available to the Agency or the Attorney General.			
The following section pertains to the	<b>AI and Automated Decisionmaking Technologies (ADT) Risk Assessment Questionnaire</b>			
<b>No.</b>	<b>Questions</b>	<b>Your Response to Consumers</b>	<b>Your Public Claims</b>	<b>How Other Entities Evaluate Your Business</b>
4.2.1	16. Please explain how the company is permitted by statutory and regulatory authority to collect, use, maintain, and share: [PI listed in PTA Data Inventory (e.g. a copy of a consumer's government-issued identification card.)	"Accenture processes personal information in accordance with our Privacy Statement, all obligations in our Binding Corporate Rules, and applicable state and federal laws."	"Accenture processes personal information in accordance with our Privacy Statement, all obligations in our Binding Corporate Rules, and applicable state and federal laws."	According to Craig S. Erickson, a California Consumer, Accenture collected and shared my personal information I submitted to them when registering as a job applicant on their job portal hosted by Workday with Avanade, an undisclosed affiliate or third party without my consent.
4.2.2	<i>[not requested]</i>	<i>[no response required]</i>	<i>[no public statement found]</i>	<i>[no source found]</i>
4.2.3	<i>[not requested]</i>	<i>[no response required]</i>	Building on our leadership in cloud security services, Accenture Federal Services serves as a FedRAMP accredited Third Party Assessment Organization (3PADs). In this capacity, we help cloud service providers bring new, innovative offerings to the federal marketplace. Serving as a 3PAD also brings us additional insight and expertise that helps us architect federal environments to achieve real cyber resilience.	<i>[no source found]</i>
4.2.4	17. For compliance with data minimization, please explain how your company extracts specific personal data elements itemized in the Data Inventory from documents and records, which also contains other personal data elements or attributes which the company is not authorized to collect:	<i>[declined]</i>	"Accenture processes personal information in accordance with our Privacy Statement, all obligations in our Binding Corporate Rules, and applicable state and federal laws."	According to Craig S. Erickson, a California Consumer, when a business demands a copy of my valid government-issued identification, such as a valid passport or driver's license my reasonable expectation assumes that each data element (with the allowance, e.g. exception, of the redaction of your driver's license number or social security number) matches personal elements in the business' data inventory of personal information. I also assume that the right to maintain the government-issued id for as long as necessary to comply with legal obligations contradicts its claim that this information will be deleted 'immediately' without specifying how it is deleted, or providing any proof it was deleted.

	18. Please describe for each contextual processing activity, the relationship between the business and the consumers.	[declined]	As an industry leader in the use of Responsible AI, Accenture provides the following services to its customers: <a href="https://www.accenture.com/us-en/services/data-ai">https://www.accenture.com/us-en/services/data-ai</a> , <a href="https://www.accenture.com/us-en/services/finance-risk">https://www.accenture.com/us-en/services/finance-risk</a> , <a href="https://www.accenture.com/us-en/services/metaverse">https://www.accenture.com/us-en/services/metaverse</a> , <a href="https://www.accenture.com/us-en/services/supply-chain">https://www.accenture.com/us-en/services/supply-chain</a> , and <a href="https://www.accenture.com/us-en/services/talent-organization">https://www.accenture.com/us-en/services/talent-organization</a> .	This determination is supported by the FTC, that Accenture acts as an 'intermediary' when providing consulting services to its customer base which in turn, uses personal information, automated decisions, and guidance from Accenture.
4.2.5	19. Please describe for each contextual processing activity of the ADT, the disclosed purpose's compatibility with the context at time of collection.	[declined]	<b>Purpose of DATA SERVICES:</b> 1) Ready your data for generative AI; 2) Improve time to market and speed to value with trusted and timely data; 3) Power better customer experiences from contact center to citizen service; 4) Accelerate AI initiatives; 5) Generate new insights; 6) Improve products, services and operations.	According to Craig S. Erickson, a California Consumer, Accenture's public claims are considered 'Forward-looking Statements' which are documented in its SEC filings under 'Risk Factors'.
4.2.6	20. For each context listed, please describe for each contextual processing activity, what the consumers' reasonable expectations are or should be.	[declined]	Accenture's Privacy Statement applies to data processing activities where Accenture is acting as a data controller.	According to Craig S. Erickson, a California Consumer, my reasonable expectation is that Accenture, Inc. meets the definition of a 'data broker', collecting and sharing personal data on consumers as components of the following services: <a href="https://www.accenture.com/us-en/services/data-ai">https://www.accenture.com/us-en/services/data-ai</a> , <a href="https://www.accenture.com/us-en/services/finance-risk">https://www.accenture.com/us-en/services/finance-risk</a> , <a href="https://www.accenture.com/us-en/services/metaverse">https://www.accenture.com/us-en/services/metaverse</a> , <a href="https://www.accenture.com/us-en/services/supply-chain">https://www.accenture.com/us-en/services/supply-chain</a> , and <a href="https://www.accenture.com/us-en/services/talent-organization">https://www.accenture.com/us-en/services/talent-organization</a> . This determination is supported by the FTC, that Accenture, acts as an 'intermediary' when providing consulting services to its customer base which in turn, uses personal information, automated decisions, and guidance from Accenture, which is currently investigation for illegitimate business practices.

4.2.7	21. Describe which significant risks to consumers' privacy are attributed to how personal information is sourced?	[declined]	<b>What are the sources of marketing data?</b> The bulk of the personal information we collect and use for marketing purposes relates to individual employees of our clients and other companies with which we have an existing business relationship. We may also obtain contact information from public sources, including content made public at social media websites, to make an initial contact with a relevant individual at a client or other company.	According to Craig S. Erickson, a California Consumer who has led Accenture teams in previous consulting engagements with Accenture customers, there is no indication that it markets or sells products or services directly to consumers.
4.2.8	[not requested]	[no response required]	<b>Purpose of DATA SERVICES:</b> 1) Ready your data for generative AI; 2) Improve time to market and speed to value with trusted and timely data; 3) Power better customer experiences from contact center to citizen service; 4) Accelerate AI initiatives; 5) Generate new insights; 6) Improve products, services and operations.	[no source found]
4.2.9	[not requested]	[no response required]	[no public statement found]	[no source found]
4.2.10	22. How does the responsible human evaluate the appropriateness of the personal information processed by, and the logic and output(s) of, the ADT for the business's proposed use(s)?	[declined]	[no public statement found]	[no source found]
4.2.11	[not requested]	[no response required]	[no public statement found]	[no source found]
4.2.12	[not requested]	[no response required]	[no public statement found]	[no source found]
4.2.13	23. What input(s) from commercial sources, including GenAI or publicly available data, are used by the ADT, and how do these inputs perform as intended for the business's proposed use(s)?	[write your response here]	[no public statement found]	[no source found]

	24. Which personal information elements disclosed in your company's Data Inventory is processed to train AI or ADT?	[declined]	[no public statement found]	[no source found]
4.2.14	25. Is the person(s) responsible for the third-party's use of ADT within their products or services named as a stakeholder in this risk assessment?	[declined]	[no public statement found]	[no source found]
	26. Does the person(s) responsible for the third-party's use of ADT within their products or services name(s) the technological component(s) used in third party ADT provided by the third party?	[declined]	[no public statement found]	[no source found]
	27. Itemize the set of safeguards designed to ensure that the technological component(s) provided does not negatively impact the validity, reliability, or fairness of the company's use of the ADT?	[declined]	[no public statement found]	[no source found]
	28. Itemize the sets of safeguards which include internal or external evaluations related to the technological component's validity, reliability, or fairness provided to or conducted by the company?	[declined]	[no public statement found]	[no source found]
	29. Please explain how other versions of the ADT or other ADT offerings for validity, reliability, or fairness for the company's proposed use(s) was evaluated:	[declined]	[no public statement found]	[no source found]
4.2.15	30. How did your company determine what the minimum personal information is necessary to achieve the purpose of the processing?	[declined]	[no public statement found]	[no source found]
4.2.16	<p><u>Risk Assessment Summary:</u>  <b>Accenture more likely than not, violated these CCPA Regulations:</b></p> <p><b>General Rules Regarding Verification. (c)(1), (c)(2), (c)(3); Restrictions on the Collection and Use of Personal Information. (a), (b)(1), (b)(2); Requests to Know. (k)(3); Requests to Correct. (j); Requests to Delete. (b)(2), (e); Requests to Opt-Out of Sale/Sharing. (c); Requests to Limit Use and Disclosure of Sensitive Personal Information. (a), (m)(1); Service Providers and Contractors. (a)(3), (c), (g); Contract Requirements for Service Providers and Contractors. (b), (c); Contract Requirements for Third Parties. (a), (b); Notice at Collection of Personal Information. (e)(4); Record-Keeping. (a), (d), (e); Personal Information Security Breaches. (a)(1), (a)(2); Overview of Required Disclosures. (a); Privacy Policy. (e)(3)(J);</b></p>			

