Section 7001(g) – "Behavioral Advertising"

CCPA's regulations are limited to "cross-context behavioral advertising" (advertising using information collected over time across unaffiliated or third-party sites) rather than behavioral advertising generally.[2] CPPA should preserve this limitation rather than institute a regulation that could encompass virtually any data used in personalized ads. This term covers activity well beyond the intended scope of CCPA and most other consumer privacy laws– i.e. cases in which a significant decision about a consumer is made.[3]

When a business uses an ad to promote a product or service to consumers, the ad itself does not make decisions about the consumer. Instead, the business running the ad makes the underlying decisions, defining the ad's objective and desired audience. Algorithms may then take those inputs and determine which environments the ad would fare best in. The only automated decision involves who might see an ad, which does not involve a sensitive decision regarding a consumer.

Additionally, the proposed definition would include ads based on both third-party and first-party sources, which would have massive downstream economic consequences for the millions of businesses, particularly small and medium-sized businesses, that rely on digital ad platforms.

Section 7001(gg) – "Physical or Biological Profiling"

This definition is overly broad and could encompass virtually any use of data about the body—even data not collected from the body itself. For instance, the phrase "Depicts or describes their physical or biological characteristics" could include any description about someone's outwardly observable characteristics– height, eye color, handedness, etc.– even if no measuring device was used in these observations. Manually entering someone's height in a spreadsheet after looking at them could fall under this definition. Similarly, the phrase "Measurements of or relating to their body" could include any observable characteristic of a person, such as a clothing size range.

Section 7001(ll) – "Publicly Accessible Place"

The California Penal Code already prohibits the invasion of a person's privacy by using cameras in places where individuals share a reasonable expectation of privacy.[4] This definition should only include as examples places that present discrete privacy or consumer protection issues, or reveal sensitive info. Medical clinics, hospitals, airports, public wi-fi hotspots, workplaces, educational institutions, government buildings would fall into this category.

---

[2] California Consumer Privacy Act, Cal. Civ. Code § § 1798.140(e)(6), 1798.140(k), 1798.140(ah), 1798.185(a)(18)(A)(vi)(III) (2018).
[3] *See, e.g.*, Connecticut Data Privacy Act, Conn. Gen. Stat. § 42-515(30); Consumer Data Protection Act, Va. Code Ann. § 59.1–575 (2023); Texas Data Privacy and Security Act, Tex. Bus. & Com. Code § 541.001(24) (2024).
[4] *See, e.g.*, Cal. Penal Code § 647(j)(3)(A).

Section 7001(ccc)(4) – "Sensitive Personal Information"

Consumer privacy laws generally distinguish between users of a service who are over and under 13 years of age, rather than 16.[5] CCIA recommends adhering to that approach here. For minors over the age of 13, businesses should be able to design age-appropriate experiences tailored to their specific customer base.

Section 7001(fff) – "Train Automated Decisionmaking Technology or Artificial Intelligence"

Fine-tuning should be excluded from this definition, as the proposed Rules should regulate consumer-facing uses of ADMT, not companies' back-end internal operations.

ARTICLE 5 – VERIFICATION OF REQUESTS

Section 7060(b) – Opt-Out Requests

This Section should clarify that businesses must honor *verifiable* requests. Doing so would make this section consistent with language in the statute to facilitate verification tools that ensure user's actual preferences are applied.

ARTICLE 9 – CYBERSECURITY AUDITS

Section 7120(b)(2) – Thresholds

The proposed text creates cybersecurity audit obligations that are broader than other industry standard cyber audits. Under this Rule, any business that is subject to CCPA would also also be a business whose processing presents a significant risk to consumers' security. Every business that is subject to CCPA would have to hire an independent auditor to audit their risk assessments annually. This Section should be revised to align with the activities defined as presenting a significant risk in Article 10, Section 7150.

Section 7121(b) – Timing Requirements

This requirement should be removed, as it is unnecessarily burdensome to require businesses to repeat the lengthy risk assessment process without any significant changes in their practices, and there is no tangible benefit to consumers from forcing businesses to repeat the same process they have already completed.

[5] *See, e.g.*, Connecticut Data Privacy Act, Conn. Gen. Stat. § 42-515(38); Consumer Data Protection Act, Va. Code Ann. § 59.1–575 (2023); Texas Data Privacy and Security Act, Tex. Bus. & Com. Code § 541.001(29)(C) (2024) (each defining "sensitive data" to include "the personal data collected from a known child," i.e. "any natural person under 13 years of age," but making no distinction between users over and under 16 when defining "sensitive data.").

ARTICLE 10 – RISK ASSESSMENTS

Section 7150(b)(3)(A) – Significant Decision

As noted above, all other state laws that define "profiling" do so in the context of a legally significant decision concerning the individual profiled, such as providing financial or lending services, housing, insurance, criminal justice, employment opportunities, etc.[6] Requiring risk assessments for *all* profiling is an untenable restraint– CPPA should instead require risk assessments only when a significant decision *will* be made using the profile, not merely when one *could* be made.

However, several terms used in this Section impose burdensome requirements on businesses for activities whose impact on consumers is merely speculative. It is unclear when a consumer will have "access to" the above services beyond the "provision or denial" of those services. Similarly, "compensation" is too vague a category to warrant imposing a lengthy risk assessment– such assessments should only be required when actual employment opportunities are at stake.

Section 7150(b)(3)(B) – Extensive Profiling

As noted above, risk assessments should be required only when a legally significant decision will be made using a consumer's profile. It is unclear what extra privacy protection the "extensive profiling" framework grants consumers. The "work or educational profiling" requirements in Section 7150(b)(3)(B)(i), for example, seem to merely duplicate Section 7150(b)(3)(A)'s requirement to perform risk assessments when using ADMT for significant work and education decisions.

Moreover, this Section contains provisions that likely exceed the California Consumer Privacy Act's scope. The CCPA explicitly exempts "publicly available information."[7] Consumers in a given public space have deliberately chosen not to shield themselves from specific audiences, and have no reasonable expectation of privacy. The CCPA is clear that requirements for businesses, processors, and contractors, including creating risk assessments, do not apply to publicly available information, which includes information collected and processed from observation of public spaces.[8] Additionally, this Section requires risk assessments for *all* behavioral advertising, not just behavioral advertising directed at California consumers, again

---

[6] *See supra* note 3 and accompanying text.
[7] California Consumer Privacy Act, Cal. Civ. Code § 1798.140(v)(2)(A) (2018) ("'Personal information' does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern").
[8] *Id.* § 1798.185(a)(14) (directing the California Attorney General to issue "regulations requiring businesses whose processing of consumers' *personal information* presents significant risk to consumers' privacy or security, to... Submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of *personal information*" (emphasis added). As noted above, the CCPA excludes publicly available information from the definition of "personal information").

exceeding the CCPA's scope. A better approach would be to require risk assessments for cross-contextual behavioral advertising, which avoids requiring assessments in cases where no consumer data is being shared with third parties.

Because the requirements in this Section all either duplicate Section 7150(b)(3)(A) requirements or exceed the CCPA's scope, CCIA recommends striking 7150(b)(3)(B) and requiring risk assessments when ADMT is used to make legally significant decisions about a California consumer.

Section 7150(b)(4) – AI / ADMT Training

Since training a model does not involve decisions impacting specific consumers, it should not be considered ADMT and should not fall within the Rules' scope. The Rules aim to cover certain high-risk AI and ADMT applications and their use in making significant decisions regarding consumers. However, as written, these Rules would also cover back-end *developing* tools that use low-risk processing merely because they *might* one day be used for significant consumer decisions. Subjecting such back-end development models to these rules is unnecessarily burdensome, since by definition it would not enhance consumer privacy. Many if not all models "could" be used to make a significant decision about consumers, but unless they are actually used for such decisions, there is no upside to extending these requirements to such models.

Because of this lack of upside, CCIA recommends striking Section 7150(b)(4). CCPA is designed to alleviate the privacy risks associated with processing personal data. The statute and rules already allow consumers to opt out of the sale or sharing of their personal information, and to limit its use and disclosure.[9] The CPPA should not require risk assessments for AI training that is by definition not tied to a consumer privacy risk. No other state privacy framework or AI law considers model training a high-risk decision. Moreover, California recently passed AB 2013, putting disclosure requirements on data.

Section 7154 – Prohibition Against Processing If Risks to Consumers' Privacy Outweighs Benefits

This Section would prohibit processing for covered activities "if the risks to consumers' privacy outweigh the benefits to the consumer, the business, other stakeholders, and the public from the processing." This is an extremely broad prohibition, far exceeding other AI regulations in scope. The EU AI Act, for instance, limits bans to very specific uses, such as subliminal messaging or facial recognition.[10] CCIA recommends instead prohibiting processing that would cause substantial harm to consumers that (a) is not reasonably avoidable, and (b) is not outweighed by benefit to consumers. This formulation would avoid penalizing companies for processing decisions that do not materially affect consumers, keep the rule within CCPA's scope, and keep the focus on actual harms rather than hypothetical risks.

[9] *See id.* § § 1798.120–1798.121.
[10] *See* Artificial Intelligence Act, 2024 O.J. (L 1689), Art. 5, § 1.

Section 7156 – Conducting Risk Assessments for a Comparable Set of Processing Activities or in Compliance with Other Laws or Regulations

CCIA recommends revising the rules governing "risk assessments" to align with the data protection assessment requirements in other states. Colorado, for example, requires data protection assessments for (1) processing personal data for targeted advertising (defined as equivalent to California's definition for cross-context behavioral advertising, not behavioral advertising) and profiling if the profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial or physical injury to consumers; (iii) physical or other intrusion on the solitude, seclusion, or private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or (iv) other substantial injury; (2) selling personal data; and (3) processing sensitive data.[11]

Additionally, other state privacy laws require risk assessments only when "sensitive data" is processed (e.g. precise geolocation data rather than all geolocation, or profiling resulting in specific consumer harms, rather than profiling in general).[12] The draft rules impose further unnecessary requirements, allowing a company to forgo a risk assessment only if the other "risk assessment" created to comply with another law or regulation covers a "comparable set of processing activities," i.e. processing activities that "present similar risks to consumers' privacy." However, until a business conducts its risk assessment, it would not know which activities present similar risks, undercutting the purpose of this provision.

Section 7157(a) – Proactive Submissions

CCIA recommends striking this section. Requiring proactive submissions of risk assessment materials is unprecedented, and given the in-depth risk assessment requirements, this could prove extremely burdensome for businesses with no corresponding upside to the consumer. If such a requirement does remain, the 10-day window should be significantly extended, as businesses cannot respond meaningfully to these requests in such a short time. After a company first submits its risk assessment materials, the obligations in Section 7157(d) should govern.

Section 7157(b) – Risk Assessment Materials to be Submitted

The proposed Rules require companies to provide CCPA with annual abridged risk assessments. Routine submission when practices have not changed is unduly burdensome, inconsistent with other state privacy laws. CCIA recognizes the CPRA mandate requiring companies to submit risk assessments at regular intervals, but there exists room for a more flexible approach within this mandate. For instance, the statute does not preclude CPPA from defining the requirements for a risk assessment and the requirements for submission

[11] Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1309(2)(a) (2023).
[12] *See, e.g.*, Texas Data Privacy and Security Act, Tex. Bus. & Com. Code § 541.105(a) (2024).

separately. Doing so would allow the CPPA to focus on assessments for high-risk activities such as selling sensitive data.

Furthermore, since most employment-related decisions are confidential and not available to competitors, CCIA recommends an exception such that businesses are not required to submit information that is confidential business or trade secret information.

ARTICLE 11 – AUTOMATED DECISIONMAKING TECHNOLOGY

Section 7200(a)(1) – Significant Decision

CCIA recommends the same revisions to this provision as to Section 7150(b)(3)(A), for the reasons described in the Section 7150(b)(3)(A) comments.

Section 7200(a)(2) – Extensive Profiling

CCIA recommends striking this provision for the same reasons as the above recommendation to strike Section 7150(b)(3)(B).

Section 7200(a)(3) – AI / ADMT Training

CCIA recommends striking this provision for the same reasons as the above recommendation to strike Section 7150(b)(4).

Section 7220(a) – Pre-Use Notice Requirements

CCPA does not allow regulations of pre-use notice of ADMT—instead, CCPA § 1798.185 calls for regulations "governing access and opt-out rights" regarding ADMT.[13] The access right covers the required information from businesses about ADMT use. CPPA should therefore not issue rules on pre-use notice, or at minimum, limit pre-use notice requirements to cases where ADMT use is already subject to access and opt-out rights. Should one of these customer rights not apply (e.g., relying on a security or fraud prevention exception), then businesses should not need to post this notice. In essence, Section 7220(a) should apply subject to the exceptions in Sections 7221(b) and 7222(a)(1). Forcing businesses to disclose how they use ADMT to perform the specified functions risks undermining the security of consumers and businesses, and requirements to make such disclosures should be minimized.

Section 7220(c)(1) – Plain Language Requirement

CCIA recommends removing the explicit prohibition on using the phrase "to improve our services," as this language can serve as part of a legitimate description of businesses' use of ADMT.

Section 7220(c)(5) – Explainability

CCIA recommends striking this provision as it is effectively an explainability requirement. Many complex AI models (which tend to be the most useful ones) are not yet fully explainable. CPPA

[13] California Consumer Privacy Act, Cal. Civ. Code § 1798.185(a)(15) (2018).

should consider whether California would benefit from this requirement, or whether human review and rigorous testing will better mitigate risk.

The draft rules also contradict the statute's explicit recognition that CCPA does not require businesses to disclose trade secrets.[14] The exception under 7220(c)(5)(C) is too narrow. This is particularly important in the HR context, as HR handles employee confidential data and pilots for products that should constitute confidential business/trade secret information.

Section 7221(b) – Requests to Opt-Out of ADMT: Exceptions

CCIA recommends expanding the list of exceptions in this Rule to include other back-end tasks such as conducting internal research, fixing technical errors, executing product recalls, and performing internal operations consistent with consumer expectations. Doing so would increase business's quality of service without degrading consumer privacy.

Section 7221(b)(1) – Requests to Opt-Out of ADMT: Security and Fraud Prevention

This exception should apply whenever ADMT is used solely for security and fraud prevention, regardless of whether it is "necessary" to use ADMT in such cases. Businesses should be free to use the method of security and fraud prevention that best protects their consumers without the requirement to show that ADMT was "necessary" in such cases.

Sections 7221(b)(4)-(5) – Requests to Opt-Out of ADMT: Employee Exceptions

As written, companies must conduct "an evaluation" and implement costly and burdensome "accuracy and nondiscrimination safeguards" to avail themselves of the exceptions in these Sections. Normally, employers are allowed flexibility to ensure employees are working and productive. However, enacting costly barriers to using these exceptions would inhibit employers' ability to ensure adequate staffing and productivity in their business. For instance, a company may use ADMT for customer service operations to ensure that callers are placed on hold for the minimum possible time. Moreover, "work or educational profiling" lacks a clear meaning in the proposed Rules, which refer to "extensive profiling," not "work or educational profiling."

Section 7221(i) – Requests to Opt-Out of ADMT: Single Opt-Out

The draft rules would force businesses to offer a single opt-out for all covered ADMT, although businesses may let consumers allow specific uses. Businesses should instead be required to offer opt-outs targeting the specific use cases applicable to a consumer's data. A general opt-out does not give consumers information about how a given consumer activity leads to a given ADMT use. Requiring context-specific opt-outs will give consumers more autonomy and insight regarding the use of their data.

Section 7222 – Requests to Access ADMT

[14] *Id.* § 1798.100(f).

