COVINGTON

BEIJING BRUSSELS DUBAI FRANKFURT JOHANNESBURG
LONDON LOS ANGELES NEW YORK PALO ALTO
SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

Lindsey Tonsager

Covington & Burling LLP
Salesforce Tower
415 Mission Street, Suite 5400
San Francisco, CA 94105-2533
T +1 415 591 7061
ltonsager@cov.com

By Electronic Mail

March 27, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Boulevard
Sacramento, California 95834
regulations@cppa.ca.gov

Re: Preliminary Rulemaking Activities on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking (PR 02-2023)

The California Chamber of Commerce ("CalChamber") submits these comments in response to the California Privacy Protection Agency ("CPPA") request for public input on the rulemaking referenced above.[1] CalChamber supports the goals of protecting consumer privacy, advancing innovation, and encouraging interoperability between the CPPA's regulations and other global legal frameworks. Our members are committed to building transparency and trust about how consumers' personal information is collected, used, and disclosed, and are committed to acting as trustworthy stewards of consumers' personal information across jurisdictions. In particular, CalChamber urges the CPPA to take action to execute on its goal of promoting innovation and interoperability, including the CPPA's efforts to draft regulations that "would not contravene a business's compliance with other privacy laws" and "simplif[y] compliance for businesses operating across jurisdictions."[2]

Across the three topics addressed in the invitation for rulemaking comments, common themes emerge, including a need to: (1) retain consistency with the statutory text, (2) harmonize the regulations with existing privacy frameworks, and (3) promote consumer privacy, while also strengthening innovation. Accordingly, and as explained in further detail below, CalChamber requests that the CPPA adopt regulations that incorporate the following concepts:

---

[1] CPPA, *Preliminary Rulemaking Activities on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking* (Feb. 10, 2023), available at: https://cppa.ca.gov/regulations/pre_rulemaking_activities_pr_02-2023.html.

[2] *See* CPPA, Notice of Proposed Rulemaking, 7 (Jul. 8, 2022), https://cppa.ca.gov/regulations/pdf/20220708_npr.pdf. *See also* Californians for Consumer Privacy, *California Privacy Rights Act Text,* Section 3(A)(8), available at: https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/#1798.140(v) ("To the extent it advances consumer privacy and business compliance, the law should be compatible with privacy laws in other jurisdictions.").

- For **cybersecurity audits**, the regulations should (A) promote interoperability and align with the processes and goals set forth in existing legal frameworks or recognized standards and (B) afford a business the flexibility to use a risk-based approach, including by tailoring cybersecurity audits to the size and complexity of the business and the nature of the data and processing activity, and to conduct thorough audits internally ("Section I");

- Regarding **privacy risk assessments** ("privacy assessments"), regulations should (A) prioritize compatibility with existing privacy statutes and (B) align with requirements in the statutory text and related requirements in the CCPA ("Section II"); and

- With respect to **automated decisionmaking** rights, regulations should: (A) define automated decisionmaking to promote coherence across legal frameworks, (B) clarify that certain automated decisionmaking is not subject to opt-out and access rights, and (C) permit a business to provide meaningful information about automated decisionmaking through its privacy policy or similar disclosures, without revealing trade secrets ("Section III").

I. The CPPA Should Align Regulations For Cybersecurity Audits With The Statutory Text And Existing Legal Frameworks.

The statutory text explicitly tasks the CPPA with creating regulations to address cybersecurity audits where processing "presents *significant risk* to consumers' privacy or security" and that take into account the "size and complexity of the business and the nature and scope of processing activities."[3] Accordingly, to effectuate the goals of the statutory text, facilitate interoperability with global privacy frameworks, and promote businesses' ability to comply with the CCPA, CalChamber requests that the CPPA: (A) recognize compliance with existing legal frameworks or recognized cybersecurity standards and (B) afford businesses with flexibility to use a risk-based approach (including by adapting any cybersecurity audit requirements to the size and complexity of the business and the nature of the data and processing activity) and conduct cyber audits internally.

A. Regulations Addressing Cybersecurity Audits Should Promote Interoperability With Existing Legal Frameworks Or Recognized Cybersecurity Standards.

CalChamber urges the CPPA to focus cybersecurity audits on those activities that "present[] significant risk to consumers' privacy or security," as required by the statutory text.[4] Consistent with this mandate, the CPPA should advance regulations that require cybersecurity audits only for those processing activities that result in ***both*** processing (1) in furtherance of a decision with a legal or similarly significant effect concerning the consumer ***and*** (2) sensitive

---

[3] Cal. Civ. Code Ann. §§ 1798.185(15), (15)(A).