<u>4.3 Use</u>	§ 7158. Submission of Risk Assessments to the Agency. (a) Upon request, businesses shall make risk assessments available to the Agency or the Attorney General.			
The following information relates to how	<b>AI and Automated Decisionmaking Technologies (ADT) Risk Assessment Questionnaire</b>			
<b>No.</b>	<b>Questions</b>	<b>Your Response to Consumers</b>	<b>Your Public Claims</b>	<b>How Other Entities Evaluate Your Business</b>
4.3.1	31. Please describe which safeguards are designed to ensure that the ADT is used for appropriate purposes by other persons.	[declined]	[no public statement found]	[no source found]
4.3.2	32. Please provide documentation of how access to the required personal information of consumers is appropriate for the disclosed purposes.	[declined]	<b>We reserve the right to deny requests from authorized agents in certain circumstances, such as where we have a reasonable belief that the request is fraudulent.</b>	[no source found]
4.3.3	<i>[not requested]</i>	<i>[no response required]</i>	[no public statement found]	[no source found]
4.3.4	<i>[not requested]</i>	<i>[no response required]</i>	[no public statement found]	[no source found]
4.3.5	33. How are output(s) from the ADT secured and governed to prevent unauthorized use?	[declined]	[no public statement found]	[no source found]
4.3.6	34. For what appropriate disclosed purposes may persons external to the company use the ADT?	[declined]	<b>Legitimate interest means that Accenture has reasonable grounds to process your personal information. We rely on our legitimate interests for a given purpose, and we are of the opinion that our legitimate interests are not overridden by your interests, rights or freedoms, given (i) the transparency we provide on the processing activity, (ii) our privacy by design approach, (iii) our regular privacy reviews and (iv) the rights you have in relation to the processing activity. If you wish to obtain further information on this balancing test approach, please contact Accenture's Data Privacy Officer.</b>	[no source found]

4.3.7	[not requested]	[no response required]	[no public statement found]	[no source found]
4.3.8	35. Do internal safeguards exist to protect personal information, such as encryption, segmentation, and access controls?	[declined]	[no public statement found]	[no source found]
4.3.9	36. To what degree is human involvement needed in the company's use of ADT?	[declined]	[no public statement found]	[no source found]
	37. Is the person responsible for human involvement in your company's use of the ADT for determining if and how rights requests will be fulfilled listed as a stakeholder?	[declined]	[no public statement found]	[no source found]
	38. What qualifications does this responsible human have for understanding the company's use of the ADT, including the personal information processed by, the logic, and output(s) of, the ADT?	[declined]	[no public statement found]	[no source found]
	39. What documentation does your company maintain on how the responsible human influences decisions on the use of ADT and its output(s)?	[declined]	[no public statement found]	[no source found]
	40. If a responsible human is not involved in evaluating the appropriateness of the personal information used for the ADT, which additional safeguards are designed to address the risks to consumers' privacy?	[declined]	[no public statement found]	[no source found]
4.3.10	<p><b>Risk Assessment Summary:</b>  <b>Accenture more likely than not, violated these CCPA Regulations:</b>  <b>Authorized Agents.: Requests to Delete. ( e ); Notice at Collection of Personal Information. ( c ) ( 1 ), ( c ) ( 2 ), ( c ) ( 3 ), ( c ) ( 4 ), ( c ) ( 5 );</b>  <b>Privacy Policy. ( e ) ( 3 ) ( j ); Training. ( a ), ( b );</b></p> <p><b>Evidence of these violations can be collected from California consumers, Accenture's employees, customers, and third parties. Evaluating the corresponding NIST 800-53r5 controls which are included in Accenture's ATO for FedRAMP, can provide critical evidence consumers need for assessing the probability of harm when exercising their privacy rights or by working for or with Accenture in any capacity.</b></p>			

4.4 Maintenance		§ 1758. Submission of Risk Assessments to the Agency. (a) Upon request, businesses shall make risk assessments available to the Agency or the Attorney General.		
AI and Automated Decisionmaking Technologies (ADT) Risk Assessment Questionnaire				
No.	Questions	Your Response to Consumers	Your Public Claims	How Other Entities Evaluate Your Business
4.4.1	41. For each itemized storage location, please describe the methodology and/or criteria for evaluating the security of personal information used as input to the ADT and / or output from the ADT:	[write your response here ]	<b>We hold an ISO27001 certification, which indicates that we adhere to strict information security standards. This is a security standard awarded by the British Standards Institution ("BSI") that serves as international certification that Accenture adheres to the highest and strictest standards. This certification is the only auditable international standard that defines the requirements for an Information Security Management System ("ISMS"), and confirms that Accenture's processes and security controls provide an effective framework for protecting our clients' and our own information.</b>	[no source found]
4.4.2	42. Does your evaluation of using ADT to process access and opt-out requests include a maintenance plan for ensuring the quality of personal information?	[declined]	[no public statement found]	[no source found]
	43. Is timeliness included as a dimension of data quality for each access or opt-out request processed by the ADT?	[declined]	[no public statement found]	[no source found]
4.4.3	44. Does a determination by the ADT for fulfilling or denying access or opt-out requests factor in the reliability of the sources of the personal information used for processing such requests?	[declined]	[no public statement found]	[no source found]
	45. Does a determination by the ADT for fulfilling or denying access or opt-out requests evaluate validity as a dimension of data quality?	[declined]	[no public statement found]	[no source found]
	46. Does a determination by the ADT for fulfilling or denying access or opt-out requests evaluate completeness of personal information as a dimension of quality?	[declined]	[no public statement found]	[no source found]

	47. Did your company factor in accuracy as a dimension of data quality in the ADT's determination of whether each access or opt-out request will be fulfilled or denied?	[declined]	[no public statement found]	[no source found]
4.4.4	48. To what degree do material changes to the logic of ADT and any underlying assumptions of the logic affect the validity of this assessment?	[declined]	[no public statement found]	[no source found]
4.4.5	[not requested]	[no response required]	<b>We will retain your personal data only for as long as is necessary. We maintain specific records management and retention policies and procedures, so that personal data are deleted after a reasonable time according to the following retention criteria:</b> <b>We retain your data as long as we have an ongoing relationship with you (in particular, if you have an account with us).</b> <b>We will only keep the data while your account is active or for as long as needed to provide services to you.</b> <b>We retain your data for as long as needed in order to comply with our global legal and contractual obligations.</b>	[no source found]
4.4.6	[not requested]	[no response required]	[no public statement found]	[no source found]
4.4.7	49. Please describe each step your company takes to process deletion requests (Cal. Civ. Code 1798.105):	[write your response here]	[no public statement found]	[no source found]
4.4.8	[not requested]	[no response required]	[no public statement found]	[no source found]
4.4.9	[not requested]	[no response required]	[no public statement found]	[no source found]
4.4.10	[not requested]	[no response required]	[no public statement found]	[no source found]
4.4.11	<p><b>Risk Assessment Summary:</b>  <b>Accenture more likely than not, violated these CCPA Regulations:</b>  <b>General Rules Regarding Verification. ( c ) [ 1 ] ; Requests to Opt-In After Opting-Out of the Sale or Sharing of Personal Information. [ a ] ; Requests to Correct. [ b ] .</b></p> <p>Evidence of these violations can be collected from California consumers, Accenture's employees, customers, and third parties. Evaluating the corresponding NIST 800-53r5 controls which are included in Accenture's ATQ for FedRAMP, can provide critical evidence consumers need for assessing the probability of harm when exercising their privacy rights or by working for or with Accenture in any capacity.</p>			