CCPA § 1798.185 instructs the CPPA to regulate access rights with respect to business's ADMT use, and requires responses to include "meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer."[15] It does not mandate separate notice to consumers. CPPA should implement a single set of rules about how businesses must provide meaningful information about their ADMT use. Businesses should be able to provide such information in a notice rather than responses to specific requests. Consumer-specific responses are not required under the statute, are often impractical or infeasible. They can also be hard to answer without disclosing confidential information, which may harm consumers subject to significant decisions using ADMT. Consumers already have separate access rights under CCPA, allowing them to obtain any personal information companies process, including ADMT inputs and outputs containing their personal information.

Furthermore, the proposed Rules risk requiring companies to disclose their proprietary information and intellectual property (e.g. by answering a request as to which key parameters affect which outputs). CCIA recommends adding a section stating that no provision of the proposed Rules shall be construed to require disclosure of trade secrets or confidential or proprietary information about an automated system's design or use. Also, per § 1798.185(a)(3), CPPA must issue rules clarifying that companies do not have to disclose trade secrets or proprietary or confidential information.[16]

Section 7222(a) – Requests to Access ADMT: When Access Rights Apply

As in several provisions above, the rights in this Section should apply only when ADMT is used to make a significant decision. The access right lets consumers determine whether they want to exercise their opt-out right and correct any errors regarding their personal information. For other ADMT uses, such as profiling for behavioral advertising, consumers can choose to opt out regardless of how the technology works. As noted above, businesses should not need to publicly disclose confidential and/or proprietary information about their technology without any direct consumer benefit.

Sections 7222(b)(2)–(4) Requests to Access ADMT: Output for Consumers

CCIA advocates removing these sections, as the statutory language already provides for equivalent access rights, and any enforcement of these measures risks forcing companies to disclose proprietary information regarding their ADMT.

Section 7222(k) – Requests to Access ADMT: Adverse Significant Decisions

The time allotted for compliance is too small given the detailed nature of the requests. Most of the required information will be of minimal assistance to individuals, and companies will need

[15] *Id.* § 1798.185.
[16] *Id.* § 1798.185(a)(3).

to expend enormous resources keeping the required information available and using it to craft a "plain language" rendition of the ADMT use in each "adverse significant decision." CPPA should consider revising this section to simplify the process for businesses, or alternatively, to extend the compliance deadlines.

* * * * *

We appreciate CPPA's consideration of these comments. We look forward to continuing to participate in the CPPA's ongoing regulatory process, including reviewing and providing feedback on the series of proposed Rules. We hope CPPA will consider CCIA a resource as these discussions progress.

Sincerely,

Jesse Lieberfeld
Policy Counsel– Privacy, Security, and Emerging Technologies
Computer & Communications Industry Association

ATTACHMENT A

Suggested Amendments to Revised Draft Rules

This Attachment contains CCIA's suggestions for specific modifications to the Revised Draft Rules. The text below is the draft Rules text after the Department of Law's revisions. CCIA's proposed deletions are in red and proposed new language is in green.

Introduction: Enforcement of the provisions in Articles 1, 9, 10, and 11 will begin one year after the Rules' effective date.

§ 7001(f) – "Automated Decisionmaking Technology": "Automated decisionmaking technology" means any solely automated technology that processes personal information and uses computation for the primary purpose of making a solely automated significant decision about a consumer ~~to execute a decision, replace human decisionmaking, or substantially facilitate human decision making. (1) For purposes of this definition, "technology" includes software or programs, including those derived from machine learning, statistics, other data-processing techniques, or artificial intelligence. (2) For purposes of this definition, to "substantially facilitate human decisionmaking" means using the output of the technology as a key factor in a human's decisionmaking. This includes, for example, using automated decisionmaking technology to generate a score about a consumer that the human reviewer uses as a primary factor to make a significant decision about them. (3) Automated decisionmaking technology includes profiling.~~

~~***§ 7001(g) "Behavioral Advertising":***~~

~~***§ 7001(gg) "Physical or Biological Profiling":***~~

§ 7001(ll) – "Publicly Accessible Place": "Publicly accessible place" means a place that is open to or serves the public. ~~Examples of publicly accessible places include shopping malls, stores, restaurants, cafes, movie theaters, amusement parks, convention centers, stadiums, gymnasiums,~~ including hospitals, medical clinics or offices, ~~transportation depots, transit, streets, or parks~~ airports, public wi-fi hotspots, workplaces, educational institutions, or government buildings.

§ 7001(ccc)(4) – "Sensitive Personal Information": Personal information of consumers that the business has actual knowledge are less than 13 ~~16~~ years of age....*§ 7001(fff) – "Train Automated Decisionmaking Technology or Artificial Intelligence":* "Train automated decisionmaking technology or artificial intelligence" means the process through which automated decisionmaking technology or artificial intelligence discovers underlying patterns, learns a series of actions, or is taught to generate a desired output. ~~Examples of training include adjusting the parameters of an algorithm used for automated decisionmaking technology or artificial intelligence, improving the algorithm that determines how a machine-learning model learns, and iterating the datasets fed into automated decisionmaking technology or artificial intelligence.~~

§ 7060(b) – Opt-Out Requests: A business shall not require a consumer to verify their identity to make a request to opt-out of sale/sharing, or to make a request to limit, ~~or to make a request to opt-out of ADMT~~....

§ 7120(b)(2) – Thresholds: The business meets the threshold set forth in Civil Code section 1798.140, subdivision (d)(1)~~(A B)~~; ~~and or (A) Processed the personal information of 250,000 or more consumers or households in the preceding calendar year; or (B) Processed the sensitive personal information of 50,000 or more consumers in the preceding calendar year.~~

~~***§ 7121(b) – Timing Requirements:***~~

§ 7125 – Comparable Industry Standard: **(a)** A business may satisfy the obligations set forth in Sections § 7120 - § 7124 by completion of a comparable industry standard cybersecurity audit such as ISO 27001, ISO 27018, SOC 2 Type 2.

(b) A single cybersecurity audit that meets the requirements of subsection (a) may address a comparable set of processing operations that include similar activities.

§ 7150(b)(3)(A) – Significant Decision: For purposes of this Article, "significant decision" means a decision using information that is not subject to the exceptions set forth in Civil Code sections 1798.145, subdivisions I-(g), or 1798.146, subdivisions (a)(1), (4), and (5), that ~~results in access to, or~~ the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice (e.g., posting of bail bonds), employment ~~or independent contracting opportunities or compensation~~, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel).

~~***§ 7150(b)(3)(B) – Extensive Profiling:***~~

~~***§ 7150(b)(4) – AI / ADMT Training:***~~

~~***§ 7154 – Prohibition Against Processing If Risks to Consumers' Privacy Outweighs Benefits:***~~

§ 7157(a)(2) – Proactive Submissions: Annual Submission. After the business completes its first submission to the Agency as set forth in subsection (a)(1), its subsequent risk assessment materials must be submitted upon request to the Attorney General as prescribed in subsection (d).~~every calendar year to the Agency, and there must be no gap in the months covered by successive submissions of risk assessment materials ("subsequent annual submissions").~~

§ 7200(a)(1) – Significant Decision: For a significant decision concerning a consumer. For purposes of this Article, "significant decision" means a decision using information that is not subject to the exceptions set forth in Civil Code sections 1798.145, subdivisions I-(g), or 1798.146, subdivisions (a)(1), (4), and (5), that ~~results in access to, or~~ the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice (e.g., posting of bail bonds), employment ~~or independent contracting opportunities or compensation~~, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel).

~~***§ 7200(a)(2) – Extensive Profiling:***~~

~~***§ 7200(a)(3) – AI / ADMT Training:***~~

§ 7220(a) – Pre-Use Notice Requirements: A business that uses automated decisionmaking technology as set forth in section 7200, subsection (a), and subject to the exceptions in section 7221(b) and section 7222(a)(1), must provide consumers with a Pre-Use Notice.

§ 7220(c)(1) – Plain Language Requirement: A plain language explanation of the specific purpose for which the business proposes to use the automated decisionmaking technology. ~~The business must not describe the purpose in generic terms, such as "to improve our services."~~

~~***§ 7220(c)(5) – Explainability:***~~

§ 7220(e) – Timeline: The requirements set forth in this Article apply to processing activities created or generated after December 31, 2026, and are not retroactive to any processing activities created or generated before January 1, 2027.

§ 7220(f) – Trade Secret Protection: Nothing in this article shall be construed as requiring a business to disclose trade secrets.

§ 7221(b)(7) – Requests to Opt-Out of ADMT: Exceptions: The business uses the ADMT solely for one or more of the following purposes: **(A)** Conducting internal research; **(B)** Fixing technical errors; **(C)** executing product recalls; and/or **(D)** performing internal operations consistent with consumer expectations.

§ 7221(b)(1) – Requests to Opt-Out of ADMT: Security and Fraud Prevention: The business~~'s~~ uses ~~of~~ that automated decisionmaking technology ~~is necessary~~ solely to achieve~~, and is used solely for,~~ the security, fraud prevention, or safety purposes listed below…

§ 7221(b)(4)-(5) – Requests to Opt-Out of ADMT: Employee Exceptions:

~~***§ 7221(b)(6) – Requests to Opt-Out of ADMT: Behavioral Advertising and Training:***~~

§ 7221(b)(7) – Requests to Opt-Out of ADMT: Necessity Exception: The business's use of that automated decisionmaking technology is necessary to provide the online service, product, or feature requested by the consumer or the aspects of the online service, product, or feature with which the consumer actively and knowingly engages; or the business can demonstrate a compelling reason that the use of that ADMT does not pose a substantial privacy risk to consumers.

§ 7221(i) – Requests to Opt-Out of ADMT: Single Opt-Out: In responding to a request to opt-out of ADMT, a business may present the consumer with the choice to allow specific uses of automated decisionmaking technology ~~as long as the business also offers a single option to opt-out of all of the business's use of automated decisionmaking technology set forth in subsection (a)~~.

§ 7222(a) – Requests to Access ADMT: When Access Rights Apply: Consumers have a right to access ADMT when a business uses automated decisionmaking technology as set forth in section 7200, subsection~~s~~ (a)(1)~~ (2)~~. A business that uses automated decisionmaking technology for these purposes must provide a consumer with information about these uses when responding to a consumer's request to access ADMT, except as set forth in subsection (a)(1).

~~***§ 7222(b)(2)-(4) – Requests to Access ADMT: Output for Consumers:***~~

From: Pat Utz <pat@abstract.us>
Sent: Monday, January 13, 2025 3:38 PM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: PatUtzCPPA-ADMTtestimony.pdf

Dear CPPA,

My name is Patrick Utz, and I'm a California-based small business owner (co-founder & CEO, Abstract). I'd like to submit the following comment to the CPPA for their consideration during the public hearing on January 14th.

***Pat Utz**, co-founder and CEO, Abstract*
San Francisco, CA

Good morning, Chair Urban and Board Members.
My name is Patick Utz, and I'm co-founder and CEO of a San Francisco-based startup called Abstract. We use AI to help our clients understand how regulatory changes will impact their business and operations. We employ 12 people, and we're working hard to find new customers and grow.

Thank you for giving me the chance to speak today. I appreciate your efforts to protect Californians' privacy, but I'm concerned that your proposed data-collection and ADMT opt-out mandates will seriously hurt California-based tech startups like mine, along with California's broader business ecosystem. Although Abstract is only a few years old, our website gets more than 18,000 hits annually, so the new regulations would immediately impact us.

We use data- and ADMT-powered advertising and sales-engagement tools to tell the right people about our services. Our target customers are large enterprises. To sell to those enterprises, we first have to reach the appropriate decision-makers. If those people have opted out of receiving data- or ADMT-powered communications — which many may do out of frustration with the proposed pop-ups — we won't be able to tell them about our business. That will make it nearly impossible for us to grow.

Similarly, if potential customers have to navigate several confusing pop-up windows before visiting our website, they may leave before they actually find out what we do — also costing us vitally important new clients.

California's economic impact statement estimates that it will cost a "typical" business over $25,000 a year, for a decade, to make their website compliant with the new regulations. That's a lot of money to ask a business — especially a startup — to invest in making its business less capable of growing.

Again, I applaud your efforts to protect Californians' data. But I urge you to consider the proposed rules' broader implications for the state's businesses. If California makes it hard for startups to find and be found by customers, and mandates costly, potentially damaging website redesigns for startups that are succeeding, it will lose its status as a center of talent, innovation, and investment. In addition, if established California-based businesses aren't able to learn

about innovative new products and services that could improve their efficiency and profitability, they will lose their competitive edge.

I believe Californians will be better served by more balanced regulations that seek to protect consumers while minimizing damage to the state's startup and broader business communities. Thank you for considering my comments.

Sincerely,
Patrick Utz

Best,
Pat Utz
626.533.4791

CEO, Co-Founder

Public Comment on Proposed ADMT Rulemaking Actions

California Privacy Protection Agency Public Hearing
January 14, 2025

Pat Utz, co-founder and CEO, Abstract
San Francisco, CA

Good morning, Chair Urban and Board Members.

My name is Patick Utz, and I'm co-founder and CEO of a San Francisco-based startup called Abstract. We use AI to help our clients understand how regulatory changes will impact their business and operations. We employ 12 people, and we're working hard to find new customers and grow.

Thank you for giving me the chance to speak today. I appreciate your efforts to protect Californians' privacy, but I'm concerned that your proposed data-collection and ADMT opt-out mandates will seriously hurt California-based tech startups like mine, along with California's broader business ecosystem. Although Abstract is only a few years old, our website gets more than 18,000 hits annually, so the new regulations would immediately impact us.

We use data- and ADMT-powered advertising and sales-engagement tools to tell the right people about our services. Our target customers are large enterprises. To sell to those enterprises, we first have to reach the appropriate decision-makers. If those people have opted out of receiving data- or ADMT-powered communications — which many may do out of frustration with the proposed pop-ups — we won't be able to tell them about our business. That will make it nearly impossible for us to grow.

Similarly, if potential customers have to navigate several confusing pop-up windows before visiting our website, they may leave before they actually find out what we do — also costing us vitally important new clients.

California's economic impact statement estimates that it will cost a "typical" business over $25,000 a year, for a decade, to make their website compliant with the new regulations. That's a lot of money to ask a business — especially a startup — to invest in making its business *less* capable of growing.

Again, I applaud your efforts to protect Californians' data. But I urge you to consider the proposed rules' broader implications for the state's businesses. If California makes it hard for startups to find and be found by customers, and mandates costly, potentially damaging website redesigns for startups that are succeeding, it will lose its status as a center of talent, innovation, and investment. In addition, if established California-based businesses aren't able to learn about innovative new products and services that could improve their efficiency and profitability, they will lose their competitive edge.

I believe Californians will be better served by more balanced regulations that seek to protect consumers while minimizing damage to the state's startup and broader business communities.

Thank you for considering my comments.

From: Nathan Lindfors <nathan@engine.is>
Sent: Tuesday, January 14, 2025 11:42 AM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: Engine CPPA ADMT Comments.pdf

Good morning,

Please find the comments of Engine attached.

Best,
Nathan
--
Nathan Lindfors
Policy Director | Engine
Nathan@engine.is

January 14, 2025

California Privacy Protection Agency
Legal Division
2101 Arena Blvd.
Sacramento, CA 95834

VIA EMAIL

Re: Comments of Engine Advocacy on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations

Dear California Privacy Protection Agency:

Engine is a non-profit technology policy, research, and advocacy organization that bridges the gap between policymakers and startups. Engine works with government and a community of thousands of high-technology, growth-oriented startups in California and across the nation to support a policy environment conducive to technology entrepreneurship. We appreciate the agency's consideration of our comments on these proposed regulations, especially ADMT, as artificial intelligence is used, developed, and deployed by startups. Given the costs to startups, the negative implications for the state and broader national economy, and foreseeable but likely unintended consequences, we encourage the agency not to move forward with these regulations without first making significant changes to mitigate these issues.