[4] Cal. Civ. Code § 1798.185(15).

personal information. Doing so furthers the CPPA's "goal of strengthening consumer privacy, while giving attention to the impact on business and innovation,"[5] as it focuses cybersecurity audits on those processing activities that create the most risk and would yield the most positive outcomes for consumer privacy. Furthermore, requiring cybersecurity audits for processing involving both in furtherance of decisions with legal or similarly significant effects and processing sensitive personal information also implements the statutory requirement that cybersecurity audits take into account the nature and scope of processing activities.[6]

In addition, the CPPA should recognize that cybersecurity audits, assessments, or evaluations performed in accordance with another legal framework or recognized cybersecurity standard satisfy the CCPA's cybersecurity audit requirement. Numerous existing global legal frameworks require cybersecurity audits. For example, both the New York Department of Financial Services and the Defense Federal Acquisition Regulation require the entities regulated (respectively) to undertake a cybersecurity assessment.[7] In addition, the EU's NIS2 Directive requires covered sectors and entities to regularly carry out targeted cybersecurity audits.[8] Moreover, the California Attorney General's 2016 data breach guidance recommended an assessment of cybersecurity risks of assets and data as part of a reasonable cybersecurity approach.[9] Entities also look to internationally recognized and consensus-based cybersecurity standards that reflect input from experts on cybersecurity best practices, many of which require a thorough review of the organization's cybersecurity posture, such as the ISO/IEC 27000-series and the National Institute of Standards and Technology ("NIST") Cybersecurity Framework.[10] Rather than set forth additional, possibly conflicting cybersecurity audit standards and

---

[5] Californians for Consumer Privacy, *California Privacy Rights Act Text,* Section 3(C)(1), available at: https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/#1798.140(v) (emphasis added).

[6] Cal. Civ. Code Ann. §§ 1798.185(15), (15)(A).

[7] *See* 23 NYCRR 500.09, available at: https://www.governor.ny.gov/sites/default/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf (requiring covered entities to conduct a periodic risk assessment). The Defense Federal Acquisition Regulation mandates compliance with the National Institute of Standards and Technology 800-171, which requires a cybersecurity risk assessment. *See also* NIST SP 800-171, Section 3.11.1, available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

[8] *See* DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (2022) [hereinafter NIS2 Directive].

[9] *See* California Attorney General, *California Data Breach Report*, 29, 30 (Feb. 2016), available at: https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf. This guidance also recognized the Center for Internet Security's Security Controls, which recommend an inventory to assess assets. *See* Center for Internet Security, *The 18 CIS Critical Security Controls*, available at: https://www.cisecurity.org/controls/cis-controls-list.

[10] *See* ISO/IEC 27000, available at: https://www.iso.org/isoiec-27001-information-security.html; *see also* NIST Cybersecurity Framework, available at: https://www.nist.gov/cyberframework.

requirements, CalChamber requests that the CPPA recognize that cybersecurity audits undertaken under a comparable legal framework or recognized standards satisfy the audit, assessment, or evaluation requirements under the CCPA. The NIS2 Directive takes a similar approach, encouraging covered entities to utilize other international standards as tools to comply with the Directive.[11] Over time, this approach would also allow the CCPA to seamlessly account for new or modified frameworks, standards, and best practices elaborated in conjunction with the rapid changes in technology and cybersecurity, without undertaking the cumbersome process to update the CCPA .[12]

B. Regulations Should Afford Businesses Flexibility To Use a Risk-Based Approach, Including By Tailoring Audits To The Size and Complexity Of the Business And The Nature Of The Data And Processing Activity And To Conduct Audits Internally.

The statutory text requires that CPPA cybersecurity audit rules consider the "size and complexity of the business and the nature and scope of processing activities."[13] Consistent with other legal frameworks, which afford covered entities with the flexibility to customize the audit to their operations,[14] CalChamber urges the CPPA to recognize that the components and approach to cybersecurity audits may need to be modified depending on the circumstances. For example, a requirement to review the organization's processing of work-related project scheduling activities should be different from the review of processing by a fertility prediction health tool due to, among other things, the different nature of data processed.

Additionally, CalChamber urges the CPPA to recognize that cybersecurity audits, assessment or evaluation can be undertaken internally and do not always require consultation or review by a third party. The fact that an organization undertakes an assessment internally does not preclude it from being comprehensive and independent. As recognized in other sections of California law and cybersecurity standards, internal audits can be performed in a way

---

[11] NIS2 Directive, art. 25 (emphasizing that member states "shall encourage the use of European and international standards and technical specifications relevant to the security of network and information systems").

[12] Regulators and agencies are undertaking efforts to set forth new and updated standards for cybersecurity. For example, the White House has launched an effort to develop a national cybersecurity strategy. *See, e.g.*, White House, *National Cybersecurity Strategy* (Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf ("Where feasible, regulators should work to harmonize not only regulations and rules, but also assessments and audits of regulated entities.").

[13] Cal. Civ. Code Ann. §§ 1798.185(15), (15)(A).