4.5 Disclose/Sh § 7158. Submission of Risk Assessments to the Agency. (a) Upon request, businesses shall make risk assessments available to the Agency or the Attorney General.				
AI and Automated Decisionmaking Technologies (ADT) Risk Assessment Questionnaire				
In the following No.	Questions	Your Response to Consumers	Your Public Claims	How Other Entities Evaluate Your Business
4.5.1	50. Which safeguards allow consumers access to processing records, such as audit or event logs, for assurance that consumers can control how their personal information is processed?	[write your response here]	<b>1) For this reporting period, Accenture does not qualify for the CCPA 11 CCR § 999.317(g) reporting requirement; 2) You have the right at all times to register a complaint directly with the relevant supervisory authority or to make a claim against Accenture with a competent court (either in the country where you live, the country where you work or the country where you deem that data privacy law has been infringed).</b>	[no source found]
4.5.2	51. Does this risk assessment determine how the storage of personal information for ADT processing may present significant risk to consumers' privacy?	[declined]	<b>We will retain your personal data only for as long as is necessary. We maintain specific records management and retention policies and procedures, so that personal data are deleted after a reasonable time according to the following retention criteria:</b> <b>We retain your data as long as we have an ongoing relationship with you (in particular, if you have an account with us).</b> <b>We will only keep the data while your account is active or for as long as needed to provide services to you.</b> <b>We retain your data for as long as needed in order to comply with our global legal and contractual obligations.</b>	[no source found]
	52. Does this risk determination on the company's use of ADT consider why each category of personal information is retained for its specified length of time?	[declined]	<b>Accenture's undisclosed specific records management and retention policies and procedures apply to 'personal data' instead of personal data elements, and retention time is defined as 'a reasonable time' until it is deleted, without specifying what method of deletion is used.</b> <b>According to the following retention criteria:</b> <b>Consumers would know how long their data is retained if they have an account with us. Otherwise, there is no way for a consumer to know if we have an ongoing relationship with them. Because Accenture does not provide services to consumers, there is no way to register for an account and no method to 'keep it active'. This is similar to registered data brokers who process personal records without having a direct relationship with the consumer.</b>	[no source found]

4.5.3	53. Will the risk assessment be shared with the consumer before obtaining their consent to the ADT processing activity?	[write your response here]	[no public statement found]	[no source found]
4.5.4	54. What methodology and/or criteria is used by your company for determining potential negative impacts to consumers' privacy, when selling, sharing, or disclosing it to a third party?	[declined]	[no public statement found]	[no source found]
4.5.5	55. How does the company determine if the disclosure or sharing of personal information for ADT processing may present significant risk to consumers' privacy when a consumer opts-in to the sale / sharing of their personal information?	[declined]	[no public statement found]	[no source found]
4.5.6	56. State the the magnitude of its potential benefits for consumers opting-in to the sale / sharing of personal information used in the ADT?	[declined]	[no public statement found]	[no source found]
4.5.7	[not requested]	[no response required]	[no public statement found]	[no source found]
4.5.8	57. Please describe which pieces of personal information can be indexed or searched on for the purpose of finding consumer data your company needs or wants to share with others?	[write your response here]	[no public statement found]	[no source found]
4.5.9	[not requested]	[no response required]	[no public statement found]	[no source found]
4.5.10	[not requested]	[no response required]	[no public statement found]	[no source found]
4.5.11	<p><b>Risk Assessment Summary:</b>  <b>Accenture more likely than not, violated these CCPA Regulations:</b>  <b>General Rules Regarding Verification. ( c )( 1 ), ( c )( 3 ); Requests to Limit Use and Disclosure of Sensitive Personal Information. ( m )( 8 ); Service Providers and Contractors. ( a )( 1 ), ( a )( 2 ), ( a )( 4 ); Contract Requirements for Service Providers and Contractors. ( b ), ( c ); Third Parties. ( b ); Contract Requirements for Third Parties. ( b ); Privacy Policy. ( a ), ( e )( 1 ); Personal Information Security Breaches. ( a )( 1 )( 2 );</b></p> <p><b>Evidence of these violations can be collected from California consumers, Accenture's employees, customers, and third parties. Evaluating the corresponding NIST 800-53r5 controls which are included in Accenture's ATD for FedRAMP, can provide critical evidence consumers need for assessing the probability of harm when exercising their privacy rights or by working for or with Accenture in any capacity.</b></p>			

<b>4.6 Destruction</b>	<b>§ 7158. Submission of Risk Assessments to the Agency. (a) Upon request, businesses shall make risk assessments available to the Agency or the Attorney General.</b>			
Describe below how the company	<b>AI and Automated Decisionmaking Technologies (ADT) Risk Assessment Questionnaire</b>			
<b>No.</b>	<b>Questions</b>	<b>Your Response to Consumers</b>	<b>Your Public Claims</b>	<b>How Other Entities Evaluate Your Business</b>
4.6.1	58. Which safeguards address negative impacts from the company uses of the output(s) secured from the ADT, and if these impacts outweigh the intended benefits?	[declined]	[no public statement found]	[no source found]
4.6.2	59. Does the company use deidentification or aggregation of personal information as a method for secure deletion / destruction of personally identifiable information?	[declined]	<b>Where we maintain or use deidentified information, we will continue to maintain and use that information only in a deidentified form and will not attempt to reidentify the information.</b>	[no source found]
	60. Does the company factor in how the disposal of personal information for ADT processing may present significant risk to consumers' privacy?	[declined]	[no public statement found]	[no source found]
4.6.3	61. After processing a delete request, how, if at all, does the business maintain that data as deleted as contemplated in Cal. Civ. Code 1798.105(c)(2)?	[write your response here]	[no public statement found]	[no source found]
4.6.4	<p><b>Risk Assessment Summary:</b>  <b>Accenture more likely than not, violated these CCPA Regulations:</b>  <b>General Rules Regarding Verification. ( a ); Requests to Opt-Out of Sale/Sharing. ( c ); Restrictions on the Collection and Use of Personal Information. ( b )( 3 ); Third Parties. ( a ); Requests to Know. ( k )( 2 ); Requests to Correct. ( b ); Requests to Delete. ( b )( 1 ), ( b )( 2 ), ( e ); Notice at Collection of Personal Information. ( e )( 4 ); Record-Keeping. ( e );</b></p> <p><b>Evidence of these violations can be collected from California consumers, Accenture's employees, customers, and third parties. Evaluating the corresponding NIST 800-53r5 controls which are included in Accenture's ATD for FedRAMP, can provide critical evidence consumers need for assessing the probability of harm when exercising their privacy rights or by working for or with Accenture in any capacity.</b></p>			



---

**From:** Carina Arroyo [REDACTED]  
**Sent:** Tuesday, August 20, 2024 2:38 PM  
**To:** Regulations@CPPA  
**Subject:** Public Comment Data Broker Registration  
**Attachments:** CA CCPA Rulemaking Data Broker Comment final.pdf

---

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Please see the attached public written comment above entitled "Comments on Proposed Rulemaking regarding Data Broker Registration Regulation."