Startups develop ADMT, but the regulations will enhance the position of larger firms.

The proposed regulations will increase burdens on startups and diminish their competitiveness to larger firms offering similar or alternative services. Startups are developing and deploying AI technologies for many socially beneficial ends, including in areas identified by the proposed regulatory text, e.g., finance, education, employment, health, and more.[1] Startups services are offered to and utilized by end consumers and customers who are businesses themselves. Moreover, the services that will fall under the ADMT regulations are the startups' main and perhaps only offering in the marketplace. As a consequence, the mechanics of the regulations will fall hardest on these burgeoning companies compared to established firms with more resources and multiple product lines.

[1] *See e.g.*, dozens of such companies, including many based in California, by visiting www.engine.is/startupseverywhere.

Considering how the regulations would work in practice reveals additional disparate costs and burdens for startups. First, the required notices, access rights, verifying consumers asking to exercise rights, and facilitation of these rights (especially when the startup is a service provider), will result in significant compliance costs compared to the resources startups have on hand. (Startups—particularly those selling to other, larger businesses—can surpass CCPA applicability thresholds when they have few employees and only tens of thousands in monthly operating budget.[2]) Further, when consumers opt-out of ADMT, firms must in practice perform the task without the use of ADMT.[3] ADMT service providers may be expected by their clients to offer this alternative. Startups will not have the capacity to do so, leading to market pressures that favor larger firms with such capacity.

The proposed regulations carry superlative costs and limited benefits.

The agency estimates that the regulations will create tens of thousands in initial costs and tens of thousands of ongoing costs for small businesses like startups.[4] The agency also acknowledges that benefits are hard to quantify. Benefits are likely overestimated,[5] and protections against discriminatory outcomes for most categories of "significant decisions" already exist in state consumer protection and federal civil rights laws. Moreover, many costs may be missing from these estimates.

Direct pecuniary costs enumerated in the estimates are not insignificant, especially compared to the resources small startups have on hand. Seed-stage startups, for example, have around $55,000 per month in resources to cover all of their expenses (salaries, R&D, marketing, etc) for one and a half to two years until they need to raise money again.[6] This means the tens of thousands in initial and ongoing costs imposed by the rules may literally shorten the life of a young company. That is bad, but the estimates should also consider the opportunity cost of those resources being redirected away from necessary startup activities like product development and customer acquisition.

These costs are not just limited to California businesses. Costs of the proposed regulations will accrue to any business or startup across the U.S. selling to (or who wants to sell to) the California

---

[2] *See* the State of the Startup Ecosystem, 5, 16-18 Engine (Apr. 2021), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/60819983b7f8be1a2a99972d/1619106194054/The+State+of+the+Startup+Ecosystem.pdf; Review of early-stage companies on data platform Crunchbase, https://www.crunchbase.com/.

[3] The proposed regulations prohibit "retaliation" for exercising opt-out rights (§7221(l)) and require that businesses enumerate "The right not to be retaliated against" in their privacy policy provided to consumers (§7011(e)(2)(H)). Not performing a requested service without the use of ADMT would likely be considered "retaliation," leaving companies to navigate impractical options.

[4] *Notice of Proposed Rulemaking (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations)*, CPPA (Nov. 22, 2024), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_notice.pdf.

[5] *E.g.*, negative externalities for consumers discussed *infra*; Michael Genest & Brad Williams, *Comments on August 2024 CPPA SRIA*, Capitol Matrix Consulting (Nov. 1, 2024), https://advocacy.calchamber.com/wp-content/uploads/2024/11/CMC_comments_on_CCPA_SRIA_11-1.pdf.

[6] *Supra* note 2.

market. These costs are not insignificant and should be accounted for, making the true economic costs of the regulations much higher than included estimates.

Another cost to California consumers and businesses is that the regulations will dissuade startups from offering or selling services to them. For example, consider an ADMT that uses data from a consumer-worn device to detect medical events (like accidental falls or cardiac events) and dispatch emergency aid if necessary. It's hard to imagine how such a product could function were a consumer of this product to opt-out of ADMT altogether. Would the company's only option to avoid running afoul of "non-retaliation" be to have a human monitoring the consumer's data 24/7 looking for falls and heart attacks? That is not practical and unlikely to be effective. And because a company cannot "retaliate," i.e., not offer the service to consumers choosing to opt-out, the company would be forced not to offer the product in the first place.

Finally the regulations are likely to produce knock-on impacts upon businesses. For example, opt-outs of profiling will diminish the ability of businesses to advertise to customers with whom they already have a relationship. Meanwhile, by increasing costs and diminishing startup competitiveness, the regulations will reduce availability and increase prices for ADMT services—negatively impacting businesses that rely on these tools.

The proposed regulations may lead to consequences contrary to CPPA goals.

Startups in AI look to industry best practices as they develop and deploy their products, including ADMTs, but adherence to some of these best practices may be undermined by the regulations. Many startups that offer ADMTs design their services to have a "human-in-the-loop," meaning a person is involved in the decisionmaking process aided by AI. Human-in-the-loop design is generally thought to carry many benefits, including for increased transparency, effectiveness, and human agency.[7] Language in the regulations—which cover ADMTs that "substantially facilitate"[8] human decisionmaking—is broad in scope and preempts (and therefore may disincent[9] use of) human-in-the loop design.

Some consumer rights created by the regulations could lead to less accurate AI products in the marketplace. For example, opt-outs of training may worsen the efficacy of ADMTs by making the pool of training data smaller and less diverse. Consider again an ADMT that uses data from a consumer-worn device to detect medical events (like accidental falls or cardiac events) and dispatch emergency aid if necessary. Such an ADMT can only be trained on real fall or cardiac data—simulated falls from actors or synthetic heartbeat data is not an alternative because it would

[7] *See, e.g.*, Ge Wang, *Humans in the Loop: The Design of Interactive AI Systems*, Stanford HAI (Oct. 20, 2019), https://hai.stanford.edu/news/humans-loop-design-interactive-ai-systems (discussing "Benefits of Human-in-the-Loop").
[8] Proposed text at §7001(f).
[9] The rules will change the choice set for impacted businesses. This especially true for resource constrained organizations (e.g., who may need to redirect human resources to facilitating opt-outs), leading to an increase in fully-automated decisionmaking rather than human-in-the-loop.

lead to inaccurate results. Reducing the training data pool through opt-outs would worsen the quality and accuracy of the ADMT and worsen health outcomes.

Finally, the ability for CPPA regulations to become enforceable with immediate effect[10] belies socially desirable goals of thoughtful and successful implementation. While parts of the regulations related to cybersecurity and risk assessments do have 24-month timelines to perform initial audits or assessments,[11] the ADMT regulations do not have any such considerations. The proposed regulations mark a sharp departure from the status quo in many ways owing to the new notices and processes to be required of businesses. Careful and meaningful compliance with the regulations, if adopted in their current form, will take considerable time and monetary resources as businesses digest the regulations, and work with legal and technical teams to craft and implement required notices and processes. These burdens will fall hardest on smaller businesses, who do not have in-house legal counsel, and who have a small team of engineers that will be pulled in to implementation (and away from critical startup activities like product development). We encourage significant changes to the regulations, not least of these should be adequate time for implementation.

* * *

We appreciate you considering our comments on the proposed regulations. We urge you to take into account the practical impacts of the proposed regulations for startups in California and beyond. As you continue weighing the proposed text, we encourage you to involve startups that stand to be negatively impacted and make significant changes ahead of proceeding with future steps of the rulemaking process.

Sincerely,

Engine

Engine Advocacy
700 Pennsylvania Ave. SE
Washington, D.C. 20003

[10] California Privacy Protection Agency v. Super. Ct., Cal. Ct. App. 3d. (2024), https://www4.courts.ca.gov/opinions/archive/C099130.PDF.
[11] *See, e.g.*, Proposed Text at §7121, §7155, §7157.

From: Zach Lilly <ZLilly@netchoice.org>
Sent: Tuesday, January 14, 2025 11:07 AM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: NetChoice CPPA NPRM Comment.pdf

To whom it may concern,

I am submitting on behalf of my organization, NetChoice, the attached document in response to the CPPA's request for public comment.

Thank you for the opportunity to participate in the process.

Best,
Zach

Zach Lilly
Deputy Director of State and Federal Affairs
zlilly@netchoice.org
425-420-8167
NetChoice

NetChoice Comments to the California Privacy Protection Agency:

Proposed Regulations on CCPA Updates: Automated Decisionmaking Technology

Zachary Lilly
Deputy Director of State & Federal Affairs

NetChoice

January 14, 2025

Introduction

NetChoice[1] is a trade association of leading e-commerce and online companies promoting the value, convenience, and choice of internet business models. Our mission is to make the internet safe for free enterprise and free expression.

We work to promote the integrity and availability of the global internet and are significantly engaged in the states, in Washington, and in international internet governance organizations.

NetChoice appreciates the opportunity to respond to the California Privacy Protection Agency's (CPPA) proposed regulations. We will focus particularly on rulemaking related to Automated Decisionmaking Technology (ADMT), as it is of particular interest to the burgeoning artificial intelligence (AI) sector and is beyond the legal scope of the CPPA's authority. While we disagree with most of the proposed regulations offered by the CPPA, we recognize the importance of this conversation and stand willing to engage with any interested parties moving forward.

Privacy is an incredibly challenging and vital area for policy making. It is important to consumers and carries with it significant trade-offs. Privacy legislation has presented such a challenge that the federal government has remained largely paralyzed even while there has been bipartisan interest to act. That is in part why the United States is currently governed by a patchwork of state-led data privacy statutes. This includes California. Before we launch into the specifics of the NPRM, NetChoice wishes to reiterate our belief that the only productive, genuinely protective path forward is a single, preemptive, federal data privacy law. Anything less invites untold layers of confusing and conflicting regulation.

Advocating for a streamlined privacy regime is not simply pro-business. Ultimately, a privacy framework is only successful if it is accessible to the consumers that rely on it. The rights or benefits that a framework bequeath to the consumer must be easy to understand and, ideally, travel with them wherever they go. Likewise, the easier for businesses of all sizes a privacy law is to comply with, the more empowered consumers actually are. A privacy labyrinth, one that this NPRM would expand, undermines the goal of improving outcomes for California consumers.

[1] The views expressed here do not necessarily represent the views of every NetChoice member company.

AI is Already Regulated

While some have called for extensive new regulations on AI, including the proposals in this NPRM, the reality is that this technology is already subject to a wide array of existing laws and regulatory frameworks. Any AI system must comply with the same rules as any other technology or business practice in its sector. This means that AI applications in healthcare are regulated by HIPAA and FDA guidelines, AI in finance is subject to FCRA and ECOA, and AI in education must adhere to FERPA. The notion that AI will inhabit some kind of lawless Wild West is simply false.

Additionally, the federal government has already made intentional lying about the time, manner, or place of an election to prevent qualified voters from voting a crime. This means the government is free to go after individuals publishing deepfakes that seek to subvert election integrity. Moreover, existing consumer protection laws, such as the FTC Act's prohibition on unfair and deceptive practices, already provide robust safeguards against AI systems that might mislead consumers or otherwise cause them harm.

To be clear, this is not to say that every conceivable AI harm is perfectly addressed by current law, or that thoughtful, targeted updates may not be warranted in certain areas. But the core frameworks for regulating the responsible development and use of AI are very much in place today. Policymakers and the public can take comfort in the fact that our existing legal structures are, by and large, well-equipped to prevent and remedy the highest-risk AI failures.

At the end of 2024, the Bipartisan House Task Force on AI (House Task Force) released a wide-ranging report.[2] This bipartisan group of legislators had been tasked by Speaker Johnson and Leader Jefferies with promoting the development of American AI while accounting for potential harms. The report is striking not simply for its bipartisan tone and substance but because of its regulatory humility. It calls for a restrained, incremental and sectoral approach to regulating AI while avoiding sweeping regulatory regimes like the one being considered here by the CPPA. We highly recommend that anyone interested in AI policymaking read the task force report in its entirety and we will address the report further in this comment.

Before rushing to pass sweeping new AI-specific regulations, we should think carefully about how they would interact with this dense, overlapping web of existing rules. The goal should be to strategically fill discrete gaps, not to create a redundant layer of AI law that could impede innovation while adding marginal protection for the public.

[2] Bipartisan House Task Force Report on Artificial Intelligence (report), December 2024

Overbroad Definitions Harm Consumers

In the NPRM, the CPPA defines ADMT as "any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking." This is, to put it plainly, a catastrophically unsophisticated definition of the types of technology that the CPPA wishes to capture under its proposed regulatory framework.

The House Task Force, in the segment of its AI report entitled "Data Privacy," calls for continued "access to privacy-enhanced data" and demands Congress act in a "technology-neutral" way."[3]

The CPPA proposes to break any sort of technologically neutral posture here. It identifies AI, particularly and peculiarly defined, as a specific target, as opposed to identifying and mitigating against specific harms. In doing so, the CPPA fails to recognize AI for what it is: a broad marketing term that encompasses many different, independent technologies. By breaking neutrality and casting a wide net, the CPPA would begin regulation of a virtually unknowable number of technologies and applications. Under the proposed definition of ADMT, an excel spreadsheet being used by a local accounting firm could rather easily qualify. Instead of protecting the privacy of California citizens, this proposed language is far more likely to burden small companies, drive more job creators out of the state, and make cutting edge AI goods and services less beneficial to consumers.

The NPRM also provides an overbroad definition for a new legal term of art: "behavioral advertising." While existing privacy legislation has dealt with the sharing of customer data across platforms or advertisers, this would be a novel attempt to restrict the use of customer data to advertise to **one's own customers**. To be clear, this appears to be an attempt to undermine, if not outright eliminate, first-party advertisement. That would mean businesses would struggle to advertise on their own sites, about their own products, to their own customers who are choosing to shop with them. Such a vague definition of "behavioral advertising" is a striking burden on commercial speech protected by the Constitution. It should be made clear that such a regulation very likely violates the First Amendment and would be ripe for challenge if enacted.

It should also be noted that such a regulation would in no way benefit California consumers. A move by the CPPA to undermine online advertising would instead harm internet users. If enacted in the extreme, and first-party advertising was genuinely impaired, many online platforms would have to be entirely reworked, likely leading to

[3] Bipartisan House Task Force Report on Artificial Intelligence, December 2024, page 38

negatively impacted services and a degraded customer experience. Even if some middle ground is struck, how is a consumer better off when a store they trust can't let them know about products or deals relevant to them?

Advertising alerts consumers to better deals, products they are interested in, and helps to make many services across the internet ecosystem affordable or lower cost. Undermining that system is a de facto tax on every single Californian. That is in addition to the reported cost of the NPRM: $3.4 billion while affecting 52,326 businesses.[4] The impact statement also recognizes that the proposed changes will make California businesses less competitive compared to out-of-state competitors and may drive some businesses out of the state.[5] Small businesses and taxpayers can't afford that type of destructive regulation.

Beyond CPPA's Authority

What is notable about much of the NPRM related to ADMT is its focus on issues peripheral to privacy. The CPPA, like any other government entity, possesses a limited scope of authority. It cannot reimagine that authority as new issues become interesting to it. This is especially true of burgeoning technologies or policy choices where the side-effects could be economically calamitous.

The attempt to regulate general computation, defined as ADMT, is straightforwardly outside the plain text of CPPA's mandate. It is hard to imagine that even the most aggressive champion of the agency would understand its authority to encompass nearly all technology and applications of those technologies from the past half century. To avoid this pitfall, the CPPA should avoid weighing in on specific technologies and, as stated previously, focus instead on particular consumer harms to privacy.

The provisions related to advertising are similarly fraught. Again, advertising is not listed in statute amongst the sort of regulations the agency is invited to construct.[6] Moreover, this type of advertising regulation is expressly at odds with the CPPA's statutory authority. The framework enacted by the California Consumer Privacy Act gave California consumers the right to opt-out of certain cross-context behavioral advertising while allowing other types of advertising, like first-party and contextual. This change would go beyond CPPA's express authority and upend a significant portion of the digital economy.

---

[4] Economic and Fiscal Impact Statement
[5] Ibid
[6] Cal. Civ. Code §1798.185

Conclusion

NetChoice remains dedicated to improving the privacy landscape for all Americans. We have consistently called for robust, comprehensive data privacy legislation at the federal level and we remain confident that such an approach remains the best option available to policymakers.

A strong privacy regime should not, however, undermine the competitiveness of small businesses, the buying power of California consumers, or diminish the innovative potential of America's free market economy. AI has been around for a long time, but many of the applications are new and will present unique challenges. Many of those challenges will be easily addressed by existing law but a few of them will require new policy solutions. We should not lose sight of the fact that AI may also be the solution to many privacy-related concerns. Hamstringing potential solutions in the name of privacy would be a disappointing, if not fitting outcome for the regulatory process.

As the legislature in California as well as the Congress in Washington continue to litigate the intersection of privacy and AI, we respectfully ask that the CPPA exercise regulatory humility and avoid some of the more onerous regulations proposed in the NPRM. Again, we appreciate the opportunity to participate in this process and are happy to discuss our concerns with you further.

From:	Dmitriy Kruglyak
To:	Regulations@CPPA
Subject:	Public Comment on CPPA regs from MarketWhiffs, Inc. (social brokerage)
Date:	Tuesday, January 14, 2025 9:15:08 AM
Attachments:	image009.jpg image010.jpg image011.jpg image012.jpg image013.jpg image014.jpg image015.png image016.png image017.png Public comments on proposed CPPA regs from MarketWhiffs, Inc. (social br....pdf

Hello,

Here are my comments. Feel free to reach out with any questions

Onwards,

Dmitriy Kruglyak

Broker-in-Charge, MarketWhiffs, Inc.
650-329-0397 | agent@kruglyak.com
https://BayAreaHomeBuyingGuide.com
DRE# 02096470 | Real Estate Gone Social

RENE	HFR	SRES	AHWD	C2EX

Book a FREE Real Estate Consultation with me!

MarketWhiffs, Inc. is a technology start-up operating as a real estate brokerage. We are preparing to launch a social platform, designed around real estate that blends common types of social functionality with real estate listings, and includes a fair amount of ADMT functionality built upon AI. This gives us a unique perspective on how CPPA may impact innovative pro-consumer startups operating in highly regulated industries

We are very concerned about the ways proposed regulations may harm innovation

Now, here are the specific comments and concerns:

1. Clarification on "Sharing" and Third-Party Analytics:

- The definition of "sharing" under the CCPA, particularly regarding its application to third-party analytics platforms like Google Analytics, requires more clarity
- The current language could be interpreted to include even basic analytics usage, where data is collected but not directly used for advertising on the business's platform.
- **Request a clearer distinction between the use of analytics data solely for internal purposes vs. cross-context behavioral advertising**. The regulations should specify what constitutes "cross-context behavioral advertising" and how it applies to platforms like Google Analytics or other tracking platforms
- The regulations need to specify how the use of de-identified or aggregated data by third party analytics platforms is considered and whether this is also considered "sharing," or whether "sharing" only applies to data that can be associated with an identifiable user
- **Request a specific carve-out or safe harbor for the use of third-party analytics** where the business does not use the collected data for its own advertising purposes and the data is not used to build profiles for advertising on other platforms. This would avoid imposing stringent compliance requirements on businesses that are simply trying to understand their audience
- **IN ADDITION WE WANT A "CARVE-OUT"/"SAFE HARBOR" FOR SHARING PERSONAL INFORMATION WITHIN THE CONTEXT OF USER INTERACTION IN A SOCIAL NETWORK (E.G. SHOWING USER'S NAME/ PHOTO IN A GROUP CHAT)**

2. Practicality of Opt-Out Mechanisms:

- The regulations should address the practicality of implementing and maintaining a "Do Not Sell or Share My Personal Information" link, as well as other required opt-out mechanisms.
- Ensure that any requirements are feasible for small and medium-sized businesses.
- **Request clarification on how to handle situations where third-party platforms update their practices and how that affects a business's compliance requirements**.
- The regulations should provide clearer instructions on how to implement opt-out preference signals and how they interact with other methods to opt out
- **Request clearer guidance on the technical specifications and standards to which opt-out signals must adhere to be considered valid**.

3. Service Provider Contracts:

- The regulations should address the limitations of enforcing compliance through contracts with third parties
- It is important to ensure that the regulations acknowledge the fact that a business has limited control over how third parties that have access to their consumer data behave, despite contractual obligations
- It should be clarified how a business should proceed if a service provider, despite the terms of the contract, violates CCPA.
- **Request guidance on standard contract language** to ensure compliance without imposing disproportionate liability for third-party actions.
- There should be a requirement for service providers to inform a business when they can no longer meet their obligations under the CCPA
- There should be a clarification about what constitutes "reasonable and appropriate steps" to ensure that the service provider is using the data as required by the contract

4. Notice at Collection:

- The regulations should offer practical guidance for providing "Notice at Collection," especially in various contexts such as website, mobile apps and connected devices.
- **Request flexible options that account for the diverse ways that businesses collect data**, including specific guidelines for providing these notices when personal information is collected over the phone or through other offline channels.
- The regulations should clarify how notices at collection should be provided when third parties are also collecting personal information on your website.
- **IN PARTICULAR WE WANT TO ENSURE ALL THE NOTICE REQUIREMENTS CAN BE FULFILLED IN A SINGLE STEP WHEN USER ACCEPTS THE TERMS OF SERVICE**

5. Data Minimization:

- The regulations should encourage the collection of only the minimum personal information necessary for a specific purpose.
- **Request that the regulations emphasize that businesses should only collect personal information that is directly related to an activity, for example, collecting an email address only if required for a particular service**.
- This should be explicitly stated to prevent the collection of unnecessary data that could trigger compliance requirements without clear business benefits.

6. Reasonable Security Measures:

- The regulations should define what constitutes "reasonable security measures" for transmitting information to consumers in response to a request to access data.
- **Request clarification on specific security protocols and standards** that a business can implement.
- The regulations should specify a minimum security standard a business must maintain when transmitting data to consumers in response to a request.
- The regulations should provide guidance on what security measures are appropriate for various sizes and types of businesses.

7. Verification of Requests:

- The regulations should clarify how a business should respond if a requestor is unable to provide the data necessary for the business to verify their request.
- **Request clearer guidance on what constitutes "reasonable" or "reasonably high" degrees of certainty when verifying a consumer's identity**, and how businesses can implement these measures without undue burden.
- The regulation should also clarify what is a reasonable time frame for implementing these verification procedures.

8. Disproportionate Effort:

- The regulations should clarify what is considered “disproportionate effort” when responding to consumer requests.
- **Request clear examples and thresholds to help businesses determine when they can legitimately claim disproportionate effort**.
- It should be made clear if the cost to the business or other measures of resources required to comply with the regulations can be considered in determination of "disproportionate effort."

9. Automated Decision Making Technology:

- **Request clarification on the definition of "automated decision making technology" and how this definition applies to specific scenarios**
- Clarification is needed on the criteria for determining what constitutes a "significant decision" concerning a consumer.
- Provide clear and specific examples for the types of business activities that fall under this definition.
- **IN PARTICULAR WE WANT A “CARVE-OUT”/”SAFE HARBOR” TO REDUCE BURDENS OF OPERATING A SIMPLE AI CHATBOT, BASED ON A COMMERCIAL LLM**

10. Cybersecurity Audits:

- The regulations should clarify what constitutes a "qualified, objective, independent professional" when conducting a cybersecurity audit.
- The regulations should also clarify what constitutes a "significant risk to consumers' security" as it pertains to the requirement for a cybersecurity audit.
- Request clarification on whether a business can rely on a third-party audit for their own cybersecurity audit requirement

11. Risk Assessments

- **Request clarification on the criteria used to determine when a business's processing of consumer personal information presents significant risk to consumers' privacy** which would trigger the requirement to conduct a risk assessment.
- Clarify if a single risk assessment can be used for similar types of processing of consumer data, or if separate risk assessments are required for each new or updated use of personal data.
- The regulations should clarify what constitutes a "material change" that would require an update to an existing risk assessment.
- **Request clarity on what criteria to use when assessing negative impacts to consumers' privacy**, as this can be highly subjective and challenging to assess objectively.
- Clarify if the business is required to maintain risk assessments even if a processing activity is discontinued, and for how long.

12. Consistency with other Laws:

- Ensure that the regulations are harmonized with other relevant privacy laws and regulations, both at the state and federal levels.
- **Request a clear articulation of how the CPPA regulations interact with other laws, to avoid creating conflicting compliance requirements**.

Grenda, Rianna@CPPA

From: White, Megan@CPPA
Sent: Tuesday, January 14, 2025 2:29 PM
To: Regulations@CPPA
Subject: FW: ATTN: PRA Coordinator - Letter from members of the California Congressional Delegation
Attachments: 25-01-14 - CPPA Proposed AI Regulation Letter SIGNED.pdf

[redacted]

[redacted]

From: Hicks, Rob <Rob.Hicks@mail.house.gov>
Sent: Tuesday, January 14, 2025 1:58 PM
To: Info@cppa <info@cppa.ca.gov>
Cc: Burns, Will <William.Burns@mail.house.gov>; Paolini, Patrick <Patrick.Paolini@mail.house.gov>; Chapinski, Connor <Connor.Chapinski@mail.house.gov>
Subject: ATTN: PRA Coordinator - Letter from members of the California Congressional Delegation

Hello,

Please see the attached letter from members of the California Congressional Delegation.

Best,
Rob Hicks
Legislative Director
Office of Congressman Jay Obernolte (CA-23)
1029 Longworth House Office Building
Washington, D.C. 20515
202-225-5861

Congress of the United States

Washington, DC 20510

Chair Urban
California Privacy Protection Agency
ATTN: PRA Coordinator
2101 Arena Blvd
Sacramento, CA 95834

January 14, 2025

Dear Chair Urban,

As Members of the California Congressional Delegation, we believe Artificial Intelligence (AI) will be the most revolutionary technology of our generation. It is poised to transform every industry and sector of our economy and bring new gains in worker productivity that will increase prosperity for all. However, like any technological advancement, AI will not come without risks, but the risks of AI will be rooted in the way humans apply this technology, not in the technology itself. These risks will be unique to each use case of AI. We believe that attempting to prematurely regulate AI in a broad manner that is not tied to the context of its use would be destructive to both California's economy and to America's global AI leadership.

That is why we believe that your recent proposed regulations to address automated decision-making technology (ADMT) would jeopardize our state and national leadership in AI. Stretching your regulatory remit to capture this specific nascent technology instead of focusing on outcomes that directly impact consumers runs contrary to your charter and will distract attention away from more direct privacy matters. To echo the words of Governor Newsom, "Safety protocols must be adopted. Proactive guardrails should be implemented, and severe consequences for bad actors must be clear and enforceable. I do not agree, however, that to keep the public safe, we must settle for a solution that is not informed by an empirical trajectory analysis of Al systems and capabilities."

Congress has been vigorously studying the issue of AI regulation during the 118th Congress. The Senate conducted nine bipartisan AI Insight Forums with a wide variety of stakeholders. The House of Representatives has recently published its own bipartisan AI Taskforce Report, which includes dozens of key findings and recommendations for how the federal government can ensure we capture the benefits of AI while mitigating its risks. A key finding of both chambers in their work is the need for incrementalism in lawmaking to address concerns with AI as they arise naturally. Congressional Committees have also been conducting their own hearings to learn how they may need to legislate on AI in an appropriately narrow scope. We expect further action in the coming 119th Congress.

There are certainly narrowly tailored issues concerning AI that the various states have the authority to address. However, by moving forward with the sweeping regulations you have proposed, you risk creating a fractured regulatory landscape between California and the rest of the country. AI is inherently an interstate commerce issue, and the broad regulation of AI in general is therefore reserved by the U.S. Constitution to Congress, not the individual states. Your actions also risk having other states take similar actions that would quickly create a

complex patchwork of state regulations that would discourage entrepreneurialism and place smaller less resourced companies at a competitive disadvantage against their larger peers. This is an outcome no one should desire.

We urge you to abandon this regulation and allow Congress and the various state legislatures to address this matter in due course.

Sincerely,

[redacted]

Jay Obernolte
Member of Congress

[redacted]

Vince Fong
Member of Congress

[redacted]

David Valadao
Member of Congress

[redacted]

Young Kim
Member of Congress

CC: Alastair Mactaggart, Vinhcent Le, Drew Liebert, Jeffrey Worthe

Grenda, Rianna@CPPA

From: Peter Goldson [redacted]
Sent: Thursday, January 23, 2025 7:58 AM
To: Regulations@CPPA
Subject: CCPA Proposed Regulations Comments
Attachments: CCPA Proposed Regualtion Comments.pdf

Attached, please find my comments to the proposed CPPA regulation..

Thank you

Comment Submission in Response to the California Privacy Protection Agency's Notice of Proposed Rulemaking

To Whom It May Concern,

I am writing to provide my comments regarding the California Privacy Protection Agency's (CPPA) Notice of Proposed Rulemaking (NPRM) concerning amendments to the existing California Consumer Privacy Act (CCPA) regulations.

Introduction

The CCPA has been instrumental in granting California residents greater control over their personal data. As a concerned citizen and stakeholder, I appreciate the efforts of the CPPA to continuously refine and improve these regulations to better protect consumer privacy.

Concerns Regarding "Significant Decisions".

While the proposed amendments are commendable, I have concerns regarding the language contain in Section 7150 discussion of processing activities that present significant risks to consumers. In particular, Subsection 3(A) identifies a "significant decision" as

> a decision using information … that results in access to, or the provision or denial of, **financial or lending services**, housing, **insurance**, education enrollment or opportunity, criminal justice (e.g., posting of bail bonds), employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel).

My concern is that the additional language in Article 12 could be read to exempt insurers who use automated decision making from the Risk Assessment requirements set forth in the proposed regulation.

While the Gramm-Leach-Bliley Act ("GLB Act") provides a baseline of data protection for consumers with respect to insurance and financial companies, it was adopted before companies could deploy large scale automated decision-making technology. Under the proposed regulation, insurers and financial services could read the regulation as permitting the use of consumer personal data, which in most instances was not collected under a privacy notice that anticipated this use, to create or be subject to automated decision making systems that would not need to undergo a risk assessment.

While it is understandable that automated decision making tools be utilized, the fact that the underlying personal data either being reviewed by the system, or that is used to train the system, is protected only by GLB Act protections, creates a situation where significant decisions involving

access to financial services or insurance is essentially unregulated because the GLB Act is silent on this issue. It should be made clear that the regulation requires Risk Assessments in the financial services and insurance context because the GLB Act does not impose its own, similar requirement.

The final language in Section 7150 should therefore clarify that all significant decisions that utilize personal data, even if "protected" by the GLB Act, is still subject to the Risk Assessment requirements of the regulation.

Conclusion

In conclusion, I commend the CPPA for its ongoing efforts to enhance consumer privacy protections through the proposed amendments to the CCPA regulations. I urge the Agency to consider the potential impact on individuals from unregulated automated decision making decisions for financial services or insurance.

Thank you for considering my comments.