Thank you,

**hite**BrennerLLP

Carina Arroyo | Project Assistant [REDACTED]

---



Consumer Data Industry Association 1090  
Vermont Ave., NW, Suite 200  
Washington, D.C. 20005-4905

Writer's direct dial [REDACTED]

[CDIAONLINE.ORG](http://CDIAONLINE.ORG)

August 19, 2024

**Via Electronic Delivery to [regulations@cppa.ca.gov](mailto:regulations@cppa.ca.gov)**

California Privacy Protection Agency  
Attn: Elizabeth Allen  
2101 Arena Boulevard  
Sacramento, CA 95834

**RE: Comments on Proposed Rulemaking regarding Data Broker Registration Regulation.**

To whom it may concern:

The Consumer Data Industry Association<sup>1</sup> submits this comment letter in response to the pending rulemaking activity with regards to data broker registration. Specifically, we would like to comment on §7603, registration information requirements.

§7603(d) (2-3) of the proposed regulation requires a disclosure of the type of personal information collected under federal laws such as the Fair Credit Reporting Act and Gramm-Leach Bliley Act amongst others. The regulation states that a data broker must disclose the specific products or services that are covered and the "approximate proportion" of data collected and sold that is subject to these federal laws. This requirement is on data that is otherwise exempt from the definition of a data broker and therefore not subject to registration with the state. Additionally, this disclosure of information does not provide a benefit to consumers, in fact such an extensive and fluid disclosure is unlikely to provide a clear benefit to consumers in exercising privacy rights or provide realistic expectations with respect to which data is subject to privacy rights.

The requirement to disclose the specific products or services "covered by" specific federal laws could force data brokers to provide disclosures to consumers without the context necessary to understand the scope of the coverage. Many of the federal laws apply to the types of data or regulated entity rather than the products. Further, the specific types of products or services can change resulting in frequent registration updates that are unhelpful or confusing for consumers. The CCPA therefore should reconsider such requirements that do not benefit consumers.

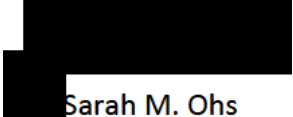
Additionally, the regulation requires a disclosure of the "approximate proportion" of data collected subject to these exempted federal laws. The requirement is drafted in such a way that does not provide data brokers clear reporting standards to determine what is required. This vague requirement, in conjunction with the lack of a standard, means that data

<sup>1</sup> 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 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, helping ensure fair and safe transactions for consumers, facilitating competition and expanding consumers' access to financial and other products suited to their unique needs.

brokers will disclose what appears to be fluid percentages. It is likely to cause greater confusion to consumers as there is no consistent standard that data brokers must follow when reporting.

The CCPA should remove the requirements in §7603(d) (2-3) because the required information does not apply to data that is subject to registration and is unnecessary to meet the statutory obligations. More importantly, the disclosure of this information, as drafted, is vague in nature and fails to benefit the consumer in any meaningful way. Such requirements are more likely to confuse consumers as the data is reported without context or a standard to follow. For these reasons we believe these requirements in §7603(d) (2-3) are unnecessary and should be removed.

Sincerely,



Sarah M. Ohs

Vice President of Government Relations



---

**From:** Matt Schwartz [REDACTED]  
**Sent:** Tuesday, August 20, 2024 2:46 PM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on Data Broker Registration Regulations - Consumer Reports  
**Attachments:** Comments of Consumer Reports In Response to the California Privacy Protection Agency's Invitation for Comments On Proposed Data Broker Regulations - FINAL.pdf

---

**This Message Is From an External Sender**

**WARNING:** This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Good afternoon,

Attached, please find Consumer Reports' comments in response to CPPA's call for public comments on data broker registration regulations.

Please feel free to reach out if you have any questions or would like to discuss our views in further detail.

**Best,  
-Matt**

Matt Schwartz  
Policy Analyst  
[REDACTED]

Pronouns: he, him, his

[CR.erg](#) Elt

\*\*\*

This e-mail message is intended only for the designated recipient(s) named above. The information contained in this e-mail and any attachments may be confidential or legally privileged. If you are not the intended recipient, you may not review, retain, copy, redistribute or use this e-mail or any attachment for any purpose, or disclose all or any part of its contents. If you have received this e-mail in error, please immediately notify the sender by reply e-mail and permanently delete this e-mail and any attachments from your computer system.

\*\*\*

Comments of Consumer Reports  
In Response to the  
California Privacy Protection Agency's  
Invitation for Comments On  
Proposed Data Broker Regulations

By

Matt Schwartz, Policy Analyst, Consumer Reports  
Justin Brookman, Director of Technology Policy, Consumer Reports

August 20, 2024



Consumer Reports<sup>1</sup> appreciates the opportunity to provide feedback on the California Privacy Protection Agency’s (CPPA) Invitation for Comments on Proposed Data Broker Regulations. We thank the CPPA for initiating this proceeding and for its other initiatives to protect consumer privacy. We are supportive of the Agency’s efforts to provide additional clarity for consumers and businesses about the scope of data brokers’ registration responsibilities under the Delete Act.

We provide responses to several of the Agency’s proposed regulations below.

## **I. Section 7601 (Definitions)**

### *“Direct Relationship”*

“Data broker” currently means a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.<sup>2</sup> The Agency proposes defining the term “direct relationship” to provide additional clarity.

This is a critical definition, as the existing framework has led to substantial ambiguity surrounding which data brokers are included in the scope of the law. This, along with the long list of other possible exemptions data brokers can claim and the lack of substantial enforcement to-date, has led to a perceived under-count of registered data brokers compared with the full universe of data brokers doing business in the state.<sup>3</sup> On top of that, data brokers employ notoriously complex and opaque data aggregation tactics, amassing data from hundreds or even thousands of different sources, which can make the determination of a “direct relationship” genuinely difficult to assess without further guidance. Ultimately, the Delete Act sought to provide consumers an easier way to manage their right to delete relative to businesses that collect and sell their personal information without their knowledge or consent — an intent that should be mirrored in the regulations.

We are therefore largely supportive of this proposed definition, which states that if a consumer intentionally interacts with a business to obtain information about or accesses, purchases, uses, or requests products or services within the preceding three years, a direct relationship exists. Providing a timeframe is helpful, as the term “direct relationship” implies an ongoing dialogue between consumer and business; businesses should not be considered as having direct

---

<sup>1</sup> Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers’ interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

<sup>2</sup> Civil Code Section 1798.99.80 (c)

<sup>3</sup> Suzzane Smalley, Delete-your-data laws have a perennial problem: Data brokers who fail to register, *The Record*, (October 17, 2023), <https://therecord.media/state-data-broker-registries-california-vermont>

relationships with consumers indefinitely just because they may have interacted at one time. Three years without interaction between consumer and business is reasonable to establish that the consumer no longer desires to continue the relationship with the business and that any consent to collect or share personal data should be considered lapsed. This understanding has precedent in other areas of the law. For example, California generally considers financial assets “abandoned” if there has been no activity on the account or contact with the owner for three years.<sup>4</sup>

The Rules would also clarify that a business is “still a data broker if it has a direct relationship with a consumer but also sells personal information about the consumer that the business did not collect directly from the consumer.”<sup>5</sup> Whether a company is acting as a data broker or engaging in the practice of data brokerage depends on the context. A company like Facebook is not generally known as a data broker, but they act as one when they sell access to consumer information that did not derive from a direct interaction with the consumer (for example, for personal data collected through the Facebook pixel embedded on third-party websites).

However, applying universal deletion requests to all personal information collected by entities that have hybrid direct-indirect relationships with consumers may carry unintended consequences that could negatively impact consumers. The Agency should consider clarifying the Rules to state that universal deletion requests should only apply to the personal information that was indirectly collected from consumers and not all of the personal information held by that entity. While a consumer’s universal deletion request should certainly apply to information that was surreptitiously collected and subsequently sold (e.g. data from third-party cookies, pixels, or other online tracking technologies), it shouldn’t also apply to information they have shared directly with the business and might reasonably want to exercise more granular control over (e.g. photos uploaded to Facebook) and for which existing CCPA rights would suffice.

At the same time, entities more widely considered to be data brokers may collect data, in some instances, directly from consumers and should not be let off the hook. For instance, until recently, major location data broker X-Mode collected some personal data directly from consumers through its Walk Against Humanity and Drunk Mode apps.<sup>6</sup> Yet X-Mode predominantly collected data from other sources, including SDKs embedded in hundreds of third-party apps<sup>7</sup> and purchases of location data from other data brokers and aggregators, which led it to become the “2nd largest US location data company.”<sup>8</sup> The proposed approach would ensure that data brokers like X-Mode would not receive a total carveout just because they

---

<sup>4</sup> California State Controller’s Office, About Unclaimed Property, [https://www.sco.ca.gov/upd\\_about\\_unclaimed\\_property.html](https://www.sco.ca.gov/upd_about_unclaimed_property.html)

<sup>5</sup> Proposed Section 7601(a)

<sup>6</sup> X-Mode Social, Inc., Complaint, In the Matter of X-Mode Social, Inc., FTC File No. 202-3038 (2024), [https://www.ftc.gov/system/files/ftc\\_gov/pdf/X-Mode-Complaint.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-Complaint.pdf)

<sup>7</sup> Express VPN, Investigation Xoth: Smartphone location tracking, <https://www.expressvpn.com/digital-security-lab/investigation-xoth>

<sup>8</sup> X-Mode Social, Inc., Complaint, In the Matter of X-Mode Social, Inc., FTC File No. 202-3038 (2024), [https://www.ftc.gov/system/files/ftc\\_gov/pdf/X-Mode-Complaint.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-Complaint.pdf)



collect a small fraction of consumer data from first-party apps. Going forward, this should help avoid creating perverse incentives for data brokers to create superficial “direct relationships” with consumers through mechanisms like a viral quiz app in order to avoid being classified as a data broker.

### *“Minor”*

The Agency proposes defining the term “minor” as persons under 16 years of age and establishing when a business is considered to have knowledge of a person’s age. We support the inclusion of this definition, as data brokers may have adopted a narrower reading of the term “minor” without further clarification. The chosen definition is consistent with the CCPA, which already implicitly creates a category for minors (including different protections for those individuals aged 0-12 and 13-15, respectively) and provides them with enhanced protections compared to those aged 16 and up.<sup>9</sup>

### *“Reproductive Health Care Data”*

The Agency proposes defining the term “reproductive health care data” to include “information about a consumer searching for, accessing, procuring, using, or otherwise interacting with goods or services associated with the human reproductive system”,<sup>10</sup> certain types of health services and treatments, and information about consumers’ sexual history and family planning. We support the proposed definition, which will provide consumers insight into whether data brokers collect any information about these especially sensitive categories of information.

Importantly, the definition also includes inferences about consumers’ reproductive health care data. This is critical, as one of the main business lines for many data brokers is to aggregate information from a variety of sources to create marketing segments that make inferences about consumers (e.g. “expectant mothers”)<sup>11</sup> that are then shared or sold to other third parties. With the vast data stores held by data brokers, it’s possible that these inferences could be generated even without collection of any other reproductive health care data. Incorrect inferences about consumers can have damaging effects, including negative economic impacts<sup>12</sup> or directly endangering individuals’ safety.<sup>13</sup> But even when inferences are correct, given the sensitivity of the assumptions in question and lack of control consumers otherwise have over data brokers,

---

<sup>9</sup> CCPA Section 1798.120(c), [https://cppa.ca.gov/regulations/pdf/cppa\\_act.pdf](https://cppa.ca.gov/regulations/pdf/cppa_act.pdf)

<sup>10</sup> Proposed Section 7601(e)

<sup>11</sup> Jon Keegan and Joel Eastwood, From “Heavy Purchasers” of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You, The Markup, (June 8, 2023), <https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you>

<sup>12</sup> See, e.g., Kashmir Hill, Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies, the New York Times, (March 13, 2024), <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>

<sup>13</sup> Suzanne Bernstein, The Role of Digital Privacy in Ensuring Access to Abortion and Reproductive Health Care in Post-Dobbs America, American Bar Association, (June 3, 2024), [https://www.americanbar.org/groups/crsj/publications/human\\_rights\\_magazine\\_home/technology-and-the-law/the-role-of-digital-privacy-in-ensuring-access-to-reproductive-health-care/](https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/technology-and-the-law/the-role-of-digital-privacy-in-ensuring-access-to-reproductive-health-care/)

these inferences are inherently harmful. And even worse, data brokers have a poor track record of sharing reproductive health information with politically motivated actors that can put people in mortal danger.<sup>14</sup> It is very likely that data brokers' ability to collect or make inferences about any aspect relating to consumers' reproductive health will be material to their decision to exercise their rights under the Delete Act.

## **II. Section 7602 (Registration Submission Requirements)**

### *Registration Transparency*

The Agency proposes clarifying that each data broker business, regardless of its status as a subsidiary or parent company to another business, is required to uniquely register so long as it "independently meets the definition of 'data broker.'"<sup>15</sup> We support this proposal, as it will prevent businesses from potentially evading disclosure of registration details that could be material to a consumer's decision to delete data held by a particular data broker. For instance, one can envisage a data broker with multiple subsidiaries independently operating as data brokers, each of which collect different types of consumer data. Each of those subsidiaries should be required to provide information required by Section 1798.99.82(b)(2), including whether they collect minors' data or reproductive health data, since these categories of personal data are uniquely sensitive and may be material to consumers' decision to exercise their rights under the Delete Act. While we don't believe that businesses should be required to register each separate legal entity in its corporate structure (e.g. Acme Data Broker Holding Company, Acme Data Broker Incorporated) since this could unnecessarily complicate the registry, businesses should be required to register subsidiaries that do business under unique business names that do not share common branding with the parent organization or that consumers would not reasonably associate with each other.

### *Penalty of Perjury*

The agency seeks to establish a rule requiring an employee or agent for the data broker to register on behalf of the data broker and to have sufficient knowledge of their practices to provide accurate information under penalty of perjury. This proposal will provide extra assurance that data broker registration information will be accurate and useful for consumers and that individuals will be held personally liable when they supply information to the Agency. As the Agency points out in the Initial Statement of Reasons, adding a penalty of perjury "provides the Agency with the option of seeking sanctions and referring the matter to law enforcement in the event that such information is not true, complete, or accurate."<sup>16</sup> The Delete Act currently only contemplates an administrative fine of two hundred dollars when data brokers fail to meet registration requirements.<sup>17</sup> Without the prospect of personal liability, some data brokers may

---

<sup>14</sup> Joseph Cox, Data Broker Is Selling Location Data of People Who Visit Abortion Clinics, Vice, (May 3, 2022), <https://www.vice.com/en/article/location-data-abortion-clinics-safegraph-planned-parenthood/>

<sup>15</sup> Proposed Section 7602(a)

<sup>16</sup> Initial Statement of Reasons, Proposed Section 7602(b), [https://cppa.ca.gov/regulations/pdf/data\\_broker\\_reg\\_isor.pdf](https://cppa.ca.gov/regulations/pdf/data_broker_reg_isor.pdf)

<sup>17</sup> Delete Act, Section 1798.99.82(c)(1), <https://legiscan.com/CA/text/SB362/2023>

decide that the benefits of providing inaccurate information outweigh the punishment of any potential fines, drastically reducing the efficacy of the registry.