Sincerely,

Peter Goldson

[redacted]

Grenda, Rianna@CPPA

From: Justine Murray <jmurray@sdchamber.org>
Sent: Tuesday, January 14, 2025 7:38 AM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance
Attachments: CPPA AI Proposed Rulemaking 01.14.25 Final.pdf

Good morning,

Please see the attached public comment regarding CPPA's proposed rulemaking from the San Diego Regional Chamber of Commerce.

Justine Murray
Executive Director of Public Affairs
San Diego Regional
Chamber of Commerce
c: [redacted]
SDChamber.org

San Diego Regional Chamber

402 West Broadway, Suite 1000
San Diego, CA 92101-3585
p: 619.544.1300
www.sdchamber.org

January 13, 2025

California Privacy Protection Agency
Attn: Legal Division – Regulations Public Comment
2101 Arena Blvd.
Sacramento, CA 95834

RE: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations

Dear California Privacy Protection Agency Board:

On behalf of the San Diego Regional Chamber of Commerce, I am writing to address our concerns regarding the proposed regulations for Automated Decisionmaking Technology (ADMT) and AI Risk Assessments. The Chamber represents over 2,200 member businesses and over 300,000 jobs, with a mission to make the San Diego region the best place to live and work. San Diego is home to some of the state and country's top tech companies, and we have significant concerns regarding the proposed draft rulemaking actions because California is a global leader in AI research, development, and deployment. Additionally, our region is poised to become a hub for AI technology, given its position as a leader in the state's innovation economy.

The CPPA's proposed regulations are not in line with the Governor's Executive Order on AI, which directs state agencies to consider how to deploy AI for the benefit of Californians while avoiding overly burdensome and confusing regulations across various state agencies. The Chamber is aware that the proposed regulations originate from a 2020 ballot measure intended to address specific privacy concerns. However, voters were assured that the measure would focus on limiting businesses from sharing personal data, providing consumers with ways to correct errors in their data, and enabling consumers to restrict the use of particularly sensitive information. Therefore, these proposed regulations stray far from this intent, creating a host of new challenges for California businesses that were not authorized by California voters.

If this rulemaking is completed as proposed, businesses and organizations using ADMT would need to provide pre-use notices to consumers, allow them to opt out, and be tasked with conducting audits of these technologies to attempt to identify risks of bias. This could require changes to existing systems and workflows and create significant and costly challenges. The economic burden of these proposed regulations is significant. California's own impact assessment predicts a $27 billion reduction in gross product and significant job losses throughout the next decade. CPPA estimates a $3.5 billion direct cost to businesses, a figure that likely underestimates the true impact. Such economic harm cannot be ignored, especially given the current challenges businesses face. In addition to corporations, small and local businesses will also face new auditing and reporting requirements that demand disclosure of internal systems' logic, outputs, and potential risks. Small businesses will be disproportionately affected, as they often lack the resources to

implement extensive compliance measures. Many may be forced to hire additional compliance staff or abandon digital tools critical to their operations, limiting their ability to compete and innovate.

Thank you for the opportunity to comment on this important matter. The Chamber respectfully opposes this proposed rulemaking as written and asks that the California Privacy Protection Agency collaborate with stakeholders to refine its approach, strengthen California's leadership in AI innovation, and support California's economy. For further discussion or questions, the Chamber encourages reaching out to Justine Murray, Executive Director of Public Affairs at the San Diego Regional Chamber of Commerce, at JMurray@sdchamber.org.

Sincerely,

Justine Murray
Executive Director of Public Affairs
San Diego Regional Chamber of Commerce

CC: Ashkan Soltani, Executive Director, CPPA

Grenda, Rianna@CPPA

From: Crenshaw, Jordan <JCrenshaw@USChamber.com>
Sent: Tuesday, January 14, 2025 2:09 PM
To: Regulations@CPPA
Cc: Richards, Michael; Overstreet, Jack
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: 250110_Comments_CCPA_CaliforniaPrivacyProtectionAgency.pdf

To Whom It May Concern:

Please find attached the U.S. Chamber of Commerce's Comments in response to the Agency's request for public comments on
CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations.

Best,

Jordan Crenshaw
Senior Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce
Direct: 202-463-5632, Cell: [redacted]

U.S. Chamber of Commerce

www.americaninnovators.com
@uschambertech

U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

January 14, 2025

California Privacy Protection Agency
Attn: Legal Division – Regulations Public Comment
2101 Arena Blvd.
Sacramento, CA 95834

Re: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations

The U.S. Chamber of Commerce ("Chamber") respectfully submits the following comments in response to the California Privacy Protection Agency's ("Agency") November 22 Notice of Proposed Rulemaking ("Proposed Rules").[1] The Chamber supports privacy protections for all Americans; however many of the Proposed Rules[2] exceed the Agency's statutory authority and its requirements, particularly those establishing requirements for privacy risk assessments and Automated Decision-making Technology ("ADMT") will be harmful to economic growth, innovation, and small businesses.

I. Introduction, Costs, and Burden on Interstate Commerce

The Chamber shares many of the same concerns as those expressed by the leading advocate and author of the California Privacy Protection Act ("CPPA" or "Act"). Agency Board Member Alastair Mactaggart stated during the Agency's November 2024 meeting that during board meetings in December 2023, March 2024, and July 2024, he "opposed these regulations" and "voice concern about their overreach, their lack of privacy protection, and the high likelihood of legal challenges" to them.[3] He also added that "at this point, the scope remains unchanged. And I believe this undermines privacy rather than protecting it."[4]

Furthermore, the Chamber, the world's largest business federation which represents all sizes of business in all fifty states, expresses concerns that the Proposed Rules on Cyber Audits, Risk Assessment, and ADMT impose an undue and impermissible burden on interstate commerce. Furthermore, the costs of the Proposed

---

[1] California Privacy Protection Agency—Notice of Proposed Rulemaking (Nov. 22, 2024) *available at* https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_notice.pdf.
[2] CALIFORNIA PRIVACY PROTECTION AGENCY – PROPOSED TEXT OF REGULATIONS (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations) (Nov. 2024) *available at* https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf.
[3] California Privacy Protection Agency Board Audio Transcription of Recorded Public Comment Session at 99 lines 5-11 (Nov. 28, 2024) *available at* https://cppa.ca.gov/meetings/materials/20241108_audio_transript.pdf.
[4] *Id.*

Rules outweigh the benefits.[5] According to the State of California's own Regulatory Impact Analysis ("RIA"), the Proposed Rules will impose a $3.5 billion direct cost on businesses "subject to the CCPA."[6] In comparison, the Congressional Review Act defines a federal "major rule" as one that has "an annual effect on the [United States] economy of $100,000,000 or more."[7]

The Agency's estimated $3.5 billion cost estimate significantly underestimates the true costs of the Proposed Rule as the RIA "anticipate[s] overall costs for these rules to be comparatively low compared to the other rulemaking given many of the requirements described in the proposed regulation were already required by existing laws, such as existing requirements under the CCPA and other state privacy laws."[8]

The Proposed Rules will have an outsized and significant impact on the national economy particularly with regard to AI. Between 2013 and 2023, private investment in AI has amounted to $335.2 billion[9] with many of the leading AI developers operating in California. The Proposed Regulations are the first in the nation to define on an economywide basis that using personal information for training generative AI is a "significant risk"[10] thus subjecting the technology to novel regulations only found in the Proposed Rules. One of these novel regulations is that generative AI data processing, among other practices, is prohibited if its benefits are outweighed by risks.[11] This contrasts with the RIA's description that costs of the Proposed Rules on ADMT will be mitigated because current laws cover most of the regulated activity already. Given this reality, it is very likely the true costs of the Proposed Rules significantly exceed the $3.5 billion estimated by the Agency and will have a significant and negative impact on the national economy.

Moreover, the RIA failed to account for the costs on businesses for providing opt-out rights for a wide range of everyday systems. Additionally, the RIA fails to assess the burdens on consumers if they have to sift through and make decisions about those opt-out rights. The RIA does not consider the harm to businesses of restricting their ability to personalize advertisements and offers to their own customers. Further, it is highly unlikely the Proposed Rules' cost will impact only businesses "subject to the CCPA."

---

[5] *See e.g.* Minnesota v. Clover Leaf Creamery Co, 449 U.S. 456. 471 (1981).
[6] Standardized Regulation Impact Analysis (Oct. 2024) *available at* https://cppa.ca.gov/meetings/materials/20241004_item6_standardized_regulatory_impact_assessment.
[7] 5 U.S.C. § 804(2).
[8] *Supra* n. 6 at 57.
[9] Charted, U.S. is the private sector A.I. leader, *Axios* (July 9, 2024) *available at* https://www.axios.com/2024/07/09/us-ai-global-leader-private-sector.
[10] *Supra* n. 2 at 103.
[11] *Id.* at 114.

II. Definitions

A. Artificial Intelligence

The Agency proposes defining "Artificial Intelligence." The CPPA should remove all AI terms and requirements from the Proposed Rule altogether as they expand beyond the scope of the ADMT mandate in the CCPA. The Agency's authority does not extend to regulating AI or creating obligations related to AI, as the CCPA's section on rulemaking authority does not explicitly mention AI. The inclusion of AI into the definition of ADMT is overly broad, encompassing nearly all imaginable software.

B. Automated Decision-making Technology

The Agency's Proposed Definition of ADMT is overly broad and not sufficiently tailored to focus on high-risk tools that operate without human oversight. Additionally, a technology that "substantially facilitates human decisionmaking" is not an automated decisionmaking technology and should not be treated as such. We strongly encourage the Agency to work with federal agencies, such as NIST, as well as industry representatives and standards development groups to determine appropriate definitions and terminology.

C. Behavioral Advertising

The Agency should strike the proposed the definition of "Behavioral Advertising," a term not included in the Act. The Agency proposes to define "behavioral advertising" as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity—both across businesses, distinctly-branded websites, applications, or services, and within the business's own distinctly-branded websites, applications, or services." This would be a significant expansion of the existing statutory definitions that would encompass first-party marketing and advertising activities.

The Proposed Rules would consider companies that use automated technology to conduct behavioral advertising as engaging in "extensive profiling" subjecting them to conduct a risk-assessment. At the same time, such conduct would be deemed by the Proposed Rules as a "significant risk."

The inclusion of behavioral advertising as a category of "extensive profiling" covered by the ADMT requirements is an incoherent approach to data protection, basic internet functionality, and serving consumers. Ads themselves are not "decision makers" - they are avenues for awareness that businesses use, across many communications channels, to promote their products and services. To run an ad, an advertiser sets up their creative, objective, and desired audiences, which are all

critical aspects of ad delivery, including delivery that involves ADMT. Conceptually, this is similar to an advertiser choosing to place their ad in a sports magazine, because of their estimation of interest to the community that reads these magazines. The Proposed Rules, as a regulation originating from the state's privacy statute, should be limited to the use of ADMT to make significant decisions about an individual. Instead, Proposed Rules follow a misguided approach of equating the use of ADMT in behavioral advertising to making a significant decision about an individual.

Additionally, the use of ADMT to conduct behavioral advertising would be subject to the Proposed Rule's Section 7200 opt-out right. Given the breadth of the behavioral advertising definitions, such an all or nothing approach to an advertising opt-out would deprive the consumers of small businesses of the benefits of personalized advertising. These tools also allow those small businesses to compete with larger companies. Sixty-six percent of small businesses nationwide have stated that losing the ability to personalize advertising will harm their operations, without achieving any meaningful consumer privacy goals.[12]

Finally, the proposed definition "behavioral advertising" would restrict first-party advertising. The Proposal's inclusion in this definition of "the targeting of advertising to a consumer based on the consumer's personal information obtained from . . . the business's own distinctly-branded websites, applications, or services" goes beyond the CCPA's text, which regulates "Cross-Contextual Behavioral Advertising" and carves out first-party data.[13] This statutory carve-out is important because it provides businesses the ability to market directly to their own customers on their own properties using data they have directly collected or inferred. For example, under the Proposed Rule's definition of "behavioral advertising" a restaurant or delivery service sending a promotion based on ordering history with that company would be "extensive profiling" subject to rigorous risk assessments and potential prohibitions. The result is that consumers will be inundated with irrelevant adds to provide them less value than personalized promotions.

D. Significant Decision

Both Articles 10 and 11 of the Proposed Rules define a "significant decision." Companies that use ADMT for a "significant decision" would be subject to the Proposed Rule's risk assessments, processing prohibitions, and consumer opt-out rights. An overly broad or ambiguous definition of "significant decision" could significantly impair innovation and the offering of affordable and tailored products and services to consumers.

---

[12] U.S. Chamber of Commerce, "Empowering Small Business: The Impact of Technology on U.S. Small Business," at 25 (Sept. 2024) *available at* https://www.uschamber.com/assets/documents/Impact-of-Technology-on-Small-Business-Report-2024.pdf.

[13] Cal. Civ Code § 1798.140(k).

Both Articles would define "significant decision" to mean "a decision… that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice (e.g., posting of bail bonds), employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel)."[14]

Consistent with a plain reading of the statute, the Proposed Rules should clarify how the existing access and opt-out rights apply in the context of ADMT. There is no basis in the statute for the Agency to create its own broad definition of "significant decision."

The focus of the Proposed Rules should be on risk assessments for high-risk ADMT that result in a denial rather than on low-risk uses such as administration of services such as health care or insurance. The proposed definition of "substantial decision" does not align with existing privacy law norms that focus on decisions that have a "material legal or similarly significant effect on the *provision or denial*" of certain benefits or opportunities.[15] For this reason and to harmonize with other states, we encourage the Agency to strike "results in access to, or" from the definition of "significant decision" in Sections 7150(b)(3)(A) and 7200(a)(1).

The Proposed Rules further define "[e]mployment or independent contracting opportunities or compensation" to include the "[a]llocation or assignment of work; salaries, hourly or per-assignment compensation, incentive compensation such as bonuses, or other benefits." This definition is also overbroad and captures HR administrative activities that are necessary parts of any job and are not considered to be high risk (i.e. allocation of work, administration and setting of payrolls). The definition of "employment or independent contracting opportunities or compensation" should align with activities that are generally considered high risk, such as recruitment, hiring, and promotion.

Many "automated decisions" in the independent contractor context involve things like surfacing the opportunity to engage with a given work or "gig" opportunity (e.g., delivering a given food order or offering a specific ride). Given the control independent contractors have to accept or deny any of these one-off opportunities (in contrast to being "hired" for ongoing employment), these "automated decisions" are not "high risk" and should not be considered "significant decisions" subject to these onerous regulations.

III. Privacy Risk Assessments (Article 10)

[14] Proposed Rule at §§7150(b)(3)(A), 7200(a)(1).
[15] *See e.g.* Colo. Rev. Stat. § 6-1-1303(10)

A. When a Business Must Conduct a Risk Assessment

The Proposed Rules required companies to conduct Risk Assessments for data processing that "presents significant risk to consumer privacy."[16] Among other things, the Proposed Rule would consider significant risks to consumer privacy to include the use of ADMT to make a significant decision or for "extensive profiling." Proposed Section 7150(b)(4) also would consider generative AI training and generation of a deepfake[17] to be a significant privacy risk. For the reasons stated hereinabove, the Chamber asserts that the Agency must make the necessary changes regarding its definitions of "significant decisions" and remove "behavioral advertising" from the term "extensive profiling."

We recommend striking Proposed Section 7150(b)(4) because the risk assessment obligations on AI exceed the CCPA's statutory authority because the Act focuses on ADMT's not AI generally. Training a model is not "automated decisionmaking" in its core—because the "training" does not involve a decision that has an impact on a specific consumer—and so should be out of scope for these rules. The rules aim to cover certain high-risk AI/ADMT applications, such as when used to make a significant decision. But here, the Proposed Rules would also cover developing tools that could provide substantial low-risk processing but would still be in the scope of the rule because they could one day be used for a higher risk application.