**Section 7603 (Registration Information Requirements)**

The agency seeks to establish a rule requiring disclosure of the types of personal information, products and services, and the proportion of data collected and sold that are subject to other laws that qualify data brokers to claim an exemption.<sup>18</sup>

The Delete Act states that data brokers do not include entities “to the extent” that they are covered by the federal Fair Credit Reporting Act, Gramm-Leach-Bliley Act, Insurance Information and Privacy Protection Act, or Confidentiality of Medical Information Act,<sup>19</sup> which introduces ambiguity regarding when data brokers must register with the Agency and what information they must provide. Many data brokers offer various business lines, products, and services, some of which may involve exempted information and some that may not. Consumers should be aware of the extent to which their deletion request will reach certain types of personal information held by the data broker and when the broker can rely on an exemption. Historically, it has been difficult for consumers, researchers, and advocates to understand who is required to comply with CCPA due to the complex interplay between exemptions and a relative lack of required disclosures when businesses are relying on an exemption.<sup>20</sup> By requiring data brokers to describe “the approximate proportion of data collected and sold that is subject to the enumerated laws in comparison with their total annual data collection and sales” consumers will be able to better anticipate the effect that their deletion request will have and plan accordingly.

\*\*\*\*\*

We thank the California Privacy Protection Agency for its consideration of these points, and for its work to secure strong privacy protections for consumers. We are happy to answer any questions you may have, and to discuss these issues in more detail. Please contact Matt Schwartz [REDACTED] or Justin Brookman [REDACTED] for more information.

---

<sup>18</sup> Proposed Section 7603(d)

<sup>19</sup> Delete Act, Section 1798.99.80(c)(1-4), <https://legiscan.com/CA/text/SB362/2023>

<sup>20</sup> See, e.g., Consumer Reports, Companies Continue to Share Health Data Despite New Laws, (January 16, 2024),

<https://advocacy.consumerreports.org/wp-content/uploads/2024/01/Companies-Continue-to-Share-Health-Data-1-16-2024-Consumer-Reports.pdf>

---

**From:** V [REDACTED]  
**Sent:** Tuesday, August 20, 2024 3:07 PM  
**To:** Regulations@CPPA  
**Subject:** Formal Comments to the CPPA - S8362

---

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Dear Ms. Allen:

Please include the following written comments at today's hearing regarding 5B362. I am uncertain I will be able to attend.

The mega data broker, Verisk, is not complying with either the spirit or letter of the law. In fact, it does not even register with the California Data Broker Registry.

When Verisk is asked about why it evades compliance, it gives absurd arguments that conflates its obligations under several California laws - ALL of which it breaks with impunity. Verisk is the data broker darling of the trillion-dollar insurance industry, allowing people throughout the world prodigious amounts of personal information of American and California citizens.

You have my permission to use my initials (preferable) or my name ([REDACTED]) if necessary.

Thank you and best regards,

VMC

Comments:

This year is the 25<sup>th</sup> anniversary of Amy Boyer's tragic murder at the hands of her stalker. This was a tragedy that would never have occurred but for the release of her private information by data brokers, which sold it for profit. After finally purchasing it from a data broker, her stalker was able to locate Amy and lay in wait for her. He shot her 11 times and then turned the gun on himself. Without the "complicity" of data brokers in her tragic death, Amy would still be alive. To date and despite many legislative efforts to stop this practice, little has actually changed. Data brokers continue these same sorts of privacy intrusions - with little regard for the consequences, if not abject impunity.

The non-compliance of data brokers in this day and age is unacceptable. The law today is crystal clear. Data brokers are required to remove data upon request. But even with clear-cut, black line laws, many data brokers just do not comply. It is obvious that some of these data brokers simply thumb their noses at state and federal laws.

Consider the insurance industry darling, Verisk, that seems to place profits far and away above compliance with the law and even the safety of crime victims.

Verisk, a global company that could only be considered an insurance industry data broker, *purposefully* puts victims' personal information at risk even though it has received actual notice from stalking crime victims that their lives are in danger. Its two top attorneys, Kathy Card Beckles (Chief Legal Officer) and Samantha Vaughan (Chief Privacy Officer) have repeatedly refused to implement privacy safeguards for victims of crime even where they were given actual notice that a situation of life endangerment exists.

This duo continued to allow access to the personal information of crime victims even when specifically given notice of the grave risks associated with allowing such access. It refuses to comply with state law, including registering with the data registry provisions pursuant to the Safe at Home constellation of statutes. *See CCP 367.3 et seq.*

Instead of complying with the Safe at Home Act, Verisk continues to retain this information in their databases and disseminate it to outside parties even if it imperils the life and safety of crime victims. It is only a matter of time before its conduct has catastrophic, if not fatal, consequences.

There needs to be a private cause of action for bad actors that do not comply with California privacy laws, including greater fines, longer jail time for the officers and directors of such compliant firms, and other sanctions to give greater teeth to these statutes. State enforcement alone is not enough.

The choice is clear: Stand in solidarity with terrified crime victims or stand with behemoth data brokers that break the law with impunity as they broker the personal details of people's lives.

<sup>[1]</sup> Amy Boyer was murdered by her stalker 25 years ago but many continue to be terrorized by stalkers each year. *See, e.g.*, LA Times, J.M. Hirsch, “Chilling Web Site Reveals a Killer’s Obsessive Plans,” (Dec. 5, 1999) <https://www.latimes.com/archives/la-xpm-1999-dec-05-mn-40632-story.html>.

--

CONFIDENTIALITY NOTE: This message is intended only for the use of the individual or entity to which it is directed and may contain information that is privileged, confidential, protected as an attorney-client communication, and/or may be exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution, review, or copying of this communication and any accompanying attachment(s) is strictly prohibited. If you have received this communication in error, please notify the sender immediately and destroy the original message. Unintended transmission shall not constitute waiver of the attorney-client or any other privilege. Thank you.

---

**From:** Shen, Lei [REDACTED]  
**Sent:** Tuesday, August 20, 2024 3:45 PM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on Data Broker Registration Regulations  
**Attachments:** Delete Act Rulemaking Comment from Client (8.20.2024).pdf

---

**This Message Is From an Untrusted Sender**

**Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.**

[Report Suspicious](#)

Please find attached comments on behalf of an anonymous client to the California Privacy Protection Agency concerning the Agency's proposed Data Broker Registration Regulations. Our client appreciates the opportunity the Agency has provided for comments.

Sincerely,  
Lei Shen

**Lei Shen**  
Cooley LLP  
110 N. Wacker Drive, Suite 4200  
Chicago, IL 60606-1511

---

This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message. If you are the intended recipient, please be advised that the content of this message is subject to access, review and disclosure by the sender's Email System Administrator.



August 20, 2024

**VIA EMAIL**

California Privacy Protection Agency  
Attn: Elizabeth Allen  
2101 Arena Boulevard  
Sacramento, CA 95834  
[regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

**RE: Public Comment on Data Broker Registration Regulations**

Dear Ms. Allen,

Please find attached comments on behalf of an anonymous client to the California Privacy Protection Agency ("Agency") concerning the Agency's proposed Data Broker Registration Regulations dated July 5, 2024, implementing and defining terms in Senate Bill 362. To be clear, these comments are not provided on behalf of Cooley LLP and do not necessarily reflect the views of Cooley LLP, but instead reflect comments from a client who asked that we submit such comments on its behalf. Our client thanks the Agency for the opportunity to provide these comments.

Sincerely,

Lei Shen  
Partner, Cooley LLP



Dear Ms. Allen,

Below please find our comments concerning the California Privacy Protection Agency's ("Agency") proposed Data Broker Registration Regulations dated July 5, 2024 ("proposed regulations"), implementing and defining terms in Senate Bill 362 (the "Delete Act").

Digital identity verification is a necessary part of making online transactions happen. Data from consumers' devices and other online credentials are important identity anchors that help businesses solve identity verification challenges and increase trust between businesses and their consumers. On balance, we support the substantive reasoning behind the Delete Act, which, if followed faithfully, should help to increase consumer trust in online platforms. However, we would respectfully request that the Agency consider the following observations regarding elements of the proposed regulations that touch on digital identity verification.