The actual use of ADMT/AI systems for these higher-risk applications would still be covered under these rules, and so extending obligations to the training of such tools is both misplaced and unnecessary. In other words, this training category greatly expands the type of technologies that are subject to these obligations because many if not all models "could" be used to make a significant decision. This "theoretical" approach is inconsistent with other risk-based frameworks focused on automated decision-making used to make a significant decision. It is also a different issue because training a model on personal data is different from making a decision about that person (or otherwise creating any risk for them).

---

[16] Proposed Rule § 7150(a).

[17] Regulation of deepfakes is beyond the remit of this privacy rulemaking and is best left to the legislature to address. In 2024, the California legislature passed multiple laws targeting deepfakes across a number of different issues, such as election information, intimate imagery, and publicity rights. Notably, none of these laws grant the CPPA any authority to enact regulations. One of the laws, AB 2839, was promptly challenged and enjoined in federal court as raising significant constitutional concerns. Accordingly, the CPPA's regulation of deepfakes would encroach on the legislature's authority and risks undermining First Amendment principles. Moreover, the draft rules diverge from other legal frameworks in how a "deepfake" is defined, creating further risks of arbitrary and capricious regulation. Accordingly, the CPPA should refrain from attempting to address deepfakes in the regulations and instead defer to the legislature on this topic.

In summary, the Chamber reiterates the position taken by Board Member Mactaggart when he said, "So how are these regs too broad? The risk assessment regs are too broad? Well, just to provide some examples, the definition of artificial intelligence, AI, is essentially all software..."[18] For the practical reasons stated by Mr. Mactaggart as well as the lack of CCPA statutory authority to regulate AI in this manner, we urge the Agency to strike Section 7150(b)(4).

B. The Prohibitions in Sections 7154 Are Impermissibly Vague and Should be Struck.

The Proposed Rule's Section 7154 places a new and potentially unconstitutionally vague prohibition that a "business must not process personal information for any processing activity identified in section 7150, subsection (b), if the risks to consumers' privacy outweigh the benefits to the consumer, the business, other stakeholders, and the public from processing." For the following reasons, Section 7154 should be struck from the Proposed Regulations.

As drafted this prohibition effectively operates as a catchall outside the explicit obligations and requirements imposed upon business by CCPA. Importantly, the new prohibition on processing with alleged privacy risks does not follow the text of the CCPA itself. The Act gives the Commission authority to require businesses engaged in data processing with significant risks to submit risk assessments to the Agency:[19]

> 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. Nothing in this section shall require a business to divulge trade secrets.

The Proposed Rules deem a wide variety of common practices in the digital economy– regardless of whether they in fact pose any meaningful "risks to privacy of the consumer" -- to pose significant risks including data sharing and sales; processing sensitive information; automated decisionmaking in lending, housing, insurance, criminal justice, healthcare; using data for personalized advertising; as well as training and operating AI. Effectively, the agency is saying the any meaningful use of personal information, other than collection, poses a significant risk to consumer privacy and

[18] *Supra* n. 3 at 100.
[19] Cal Civ. Code § 1798.185(15(B) (emphasis added).

should be subject to risk assessments and a vague balancing test to determine the legality of core business practices in the digital economy. Such an approach will chill investment and innovation because businesses will be subject to a highly subjective and unknowable standard if the Agency second guesses whether a business's data processing practices benefits are outweighed by personal or societal risks.

According to the United States Supreme Court[20],

> It is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined. Vague laws offend several important values. First, because we assume that man is free to steer between lawful and unlawful conduct, we insist that laws give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly. Vague laws may trap the innocent by not providing fair warning. Second, if arbitrary and discriminatory enforcement is to be prevented, laws must provide explicit standards for those who apply them. A vague law impermissibly delegates basic policy matters to policemen, judges, and juries for resolution on an *ad hoc* and subjective basis, with the attendant dangers of arbitrary and discriminatory applications.

Proposed Section 7154 as drafted would violate due process for companies who have no discernible standard other than to weigh the benefits and risks of data processing practices. Further complicating this vague standard is the fact that Section 7152 requires companies to identify in a granular manner data processing benefits to consumer and expected financial profits when possible.[21] Yet, the Agency contemplates that businesses will identify privacy risks to consumers as broad and unquantifiable as chilling expression, anxiety, and stigmatization.[22]

Other so-called "privacy" risks identified by the Agency include a broad range of potential "economic harms," like "charging consumers higher prices" or "compensating consumers at lower rates." These are not "risks to privacy" in the ordinary sense of the word (which, per the CCPA, are the only types of risks the CPPA can consider). Rather, the regulation of these broad "economic harms" is well outside the CPPA's authority and properly within the purview of other regulators. If this part of the rules is not changed, the rules would give the CPPA (or the AG) the authority to shut down business activities that, in the agency or AG's judgment, pose a greater risk of "economic harm" to consumers or workers than the potential financial benefits. That is not privacy regulation – that is a potentially sweeping form of commerce, labor, and competition regulation.

---

[20] *Grayned v. City of Rockford*, 408 U.S. 104, 109 (1972).
[21] Proposed Section 7152(a)(4).
[22] *Id.* at § 7152(a)(5).

The primary purpose of a Risk Assessment should be for companies to proactively consider privacy as they build, develop, and implement their data processing practices. While the Proposed Rules in Section 7152 require companies to weigh the benefits of data processing posing a significant risk against the risks to individuals and society, Section 7154 fails to state that the Agency will not second guess the results of the Risk Assessment and use instead its own judgement to determine whether an activity should be prohibited. This is important because the Proposed Rules require businesses to conduct extensive risk and benefit analyses without any clear standards to determine whether individual or societal risks outweigh the benefits of what is pre-determined by the Agency in the Proposed Rules to be a significant risk under Section 7150(b).

As the Agency provides no clear formula for its risk assessment determinations, if two companies effectively conduct the same processing with "significant risks" yet come to different conclusions whether benefits outweigh risks, as drafted the Agency could impose blanket prohibitions on all industry that go beyond the scope of CCPA. Alternatively, under this scenario, the CCPA would be applied unequally across industry.

Without clear indication that the Agency will honor companies' conclusions in their Risk Assessments, the Proposed Rules impose on companies a requirement to establish a record for the Agency to arbitrarily prohibit legitimate processing by weighing metrics which are akin to comparing apples (i.e. economic benefits) and oranges (i.e. intangible harms like reputational risks). The Proposed Rules fail to enumerate a clear standard to determine how a data processing practice's benefits are not outweighed by individual and societal risks, particularly when there are not quantifiable metrics for many of the Agency's contemplated privacy harms. Such authority gives the Agency both legislative and enforcement authority if it chooses to replace its own judgement for what is determined by a company in its Risk Assessment.

Even if the Agency honors a business's Risk Assessment which shows benefits may be outweighed by risks, the Proposed Rules are not narrowly tailored to match the statutory text of the Act. The CCPA states that Risks Assessments should be submitted "with the goal of *restricting or* prohibiting the practice." Instead, the Agency has arbitrarily determined that most meaningful and common data practices and analytics outside of data collection are subject to outright prohibition, not mere restriction, if it believes a privacy risk has outweighed benefits. For example, some data practices could be more harmful to a more sensitive or vulnerable individual yet provide innovative insights on how to solve societal problems for that same category of sensitive or vulnerable people. Given competing interests, benefits, and risks, a data practice might be more suitable for restriction to prevent individual harm that

outright prohibition, but the Proposed Rules provide only for outright prohibition, allowing for only the most aggressive reading of the CCPA and expressly excluding the more tailored statutory option.

Alternatively, if the Agency does intend to determine on its own whether to prohibit practices with substantial risk that outweighs benefits, it should limit the considerations in Risk Assessments or provide much more granular guidance for metrics that are quantifiable and not abstract or subjective standards like chilled expression or anxiety.

Finally, the CCPA states that Risk Assessments should be submitted with the "*goal* of restricting or prohibiting the practice." Given the many difficult to compare and unquantifiable metrics as well as the competing societal, individual, business, customer-supporting, and innovation interests, the statute does not explicitly state the Agency *must* restrict or prohibit processing practices. The *goal* of Risk Assessments could be to encourage companies to voluntarily restrict or stop their own practices to protect their customers, assets, and reputation. From a government perspective, if a *goal* of the Act is to enact further legal restrictions or prohibitions on business, it would be more appropriate for the Agency to be informed by Risk Assessments to make recommendations to the California legislature for amendments to CCPA that deal with discrete risky data practices.

C. Timing and Submission of Risk Assessment to the Agency

The Agency Proposes in Section 7157(a) to require businesses to submit Risks Assessments to the Agency within 24 months of the effective date of the regulations and then every year after. No other jurisdiction in the United States requires such a proactive submission schedule.[23] To harmonize with other state laws, the Agency should require an initial impact assessment and submission upon request by the Agency or Attorney General in the context of an investigation.

Proposed Section 7157(d) would require businesses to turn over their unabridged Risk Assessments to the Agency or Attorney General within ten days. Given the broad scope of the assessments, we suggest that response time should be thirty days.

The Proposed Rules at Section 7155(a)(3) would also require companies to conduct a new risk assessment "immediately" upon a "material change" to a processing activity. We would encourage the Agency to require this new assessment to be completed done within a "reasonable time" instead.

[23] *See e.g.* Colorado Revised Statutes § 6-1-1309.

We also urge the Agency to allow for interoperability of other privacy impact assessment requirements in other states. For example, if a submission of a company's Privacy Impact Assessment under the Colorado Privacy Act adequately addresses California's requirements, companies should not be required to complete and submit duplicative assessments.

IV. Cybersecurity Audits (Article 9)

A. Article 9 Generally

Article 9[24] of the Proposed Rules would require businesses that process personal information in such a way that poses a "significant risk" to an individual's privacy or security to conduct and submit an annual cybersecurity audit. The cybersecurity requirements proposed in sections 7120 through 7124 represent a bold departure from standard cybersecurity requirements currently employed throughout the U.S. industry landscape and will impose a possibly insurmountable compliance burden on businesses with operations in California, particularly small and medium-sized businesses. At a foundational level, the Chamber believes that any proposed cybersecurity law or regulation must be harmonized with existing regulations to the greatest extent possible and be based on risk.

Furthermore, we question the statutory authority of the Agency to impose specific cybersecurity requirements and practices on businesses. Indeed, Section 1798.185(a)(14)(A) of the CCPA allows the Agency to issue regulations exclusively with respect to an audit:

> *"Perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent. The factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities."*[25]

This language provides the Agency authority to require cybersecurity audits with a defined scope, but it does *not* provide the Agency any authority to require a business to establish specific security processes.

That being stated, the following represent comments, questions, and suggested changes to Sections 7120 through 7124 of the Agency's proposed regulations.

B. Section 7120 – Requirement to Complete a Cybersecurity Audit

[24] Supra n.2 at 91.

[25] https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Section 7120 introduces the annual cybersecurity audit requirement and outlines the applicability threshold under which businesses must operate. As written, the proposed regulations suppose that any business that processes personal information poses a significant risk to consumer security. This threshold is too low, both in terms of the breadth of businesses as well as the type of activities deemed a "significant risk." The Agency should instead focus its audit requirements on activities that pose significant risk to the most sensitive data. At the very least, the Agency should refer to its own text in Article 10, Section 7150, which acknowledges the following as presenting a significant risk: selling or sharing personal information, processing sensitive personal information, using ADMT to make significant decisions, or using personal information to train ADMT and/or artificial intelligence[26]. While still broad, this language would at least provide a degree of clarity to businesses considering the applicability of the proposed regulations.

C. Timing for Requirements for Cybersecurity Audits

Section 7122 requires that the cybersecurity audits outlined in the proposed regulations occur no more than every 12 months following a business' initial audit[27]. This requirement is inconsistent with all other U.S. privacy laws regarding risk assessment and Data Protection Impact Assessments (DPIA) and should be amended to a less frequent occurrence, such as once every three years. The Agency should also consider allowing businesses to complete an initial audit and subsequently certify that said audit remains valid going forward.

D. Thoroughness and Independence of Cybersecurity Audits

In Section 7122, the proposed regulations outline requirements for businesses to ensure that cybersecurity audits are both thorough and independent. Many of these requirements, particularly those found in Section 7122(a)[28], conflict with existing federal cybersecurity requirements and guidelines, including requirements related to the nature, independence, and characteristics of internal auditors; the requirement that the audit be reported directly to the board; the requirement that the board have direct responsibility over the auditor's performance and compensation; requiring employee training after every data breach; and other prescriptive requirements. In general, we request that requirements concerning the use of an internal auditor be more flexible and harmonized with existing regulations.

Similarly, the prescriptive requirements for the cybersecurity audits outlined in Section 7122(e) should be harmonized with existing audit requirements and standards,

[26] *Id.* at 103.
[27] *Id.* at 91.
[28] *Id.* at 92.

such as the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF)[29], international frameworks, and other existing cybersecurity standards and requirements already utilized by and familiar to the business sector. If a business reasonably conforms with these standards, then they should be considered in compliance with the Agency's requirements.

An issue of particular concern for businesses are the requirements involving a given business' board of directors, such as language in Section 7122(i)[30] and Section 7124(c)[31] that require a member of a business' board of directors to sign a statement certifying specific facts of the audit as outlined in Section 7123. The Chamber asserts that a board should provide guidance on the organization's strategic direction and plans, monitor management's performance in implementing such plans, and account for the institution's risk appetite, resources, and controls. However, a board of directors should *not* be expected to serve as technical cybersecurity risk management practitioners themselves. Therefore, the Agency should revise the proposed governance requirements to recognize the role that boards play in a business' structure. The board should be allowed to focus on the overall enterprise risk management of the business and leave in-depth reviews and approvals of cybersecurity policies for the cybersecurity experts who possess the capacity to manage those policies daily. This is also true for the proposed requirement to have the board evaluate performance and set the compensation for an internal auditor.

E. Scope of Cybersecurity Audit

Section 7123 describes the various aspects of the cybersecurity audits and includes specific requirements for businesses seeking to comply with the proposed regulations.[32] The details outlined in this section are more extensive and prescriptive than any other government requirements at the federal or state level and are not based on an existing specific cybersecurity framework, nor do they refer to specific standards. Again, the requirements outlined in Section 7123 must be harmonized with existing federal standards to ensure as little a burden as possible for businesses already employing sufficient cybersecurity practices.

In Section 7123(b)[33], the Agency lists the cybersecurity components and requirements that businesses must address and employ to comply with the proposed regulations. As stated above, the Chamber questions the statutory authority of the Agency to require specific cybersecurity practices for businesses. Even with the

---

[29] NIST Cybersecurity Framework (Feb. 26, 2024) *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.
[30] *Supra* n. 2 at 94.
[31] *Id.* at 102.
[32] *Id.* at 94.
[33] *Id.*

appropriate statutory mandate, the practice of basing regulation around specific cybersecurity requirements is an inappropriate method of regulation and generally unproductive. Further, such a method neglects to acknowledge the ever-changing nature of the current cybersecurity environment as well as the need for businesses to have the flexibility to protect digital infrastructure in the most appropriate manner. Should the Agency continue down this route, it should at least realign these requirements with existing federal cybersecurity frameworks and ensure that this program remains based on risk, rather than prescriptive, requirement-based regulation.

Additionally, it is worth noting that many of the listed cybersecurity requirements do not appear to be limited to the protection of personal data. For example, the requirements contained in Section 7123(b)(2)(F)[34] deal with the secure configuration of hardware or software. The Agency must clarify that these requirements are limited to situations in which personal data is involved. Without such language, these requirements could be read to require an enterprise-wide assessment and retooling, which would be needlessly complex and burdensome as well as outside the statutory purview of the Agency.