### **1. Proposed Definition of the Term "Direct Relationship" (Sec. 7601(a))**

The Agency's proposed regulations define the term "direct relationship"<sup>1</sup> with the intent of "provid[ing] clarity on what businesses are data brokers and ensur[ing] the definition is consistent with [the text of the Delete Act]."<sup>2</sup> However, we request the Agency to consider the following three concerns regarding the proposed definition.

First, the proposed definition of "direct relationship" departs from and significantly broadens the scope of both what Assembly Bill No. 1202 ("AB 1202")<sup>3</sup> provided to be a direct relationship between a business and a consumer, and the Delete Act's intended scope of which businesses would qualify as data brokers.

Second, the proposed definition is inconsistent with similar state data broker laws, which expressly acknowledge that a consumer using a business's services establishes a direct relationship with that business without exception.

Third, the proposed definition requires clarification in regard to the exemption "*for the business to verify the consumer's identity.*" It is not clear if this exemption only relates to the identity verification conducted in connection with a consumer exercising the consumer's rights under the law, or if it should be read more broadly as a general exemption for identity verification purposes.

<sup>1</sup> Proposed Regulations § 7601(a) (defining the term "direct relationship" as "a consumer intentionally interacts with a business for the purpose of obtaining information about, accessing, purchasing, using, or requesting the business's products or services within the preceding three years. A consumer does not have a 'direct relationship' with a business if the purpose of their engagement is to exercise any right described under Title 1.81.5 of Part 4 of Division 3 of the Civil Code, or for the business to verify the consumer's identity. A business is still a data broker if it has a direct relationship with a consumer but also sells personal information about the consumer that the business did not collect directly from the consumer.").

<sup>2</sup> See California Privacy Protection Agency – Notice of Proposed Rulemaking: Data Broker Registration (published July 5, 2024) at 4.

<sup>3</sup> See A.B. 1202, Chapter 753, Statutes of 2019 (Ca. 2019).

**A. The Agency should retain AB 1202’s explanations regarding how direct relationships between consumers and businesses may be formed, which include more appropriate clarifications on the types of businesses that *do not* qualify as data brokers.**

AB 1202 has been the primary regulatory framework governing data brokers since its passage by the California legislature in 2019, and businesses have relied on the explanations in this law to understand whether they qualify as a data broker. While the Delete Act amended AB 1202, the Delete Act retained AB 1202’s definition of “data broker” as “a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.”<sup>4</sup> However, the Delete Act did not carry over an important explanation in AB 1202 regarding what constituted a “direct relationship,” which stated:

There are important differences between data brokers and businesses with whom consumers have a direct relationship. *Consumers who have a direct relationship with traditional and e-commerce businesses, which could have formed in a variety of ways* such as by visiting a business’ premises or internet website, or by affirmatively and intentionally interacting with a business’ online advertisements, *may have some level of knowledge about and control over the collection of data by those businesses*, including: the choice to use the business’ products or services, the ability to review and consider data collection policies, the ability to opt out of certain data collection practices, the ability to identify and contact customer representatives, and the knowledge necessary to complain to law enforcement. *By contrast, consumers are generally not aware that data brokers possess their personal information*, how to exercise their right to opt out, and whether they can have their information deleted, as provided by California law.<sup>5</sup>

This explanation in AB 1202 highlighted an important distinction in identifying what is a direct relationship with a business versus a relationship with a data broker — a “direct relationship” with a business is one where a consumer has “some level of knowledge about and control over the collection of data by [the business],” whereas a relationship with a data broker is one where a consumer is unaware that the data broker possesses the consumer’s personal information.

Many businesses with direct consumer relationships supplement the data they obtain directly from the consumer with data they obtain from other sources. Such businesses may include businesses that operate in hybrid business-service provider capacities (where they also obtain information from their business customers) or that otherwise *require* externally-sourced data in order to provide their services to an end-user consumer. AB 1202’s explanation helped clarify that such companies would still be considered as having a “direct relationship” with the consumer (*i.e.*, would not be treated as data brokers).

In contrast, the proposed regulations’ definition of “direct relationship” is far too expansive — it states that “[a] business is still a data broker if it has a direct relationship with a consumer *but also sells personal information about the consumer that the business did not collect directly from the*

<sup>4</sup> See A.B. 1202 at Section 2(d); Delete Act at Section 1(c).

<sup>5</sup> A.B. 1202 at Section 1(g)-(h) (emphasis added).

consumer.”<sup>6</sup> Because the Delete Act utilizes the broad definition of “sell” from the California Consumer Privacy Act of 2018 (“CCPA”),<sup>7</sup> this proposed definition of “direct relationship” would capture as data brokers an expansive range of companies that, although leveraging third-party data sets (including those of which the consumer may be aware or otherwise have control over), are still delivering important services to or for consumers with whom they have direct relationships. For example, the proposed definition could capture as data brokers companies that provide fraud prevention and identity verification services, despite such companies providing these services with the consumer’s knowledge and to their direct benefit.

We agree with the Agency that the existence of a direct relationship is the correct standard for defining whether a business is a “data broker.” However, we respectfully request that the Agency retain AB 1202’s original intention and explanation regarding what constitutes a “direct relationship” so as to resolve the concerns noted above.

**B. The Agency should revise its definition of “direct relationship” to align with the exclusions in similar state data broker laws, to promote uniformity regarding the types of businesses that *do not* qualify as data brokers.**

There are currently three other U.S. states with data broker-specific laws in effect: Vermont, Oregon, and Texas.<sup>8</sup> While these laws are substantially similar to the Delete Act in several aspects, unfortunately the Agency’s proposed exception to what is considered to be a “data broker” in its proposed regulations (in its definition of “direct relationship”) would materially deviate from the other laws’ approach to which entities are captured as data brokers. For example, the Vermont and Oregon definitions of “data broker” both categorically exclude from scope any customer, subscriber, or user of the business entity’s goods or services,<sup>9</sup> whereas the proposed regulations would still capture such entities if they happen to “sell personal information about the consumer that the business did not collect directly from the consumer.”<sup>10</sup>

As a result, the proposed regulations would lead to materially inconsistent and conflicting applicability and obligations among the state data broker laws. To avoid this, we respectfully request that the Agency consider revising its proposed regulations to *strike* the following sentence from the proposed definition of “direct relationship”: “*A business is still a data broker if it has a direct relationship with a consumer but also sells personal information about the consumer that the business did not collect directly from the consumer.*”

<sup>6</sup> Proposed Regulations § 7601(a) (emphasis added).

<sup>7</sup> See Cal. Civ. Code § 1798.140(ad)(1).

<sup>8</sup> See e.g., Vermont Act 171 (2018); Oregon H.B. 2052 (2023); Texas S.B. No. 2105 (2023).

<sup>9</sup> See e.g., 9 V.S.A. § 2430(4)(A)(B)(i) (defining “data broker” as “a business [...] that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship” and explaining that a direct relationship with a business includes if the consumer is “a past or present customer, client, subscriber, user, or registered user of the business’s goods or services”); O.R.S. § 646A.593(1)(c)(B)(ii)(I) (excluding from its definition of “data broker” a “business entity that collects information about a resident individual if the resident individual is or was a customer, subscriber or user of the business entity’s goods or services.”).

<sup>10</sup> Proposed Regulations § 7601(a) (emphasis added).

### C. Clarification of the phrase “verify the consumer’s identity.”

Lastly, the proposed definition of “direct relationship” includes an exemption stating that “[a] consumer does not have a ‘direct relationship’ with a business if the purpose of their engagement is to exercise any right described under [the CCPA], or for the business to verify the consumer’s identity.”<sup>11</sup> It is not clear if this exemption only relates to the identity verification conducted in connection with a consumer exercising the consumer’s rights under the law, or if it should be read more broadly as a general exemption for identity verification purposes. Accordingly, we respectfully request that the Agency provide clarification on this ambiguity.