Further, in Section 7123(b)(2)(Q)[35], the Agency defines "security incident" as:

> *"...an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of the business's information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of the business's cybersecurity program. Unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information is a security incident."* [36]

This definition is problematic for multiple reasons. For one, the wording "or potentially jeopardizes" would require compliance over an incident that has not yet occurred, which is unnecessarily vague and will demand thorough analysis of any potential threat that has yet to materialize. Furthermore, the phrase "...or availability of a business's information systems or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of the business's cybersecurity program..." could be read to expand the proposed regulations to a business' entire information system, which goes well beyond the Agency's statutory authority, perceived or otherwise. This definition must be amended to clarify

[34] *Id.* at 97.
[35] *Id.* at 99.
[36] *Id.*

that only information systems dealing with sensitive personal data are covered in this language as well as remove any vagueness related to the types of incidents against which businesses must protect. As an alternative, the Chamber suggests using the "breach of the security of the system" definition contained in California's general breach notification statute (1798.82(g)), which reads:

> *(g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.*[37]

Section 7123(c)(4) requires businesses to include the *"...title(s) of the qualified individuals responsible for the business' cybersecurity program."* [38] For larger organizations, this requirement could include hundreds of employees. This requirement should be focused on those within a business who are "primarily" responsible for a business' cybersecurity program.

Section 7123(e) states:

> *If the business was required to notify any agency with jurisdiction over privacy laws or other data processing authority in California, other states, territories, or countries of unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information, the cybersecurity audit must include a sample copy of the notification(s), excluding any personal information; or a description of the required notification(s) as well as the date(s) and details of the activity that gave rise to the required notification(s) and any related remediation measures taken by the business.*[39]

As written, this language would require a business with operations in California to include in the cybersecurity audit any personal data breach occurring in any jurisdiction globally, assuming the jurisdiction required a breach notification. This requirement exists far outside the Agency's purview and represents a huge expansion of state authority. The Agency lacks the authority to regulate activities wholly outside of California. Further, in the case

[37] Cal. Civ. Code § 1798.82(g).
[38] *Supra* n. 2 at 100.
[39] *Id.* at 101.

of some financial institutions, visitorial rights restrict the ability of states to inspect, examine, and generally regulate said institutions in this manner. As such, we strongly urge that this requirement be removed.

A consistent request made both in this comment submission and by industry in general is the harmonization and alignment of cybersecurity regulations. To that end, the Agency provides some flexibility with existing cybersecurity regulations in Section 7123(f)[40] where it clarifies that a business is "not required to complete a duplicative cybersecurity audit" if the audit "meets all of the requirements of this article." While the intention of this language is generally appreciated, it does not go far enough and, in certain cases, will inadvertently create additional burdens for businesses seeking compliance. For example, the language requires that businesses "specifically explain how the [external] cybersecurity audit…meets all of the requirements set forth in this article." Instead of avoiding duplication, this language adds further burdens to businesses executing cybersecurity measures while already managing a duplicative, overlapping, and at times contradictory regulatory framework.

V. Automated Decision-making Technology (Article 11)

A. Article 11 Generally

The Chamber wishes to express its concerns regarding the proposed rule, specifically the Automated Decision-Making Technology (ADMT) sections, which exceed the agency's statutory authority. We have significant concerns about this duplicative effort, as it overlaps with several ongoing regulatory initiatives in California. Notably, the California Civil Rights Department (CCRD) has proposed modifications to employment regulations concerning automated decision systems within the employment context. Concurrent regulatory initiatives from different agencies create significant challenges for the business community, leading to unnecessary confusion and potentially conflicting regulations. We believe provisions of Article 11 exceeds the authority granted to the Agency under the CCPA.

The Chamber believes that the CPPA should halt further efforts to regulate ADMT until it has been granted statutory authority to proceed with such rulemaking. We offer the following feedback on Article 11: Automated Decision-Making Technology (ADMT).

B. Scope of ADMT Regulation

[40] *Id.*

The Agency's expansion of the scope of ADMT regulation is problematic and potentially duplicative. We are particularly concerned about the expansion into areas such as generative AI and behavioral advertising, which extend beyond the scope of the voter-approved statute. These advertisements are not decisions but instead means to raise consumer awareness and personalize experiences.

Moreover, the activities covered by Article 11 sweep extremely broadly. For example, Proposed Sections 7220 and 7222 are tantamount to full-scale AI Impact Assessment legislation as opposed to mere access rights which were contemplated in the text of CCPA.

C. Broad Definition of ADMT

As we highlighted hereinabove, we are deeply concerned that the definition of ADMT is overly broad and not sufficiently tailored to focus on high-risk tools that make significant decisions about consumers and operate without human oversight.

We urge you to reconsider concerns raised by Mr. Mactaggart with the Proposed Rule's definition of ADMT[41] that "our definition of ADM includes the use of almost any computerized technology in a way that describes how humans have used computers for 30 or 40 years." The author of the Act's ADMT provision is stating the intent is not to create new rules around specific technology but in a technology neutral way address privacy harms.[42]

D. Opt-Out Provisions

The Agency's requirement for consumers to have the "Right to Opt-Out," irrespective of the technology's risk level, is highly problematic and impractical. Providing these opt-out rights is impractical, particularly because of the expansive range of systems that are captured by the overbroad definition of ADMT. The result is that businesses must evaluate a wide range of systems – many of which have little or no connection to consumer privacy risks -- to determine when an opt-out process needs to be built or whether an exception to the opt-out exists. We are also concerned about the requirement for businesses to disgorge personal information previously processed upon a consumer's opt-out request, as this could lead to significant operational challenges and may be unworkable.

We recommend that only verifiable requests be subject to opt-out requirements, as well as a need for an exception to be added for critical security and fraud tools. These will ensure user preferences are accurately followed, and companies can proactively protect consumers from unwarranted security and fraud

[41] *Supra* n. 3 at 100.
[42] *Id.*

concerns. This is why, like CCPA and other state privacy laws, they have substantial exemptions for opt-out provisions for activities that prevent and secure against fraud. Section 7221(b)(1)(B) should be strengthened to clarify that the opt-out right does not apply to activities that are aimed "to resist, prevent, and detect, malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions; or[...]."

E. Pre-Use Notice Requirements

The Proposed Rules would require businesses to explain detailed uses and purposes for ADMT, which is excessively burdensome. Additionally, the prohibition of standard business terms such as "to improve our services" is overly restrictive. We are concerned that pre-use notice requirements could be construed as requiring companies to disclose trade secrets and sensitive business information. The overbroad definition of ADMT will bring in a wide range of everyday business systems that will overwhelm consumers and make it harder for consumers to find important vital information. Furthermore, we believe the agency should provide clarification that any requirements set forth within the regulations is prospective and not retroactive and excludes third parties which have no ability to provide notice.

F. Clarity on Exemptions

The Chamber expresses concern that the current draft of the rule does not align with the established precedent of exemptions under the California Privacy Rights Act (CPRA). We respectfully request that any revised draft maintain consistency with the statutory language and explicitly state that the exemptions provided under the CPRA are also applicable to the ADMT. For example, the "opt-out" provision not operational because of the lack of a carve out to prevent fraud, but because that the services that a firm provides and offers in many cases may only be through "ADMTs."

G. ADMT Access Rights

The Chamber has significant concerns about the requirements for responding to the new "right to access ADMT," as they are overly broad and burdensome for businesses. We recommend that §7222(b) be simplified and aligned with existing legal language. Additionally, the requirement to inform consumers about alternative actions they could have taken to secure a different decision is excessively prescriptive and not consistent with existing laws, which already provide consumers with substantial information rights.

The obligations imposed on service providers to assist businesses with ADMT requests are unnecessary and should be eliminated, as they are already covered by

current CCPA obligations regarding data subject rights. Therefore, §7222(h) should be deleted.

- Prescriptive requirements for using ADMT with a consumer more than four times in 12 months are unnecessary and should be eliminated. Thus, §7222(i) should be deleted.
- The CCPA already ensures that consumers have the general right not to be retaliated against for exercising data subject rights. Therefore, §7222(j) is duplicative and unnecessary and should be deleted.
- Section 7222(k) introduces an additional notice requirement for certain "adverse significant decisions," including "financial or lending" decisions. These additional notice requirements are highly prescriptive and burdensome and should be deleted.

VI. Definitions Broadly

The Proposed Regulations would define "sensitive personal information" ("SPI") to include "[p]ersonal information of consumers that the business has actual knowledge are less than 16 years of age. A Business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age."[43] Such data would be subject to the full CCPA's consumer data minimization and disclosure limitation rights.

We are concerned that defining personal information of users age thirteen and older would undermine the ability of business to tailor their products and services to deliver age-appropriate experiences for minors. We urge the Agency to remove this overly broad designation.

VII. Revisions to Current Regulations

Certain proposed revisions to Article 3 conflict with other areas of the CCPA, do not consider the operational impact, and create a compliance burden without providing consumers with significantly greater protection. Specifically:

- **Method for submitting CCPA requests and obtaining consent (§7004(a)(2)(A))** – The symmetry in choice requirement does not reflect the fact that there is an inherently different amount of work that is needed in order to opt-in (which can be done by clicking a single link) versus to opt someone out of sharing their information – for example, once they click the link, the business still needs to verify them. The regulations should revert to how they were previously drafted and require symmetry, but not limit opt outs to the "same or fewer" steps.

[43] Proposed Rule §7001(ccc)(4).

- **Method for submitting CCPA requests and obtaining consent (§7004(a)(4)(C)** – The prohibition on using general terms of acceptance conflicts with the CCPA which requires businesses to provide consumers with a notice at collection. This prohibition does not relate to or address dark patterns and should be deleted.

- **Requests to Delete, Know, Opt-Out of Sale/Sharing (§7022(g)(5), §7024(e)(3), §7026(e))** – Requiring businesses to provide consumers a disclosure that they can file a complaint with the CPPA even if there are valid reasons for denial is counterintuitive and will result in unfounded complaints from consumers who interpret the complaint disclosure as a required next step. **Therefore, this provision should be removed.**

- **Requests to Correct (§7023(f)(3)(g)** – the draft regulations require that, if a business denies a right to correct it must then inform the consumer that it will note both internally and to third parties to whom is disclosure the personal information that the accuracy of the PI is contested. This provision goes beyond the scope of the law and should be deleted. The CCPA provides for an obligation to correct and exception to that obligation. The CPPA should not place additional and burdensome requirements on businesses that will not be practical to operationalize.

- **Requests to Know (§7024(d)(2)** – the draft regulations require businesses to provide consumers with a way for consumers to confirm that SPI information is the same as what the consumer expects it to be, while also prohibiting businesses from disclosing such SPI. It is unclear to comply with this requirement without disclosing such information.

- **Revisions to Sections 7022, 7024, and 7026** would require businesses to inform consumers they can file a complaint with the CPPA. However, disclosure that they consumers can file a complaint with an Agency even if there are valid reasons for denial is counterintuitive and will result in unfounded complaints from consumers who interpret the complaint disclosure as a required next step.

VIII. Insurance Companies

The Agency Proposes defining insurance companies for the purposes of the rules as persons subject to the California Insurance Code. Proposed Article 12 would impose the obligations and requirements of the CCPA to insurance companies with regard to any personal information not subject to the Insurance Code and its regulations. For example, those insurance companies "shall comply with the CCPA for personal information that is collected for purposes not in connection with an insurance transaction, as that term is defined in Insurance Code, section 791.02."

Insurance companies are subject to more laws and regulations that merely the Insurance Code. We proposed that the Agency strike the language stating "For example, those insurance companies shall comply with the CCPA for personal information that is collected for purposes not in connection with an insurance transaction, as that term is defined in Insurance Code, section 791.02" to align with this reality and avoid duplicative regulation.

If you have any questions, please contact Jordan Crenshaw at jcrenshaw@uschamber.com. For questions concerning Article 9, please contact croberti@uschamber.com.

Sincerely,

Jordan Crenshaw
Senior Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce

Christopher D. Roberti
Senior Vice President
Cyber, Space, and National Security
Policy Division
U.S. Chamber of Commerce

Grenda, Rianna@CPPA

From:	Marie-Charlotte BOUQUET <mariecharlotte@idside.eu>
Sent:	Monday, January 20, 2025 7:08 AM
To:	Regulations@CPPA
Subject:	Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments:	CCPA PUBLIC CONSULTATION Consent-IDside inputs.pdf

Dear CCPA team in charge,

Please find attached ID side comments on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations focusing mainly on opt-out signals and consent provisions.

Marie-Charlotte BOUQUET
ID side Principal & Research Lead

To set my Privacy right(s)

CONTRIBUTION OF ID side to CCPA PUBLIC CONSULTATION ON THE "PROPOSED TEXT (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations)"

1. Our Organization in a nutshell

ID side is a French independent start-up created in 2019, right after the adoption of the GDPR in EU, by 3 associates: an expert in Privacy (Marie-Charlotte Roques-Bonnet, 20 years' experience), an expert in Security (Alain Pannetrat, 20 years' experience) and a Data visualisation expert (Damien Bouquet, 15 years' experience).

We created ID side with the objective to give control back to internet users over commercial targeting online, empower them to set their privacy Choices in few clicks & **share their specific commercial interests seamlessly online**. Our goal is to foster ethically & environmentally sustainable business models and facilitate qualitative exchanges between individuals and the Companies they trust or like.

The objective of ID side is also to help anyone effectively set their choices online (i.e. regarding Privacy, Safety, commercial preferences or Artificial Intelligence) and exercise their privacy rights seamlessly and automatically.

After years of Research and patenting our Tech, including in the US, we decided in 2024 to shift our main focus from at tool automatically sharing our reasonable expectations regarding "Cookie banners" (see our PoC on idside.eu / and the page idside.eu/cookies) to:

- Designing the second prototype for our "Personal Data Choices Management Platform" with the view of "sandboxing" it;
- launching a new "personal and private marketplace" -to be rolled out in February- so that individuals can easily set their commercial & algorithmic preferences (ID side app on iOS and Android).

On the long-run, ID side promotes an alternative and user-centric approach to online commercial targeting that we call the Light Web. In 2020, online commercial personalisation & ad targeting worked as follows:

- My data is collected online 24/7.
- It is sold so that ads get better directed to me.
- Companies sell such data without giving me control.

With ID side, and the Light Web model, individuals are empowered to take control over their data & ads displayed to them. They decide:

- How they want personal data to be collected online (our cookie banners extension).
- By Whom, When and How they want to be targeted (our personal & private marketplace).
- Which Companies they want to create a trusted relation with.

In conclusion, our Research, Proof of Concepts (auto-filling of cookie banners) and latest prototypes (a personal and private marketplace) promote the **Light Web**, that is to say a digital business model in which there are less data collected "in my back", I have more control on targeting & ads and companies unleash the benefits of an alternative **ethically & environmentally sustainable model**.

2. Why is it relevant for ID side to contribute to CCPA Public consultation?

ID side team has a sound expertise in data protection and struggles to advance digital fundamental rights' state of the art tools -specifically with regards to individual-choices-automatic-sharing-online. Its "Personal Data Choices Management Platform" is designed to empower internet users to share opt-out signals about any individual choice or right (regarding Privacy, AI, safety or any other right) and their commercial preferences (into brands, products, sectors), which is part of the mechanisms that could be relevant to this consultation.

Separately, our team noted in "7025. Opt-out Preference Signals" (a) (2) that "*The configuration or disclosure does not need to be tailored only to California or to refer to California*". In the light of our germinating exchanges with DAA about Webchoices 2.0 Token ID, we considered it was relevant to share about our Technology and prototypes.

3. Consultation scope & specific provisions at stake

ID side team recognizes the significance of the consultation and the CCPA's role in advancing privacy rights globally. We also express appreciation for the opportunity to provide feedback specifically about "Opt-out preference signals" and consumer consent & rights online.

To our view, this consultation is a vital step toward ensuring robust consumer privacy protections worldwide while fostering transparency and trust between consumers and businesses.

Our contribution will mainly focus on 3 topics, specifically tied to our "niche" expertise:

1. Consumer consent: *"§ 7004. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent*", and specifically (a) (2) (C), (a) (3) (C) & (D), (a) (4) (A) & (a) (4) (C), (5) and 5(C).
2. Sharing of preferences signal online: "*7025. Opt-out Preference Signals*" , and specifically (a)(2), (c) (2), (7) (C), (7) (E).
3. Automatic submission of individual requests: *"§ 7026. Requests to Opt-out of Sale/Sharing*", specifically (a) (2), (a) (4), (b), (c), (j), *"§ 7027. Requests to Limit Use and Disclosure of Sensitive Personal Information*", specifically (a), (b) (1), (b) (2), (b) (3) and (c) (5) and "§ 7028. Requests to Opt-in After Opting-out of the Sale or Sharing of Personal Information or Limiting the Use and Disclosure of Sensitive Personal Information" (b).

4. Our Objective: bringing a practical view and sharing about state-of-the-art Tech available in the US and internationally

In this submission, ID side team would like to provide feedback on the implementation of opt-out rights and, beyond those of any right online, but also the automatic sharing of reasonable expectations, choices or preferences in a state-of-the-art and seamless way for individuals. Part of our team has formerly worked for Privacy regulators (i.e. CNIL in France) and would be keen on contributing to a consistent understanding of what Tech-enabled-consent tools should look like.

We hope this contribution will provide practical insights and align with the shared goal of ensuring strong privacy protections for consumers while enabling businesses to operate effectively within California's innovative economy.

5. Our Contribution & comments in detail

A. Consumer consent: *§ 7004. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent*

1/ As set in (a) (2) (C), "*Framing the consumer's options in this manner impairs the consumer's ability to make a choice*", ID side team respectively suggests that CCPA teams would envisage alternative techniques that could be put at the service of individuals online to empower them and give them the ability to make choices freely -as **described in Appendix 1** of this contribution.

2/ Based on (a) (3) (C) and (D), we respectively outline that any service that would be user-centric (starting from individuals' choices cross-platforms, and their reasonable expectations, would help to affirmatively consent, avoid confusing individuals -whatever the design of buttons or choice architecture would be ("*Businesses should also must not design their methods in a manner that would impair the consumer's ability to exercise their choice because consent must be freely given, specific, informed, and unambiguous. Illustrative examples and requirements follow*").

3/ Based on (a) (4) (A) -and (a) (4) (C), ID side provides an example of architecture that does not require " *the consumer to click through disruptive screens before they are able to submit a request to opt-out of sale/sharing is a choice architecture that impairs or interferes with the consumer's ability to exercise their choice*": the "**Personal data choice management platform**" (see PDCMPs' full description in Appendix 1).

Contrary to traditional "Consent management platform", "***Personal data choice management platforms***" (like ID side) allow users to automatically share their by-default preferences regarding Privacy (i.e. by-default cookie choices) or commercial interests (i.e. contrary to all other companies they do not have an interest in -companies B, C and D- they would flag agreement to be tracked by company A because they like their products or sector (a) because ads from this sector would be relevant).

In a first time, personal data choice management platforms allow users to share their individual reasonable expectations regarding for instance their personal data being sold or reused by first and third-party cookie providers. For instance, if an individual's reasonable expectation is not to be tracked online except by Company A or for products and services of sector (a), only Company A or providers of products and services of sector (a) are entitled to send a consent request to the individual. **They do not aim at collecting consumers' consent but at streamlining consent requests that could be sent in a second time**.

Of course, all users of personal data choice management platforms are empowered to change and update their individual reasonable expectations over time, in few clicks.

In a second time (that is to say only when consistent with the individual reasonable expectations set by individuals), first-party and third-party service providers online should be entitled to ask for a

valid consent (that is to say freely given, specific, informed, and unambiguous). This mechanism is the core feature that would help empower consumers and substantially reducing consent requests -also drastically reducing "consent fatigue" online because: 1. Consent requests are drastically reduced based on the reasonable expectations I share wherever I browse; 2. I monitor consent requests in a trusted platform centralising all consent requests to monitor. In ID side for instance, such consent could be sent by Company A or sector (a) providers to a targeted-consent "contact inbox" (or individual "spambox") designed for individuals to be in capacity to read the specific information needed and validly consent, when they do have time and interest to do so. They would then freely agree to the processing of their personal data -or not.

NB: "***Consent management platforms***" are a mechanism allowing people to consent at a given time, that is to say when individuals browse a website and are willing to access content. Such mechanisms are widely spread across the web. Importantly, they do not allow users to share their individual reasonable expectations in advance, nor to update those or to have those automatically and seamlessly shared as they browse. Most of all, they do not reduce the number of consent requests shared by first-party and third-party cookie providers, nor the time needed for individuals to consent (contrary to Personal data choice management platform, it is not when they are ready to do so, but only "on the fly" and as they browse). Therefore, by nature, such mechanisms do not, per se, a tool to collect freely given consent and do not address the consent fatigue problem.

4/ Regarding (5), and the "Easy to execute" test, ID side stresses that businesses using PDCMPs do "*not add unnecessary burden or friction to the process by which the consumer submits a CCPA request or provides or withdraws consent*" but on the contrary substantially alleviate attention and steps needed. As Methods should "*be tested to ensure that they are functional and do not undermine the consumer's choice to submit the request*", we would respectively suggest adding an illustrative example about PDCMPs that would enhance interfaces can avoid having "the effect of substantially subverting or impairing user autonomy, decision making, or choice" ((5)(c)).

B. <u>Consumer Preferences: 7025. Opt-out Preference Signals.</u>

1/ As set in (a), "*The purpose of an opt-out preference signal is to provide consumers with a simple and easy-to-use method by which consumers interacting with businesses online can automatically exercise their right to opt-out of sale/sharing*". We believe there is no easier method than PDCMPs that could help individuals share their preferences seamlessly.

2/ As set in (c)(2), (7)(A), (7)(C) and (7)(E) examples, ID side team would also be keen on referring to PDCMPs' mechanism.

C. <u>Consumer Requests: 7026. Requests to Opt-out of Sale/Sharing.</u>

1/ In (a) referring to *"available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of sale/sharing*", CCPA mentions that "*at least one method offered shall reflect the manner in which the business primarily interacts with the consumer*". Illustrative examples could also include PDCMPs' mechanism.

2/ Regarding (j), ID side team does not fully grasp whether such § would impede or slow down the adoption of cross-platforms solutions that would benefit individuals online (such as PDCMPs) and respectfully invites drafters to consider less demanding/formal alternatives.

D. Consumer Requests: 7027. Requests to Limit Use and Disclosure of Sensitive Personal Information

1/ In (a) and (b), ID side team invites to consider whether PDCMPs could count among the "*two or more designated methods*" to consider and expand its illustrative examples.

2/ Such option seems to primarily align with the initial drafting consideration, taking into due consideration:
- (3) ("*Other methods for submitting requests to limit include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, and a form submitted through the mail.*");
- (c) ("*A business's methods for submitting requests to limit shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004*").

E. Consumer Requests: 7028. Requests to Opt-in After Opting-out of the Sale or Sharing of Personal Information or Limiting the Use and Disclosure of Sensitive Personal Information.

1/ Finally, considering: "*Requests to opt-in to sale or sharing of personal information and requests to opt-in to the use and disclosure of sensitive personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in*", Appendix 1 here-below describes how the PDCMP model implements the 2 steps mechanism, starting from a user-centric handling of individual reasonable expectations and going back to a specific consent request by service providers online only when it makes sense -based on the reasonable expectations set by each individual.

ID side team would be happy to provide more information or targeted insights as needed.

6. "*Online Consent: How to make it valid in practice?*" – ID side draft contribution to IAPP Data Protection Engineering Board & online blog

Should it shed light on ID side overall understanding of the challenges at stake, and appear to be useful to consider, our team takes the liberty to share an extract of its contribution to IAPP reflection on the topic of consent online & the exercise of individual rights in Appendix 2.

APPENDIX 1 - Additional background & information on ID side and the "Personal Data Choices Management Platform" (PDCMP) designed by ID side

---

Additional background & information on ID side and the PDCMP designed by ID side

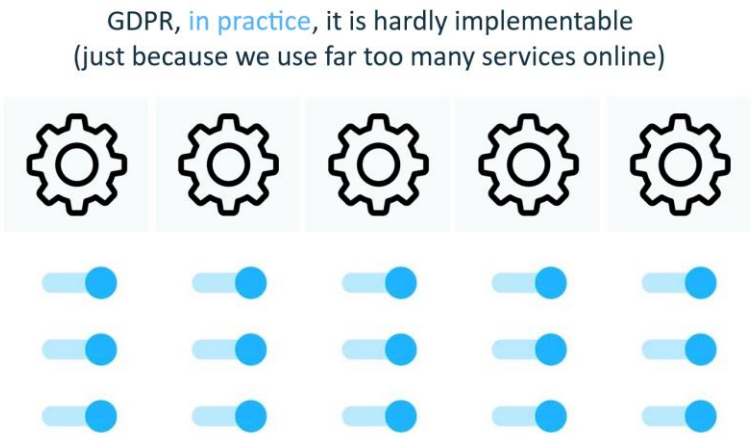
ID side solution is architected to technically empower internet users and share their by-default choices wherever they browse (such choices could be Privacy, Safety, AI or commercial ones).

Doing so, our solution reduces consent fatigue: because our tool technically empowers individuals to seamlessly and automatically share their Privacy & commercial reasonable expectations online, it allows them to receive streamlined consent requests from first-party and third-party providers (but also providers of URL and pixel tracking, local processing, tracking based on IP only, intermittent and mediated Internet of Things (IoT) reporting and unique Identifier).

Few months ago, ID side substantially contributed to **advancing discussions in EU in the frame of the "Cookie Pledge" initiative, notably presenting its "Proof of Concept"** (PoC) to DG Connect and all participants. Within this EU framework, we count among those that inspired the drafting of Principle H of the Pledge: "*Signals from applications providing consumers with the possibility to record their cookie preferences in advance […] will be accepted*".

We also contributed to EDPB's work on the Technical Scope of Art5(3) of ePrivacy Directive, which content is available online and that we take the liberty to summarise here-below. Our patent details are also available. Our team remains at your disposal to provide additional information.

The Problem we address today



While creating ID side in 2019, notably with a former security expert from CNIL, we wanted to make consent definition as in rec. 32 GDPR ("*a clear affirmative act establishing a freely given, **specific, informed** and unambiguous indication of the data subject's agreement*") applicable in practice. We wanted to give users real control over the way their (meta)data gets collected online, specifically because consent collection would be substantially streamlined, individuals would have time to read specific and relevant information and, then only, once they are ready, to freely consent.

We started from the observation that actually today, no one **validly** consents for 3 reasons (on the top of imbalance of powers and "Pay or ok").
1/ **Privacy policies** (2012 Carnegie Mellon Research: 76 Working days to read privacy policies) and targeted Privacy information reading is just impossible.
2**/ Cookie banners bombing** and requiring endless/complex validation and repetition of individuals' basic choices often triggers "systematic acceptance" of any term & condition or privacy specification, just to "get rid of it" and be able to access content.
3/ It is really difficult to **find appropriate and effective privacy settings** online: where are they? What controls am I actually given (potentially accessing also to a binary I accept/I do not use the service options or dark patterns' requests)?

$$x = Compliance$$
$$y = Control$$

$$f(x) = y?$$

In other words & in practice:
How can the GDPR provide
more effective Users' control?

Inspired by recital 68 of the GDPR and article 12 of the GDPR, we wanted to address this problem and empower internet users in practice and developed the solution we present you here below. It seems all the more necessary to put internet users in control in IoT/Data Spaces/metaverse environments in which most of our personal data is coded, embedded in an IoT mapping of our activities and a 360 digital profile of each of us is likely to be established.

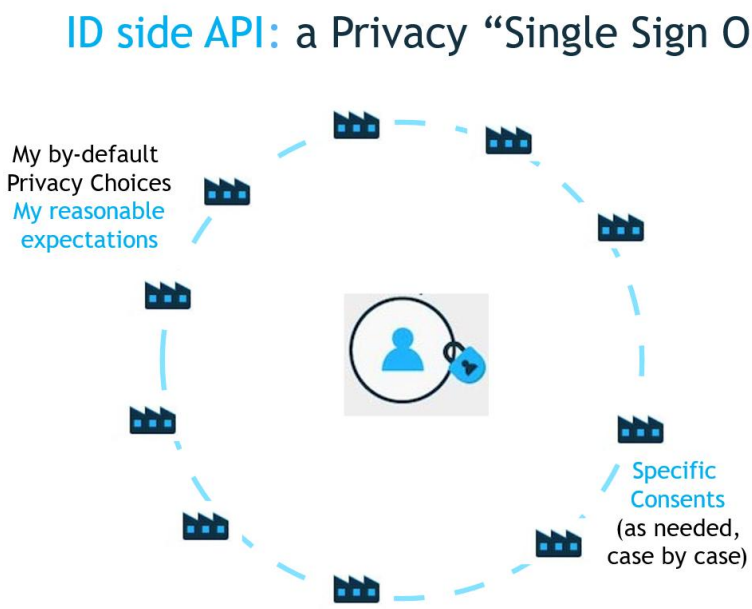
How could compliance with GDPR bring more control to individuals, specifically online? Our view is that a **mechanism** is missing to empower individuals so that they have genuine **control over their personal data processing online**. This is ID Side's quest: designing a tool that will help users exercise their privacy choices efficiently and seamlessly in practice. So that they have control on all personal data processing carried out based on their browsing.

Our Proof of Concept and its impact on Consent online

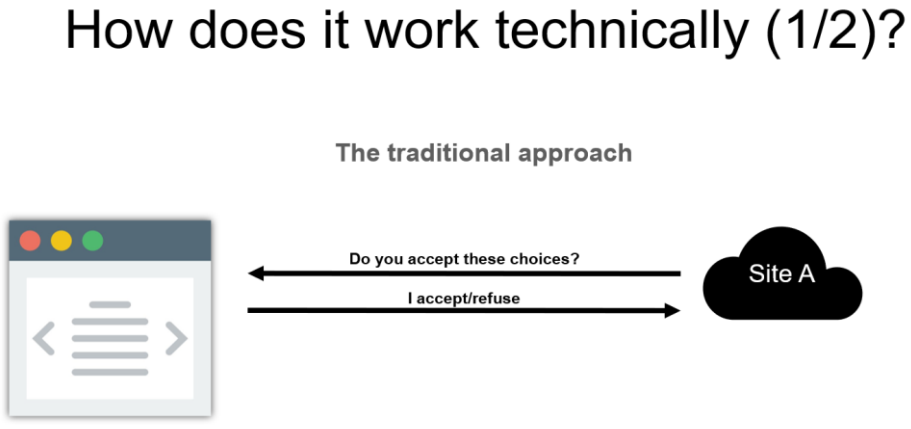
ID side is about making personal choices setting/monitoring possible, based on a tool or mechanism that is **user-centric and cross-platform**. Let's take the example of cookie banners. In addition to dealing

with the issues we highlighted previously (too many privacy policies to read, too many settings, not enough time), ID side's proposal is to start from the existing online business environment and help individuals:

1. set their **Privacy Choices by-default** (that is to say their **individual reasonable expectations**)
2. **automatically & seamlessly share those choices**, wherever they browse
3. **decide, when they are ready to so, and based on their personal interests at a the time, to consent to specific data processing**.



How does ID side work technically?



The current & traditional model is summarised above -in summary: far too many websites, policies, settings along with potentially limited choices (accept/refuse) or dark patterns.