#### 2. Exemptions for Fraud Prevention and Identity Verification Purposes (Sec. 7601)

In light of the points noted above, and for additional reasons explained below, we strongly encourage the Agency to include in any subsequently proposed regulations *express* exemptions for fraud prevention and identity verification data-use purposes, in addition to the exemptions indirectly referenced in the CCPA.

Fraud prevention and identity verification services are critically important to and an integral component of today’s online economy.

In order to operate correctly, these fraud prevention and identity verification services rely on data collected from a variety of sources — including data from consumers’ devices and other online credentials, as well as from other third-party sources. Without exemptions protecting this type of use, companies that deliver these crucial services would be erroneously considered to be data brokers and, given the broad right to delete under the Delete Act, may no longer have access to the data required to properly provide such services. This could significantly undermine consumer fraud protection efforts nationwide.

Accordingly, we respectfully request that the Agency add an additional exemption to Section 7601, stating that the term “data broker” does not include “*an entity to the extent that it collects, sells or uses the personal information for the purpose of protecting against malicious, deceptive, fraudulent or illegal activity or for an entity’s legitimate business interests, such as identity verification and fraud prevention.*”

We appreciate the Agency’s work on the proposed regulations, and we appreciate the opportunity to provide these comments on the proposed regulations.

Sincerely,  
Anonymous

<sup>11</sup> Proposed Regulations § 7601(a) (emphasis added).

---

**From:** Jose Torres [REDACTED]  
**Sent:** Tuesday, August 20, 2024 4:03 PM  
**To:** Regulations@CPPA  
**Cc:** Dylan Hoffman; Andrea Deveau; Jason Schmelzer  
**Subject:** TechNet Public Comments on Data Broker Registration Regulations  
**Attachments:** TechNet Rulemaking Comments on Data Broker Registry 8-20-24.pdf

---

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Good afternoon,

On behalf of TechNet we are submitting our written comments on the proposed Data Broker Registration Regulations. If there are any questions or concerns, please feel free to contact us.

Best,

Jose Torres, MPA  
Deputy Executive Director | California & the Southwest  
TechNet | The Voice of the Innovation Economy

Twitter: [REDACTED]





**TECHNET**  
THE VOICE OF THE  
INNOVATION ECONOMY

TechNet Southwest | Telephone 505.402.5738  
915 L Street, Suite 1270, Sacramento, CA 95814  
www.technet.org | [REDACTED]

August 20, 2024

California Privacy Protection Agency  
Attn: Elizabeth Allen  
2101 Arena Blvd.  
Sacramento, CA 95834

**Re: COMMENTS ON PROPOSED RULEMAKING: DATA BROKER  
REGISTRATION**

Dear Board Members,

TechNet appreciates the opportunity to provide the California Privacy Protection Agency ("CPPA/the Agency") comments on its Proposed Rulemaking pertaining to the DELETE Act and data broker registry. We believe these comments will help to enhance interoperability across state lines for compliance purposes.

TechNet is the national, bipartisan network of innovation economy CEOs and senior executives. Our diverse membership includes dynamic American businesses ranging from revolutionary start-ups to some of the most recognizable companies in the world. TechNet represents over 4.4 million employees and countless customers in the fields of information technology, e-commerce, sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

Current law (1798.99.80) defines a "data broker" as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. While we appreciate the proposed changes to this definition that clarify what a "direct relationship" is, we are concerned that the Agency has unnecessarily expanded the definition of "data broker" in a manner that significantly exceeds the scope of the Agency and goes beyond its regulatory authority. By adding the statement that "[a] business is still a data broker if it has a direct relationship with a consumer but also sells personal information about the consumer that the business did not collect directly from the consumer," the regulations explicitly contradict the statutory language and aim to ensnare numerous businesses that do not meet the definition of "data broker."

Additionally, the Agency's determination that "three years was a reasonable time limit for a direct relationship" is arbitrary and capricious. While we agree that an indefinite period could run contrary to consumer expectations, the Agency fails to provide any evidence or basis in law for its conclusion beyond a statement of belief.

The Agency also states that it developed the proposed regulations to address obstacles and common questions that arose for data brokers. However, instead of

ensuring that those meeting the definition of data broker provide "accurate and adequate information," the Agency will proliferate the number of businesses defined as "data brokers." The policy rationale during the passage of the data broker registry by AB 1202 (Chau, Chapter 753, Statutes of 2019) was to ensure greater transparency for consumers who wanted to initiate their consumer rights provided under the CCPA but who lacked contact information for businesses with whom they did not have an account. However, the plain language of the statute indicates that the purpose is focus on entities with whom the consumer *does not have a direct relationship*. By attempting to claim that a business may be a data broker if it has a direct relationship with the consumer is a clear diversion from the law. If, as the Agency states, that "[a] core purpose of SB 362 is to provide consumers with a list of businesses that may be collecting and selling their personal information without their knowledge," then it should recognize that other businesses are already subject to CCPA requirements to disclose to consumers information regarding the data that they collect, how it is shared or sold, and the opportunity to opt-out from the sale of that data, among other things.

We propose the removal of the last sentence of 7601(a) and recommend the Agency work with stakeholders to better define "direct relationship."

We appreciate your consideration. If you have any questions regarding our comments, please contact Dylan Hoffman at [REDACTED]

Sincerely,

[REDACTED]

Dylan Hoffman  
Executive Director for California and the Southwest  
TechNet

---

**From:** Lucy Chinkezian [REDACTED]  
**Sent:** Tuesday, August 20, 2024 4:39 PM  
**To:** Regulations@CPPA  
**Cc:** **Kyla** Christoffersen Powell  
**Subject:** Public Comment on Data Broker Registration Regulations - OAC  
**Attachments:** CJAC Comments on CPPA Rulemaking 8-20-24.pdf

---

**This Message Is From an External Sender**

**WARNING:**This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

---

**Report Suspicious**

---

Dear Elizabeth:

Please find attached public comment on the data broker registration regulations by the Civil Justice Association of California.

Lucy Chinkezian

Counsel

Mobile

| [www.cjac.org](http://www.cjac.org)

**E** !!!!!!!J!CE





**CIVIL JUSTICE**  
ASSOCIATION OF CALIFORNIA

August 20, 2024

*Sent via email*  
regulations@coppa.ca.gov

California Privacy Protection Agency  
Attn. Elizabeth Allen  
2101 Arena Blvd.  
Sacramento, CA 95834

Re: Comments by the Civil Justice Association of California on Proposed  
Rulemaking – Data Broker Registration

Dear California Privacy Protection Agency Board:

Thank you for the opportunity to provide comments on the California Privacy Protection Agency's proposed rulemaking regarding data brokers. Founded in 1979, the Civil Justice Association of California (CJAC) is the only statewide association dedicated solely to improving California's civil liability system, in the legislature, the regulatory arena, and the courts. Our membership base consists of businesses and associations from a broad cross-section of California industries.

We write to respectfully oppose the significant expansion in the proposed regulations of California's existing statutory definition of "data broker."

The Delete Act defines "data brokers" to mean a business that knowingly collects and sells to third parties the personal information of consumers with whom the business does not have a "direct relationship." The Act does not define "direct relationship."

The proposed regulations impose a definition of "direct relationship" to now mean where "a consumer intentionally interacts with a business for the purpose of obtaining information about, accessing, purchasing, using, or requesting the business's products or services within the preceding three years." This proposed definition is vague and overly broad and will create uncertainty around which entities are Data Brokers. This could result in capturing entities that would not otherwise qualify as data brokers under the statute and the regulation's authority.

The Delete Act authorizes the CPPA to issue regulations solely to "implement and administer" the act. Changing this definition and in turn the scope of the law

exceeds that authorization. Any expansion of the definition of data broker should be done through legislation and not regulation.

We therefore request the CPPA limit the definition of "data broker" to the confines of the statute.

Thank you for your consideration, and we are happy to address any questions you have.

Respectfully submitted,

A solid black rectangular redaction box covering the signature area.

Lucy Chinkezian  
Counsel