[14] New York State Department of Financial Services, *Cybersecurity Resource Center*, FAQ 10, available at: https://www.dfs.ny.gov/industry_guidance/cybersecurity ("DFS does not require a specific standard or framework for use in the risk assessment process. Rather we expect Covered Entities to implement a framework and methodology that best suits their risk and operations.").

that is independent and promotes a thorough review of practices.[15] Moreover, a rule that requires a third-party independent audit under all circumstances would result in an unworkable burden for many companies, particularly small- and medium-sized businesses. Instead, the CPPA should recognize that thorough internal cybersecurity audits, assessments, or evaluations against an organization's reasonable governance, risk management, and internal controls satisfy requirements and protect consumers under the statute. The regulators' ability to review these audits assures their adequacy by incentivizing companies to be thorough in their review and consideration of mitigation measures.

II. Regulations Regarding Privacy Assessments Should Promote Harmonization Across Legal Frameworks And With The Statutory Text Of The CCPA.

The CCPA will join the growing number of privacy frameworks that require privacy assessments for certain processing activities. For example, Virginia, Colorado, and Connecticut recently passed laws that require companies to assess certain data processing activities.[16] Additionally, both the GDPR and LGPD require assessments in certain circumstances.[17] Consistent with the CPPA's goal to promote consumer privacy and "simplif[y] compliance for businesses operating across jurisdictions,"[18] CalChamber encourages the CPPA to prioritize compatibility with these existing privacy statutes and harmonize the provisions with other requirements of the CCPA statute and regulations.

A. The CPPA Should Prioritize Compatibility With Existing Privacy Statutes

CalChamber requests that the CPPA develop regulations that are aligned with the statute's intent by furthering "compatib[ility] with privacy laws in other jurisdictions," where

---

[15] *See, e.g.*, Cal. Gov. Code § 13887 ("In order to achieve independence and objectivity. . . the internal auditor operations" shall meet certain requirements, including reporting audit findings to agency leadership); Cal. Ins. Code § 900.3 ("An insurer or group of insurers doing business in this state shall establish an internal audit function to provide independent, objective, and reasonable assurance . . . regarding the insurer's governance, risk management, and internal controls."); *See also* Payment Card Industry, Data Security Standard Version 4.0 (Mar. 2022), available at: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf (permitting self-assessments).

[16] *See, e.g.*, VCDPA § 59.1-575 *et seq.*; CPA § 6-1-1301 *et seq.*; CTDPA.

[17] General Data Protection Regulation, Article 35; Brazilian General Data Protection Law ("LGPD"), Articles 5, 10, 38.

[18] *See* CPPA, Notice of Proposed Rulemaking, 7 (Jul. 8, 2022), https://cppa.ca.gov/regulations/pdf/20220708_npr.pdf; *see also* Californians for Consumer Privacy, *California Privacy Rights Act Text,* Section 3(A)(8), available at: https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/#1798.140(v) ("To the extent it advances consumer privacy and business compliance, the law should be compatible with privacy laws in other jurisdictions.").

doing so "advances consumer privacy and business compliance."[19] With this in mind, CalChamber asks the CPPA to recognize that reasonably similar assessments meet CCPA obligations, limit assessments to profiling in furtherance of decisions with legal or similarly significant effects concerning the consumer, and permit businesses to complete a single assessment for multiple similar activities.

The CCPA joins the growing number of data privacy frameworks around the world that require assessments for certain processing activities.[20] Like many of these frameworks, the CCPA regulations should recognize assessments with a reasonably comparable scope and effect, which would also align the CCPA regulations with other state frameworks in a manner that furthers the goals of interoperability and compliance.[21] For example, the Virginia Consumer Data Privacy Act and the Colorado Privacy Act Regulations recognize that privacy assessments conducted "for the purpose of compliance with other laws or regulations" may also comply with requirements under those laws, so long as those privacy assessments have a "reasonably comparable scope and effect."[22] Here, too, CalChamber urges the CPPA to recognize a role for similar privacy assessments completed under other jurisdictions' privacy laws, which will not only promote consistency across legal frameworks, but will also allow businesses to focus their resources on a single meaningful and fulsome review, rather than undertaking multiple similar privacy assessments that result in no meaningful benefit for consumers.

The CCPA requires the creation of regulations for privacy assessments where the processing "presents significant risk to consumers' privacy."[23] Because not all processing requires an assessment under the statutory text — only those processing activities that present a significant risk to privacy — the regulations should clarify that those processing activities that present a significant risk to consumers' privacy are those that involve profiling in furtherance of a decision with a legal or similarly significant effect concerning the consumer – i.e., decisions

---

[19] *See* Californians for Consumer Privacy, *California Privacy Rights Act Text,* Section 3(A)(8), available at: https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/#1798.140(v).

[20] VCDPA § 59.1-580; CTDPA § 8; CPA § 6-1-1309.

[21] VCDPA § 59.1-580(E) ("Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may comply under this section if the assessments have a reasonably comparable scope and effect."); CPA Regulations 8.02(B) ("If a Controller conducts a data protection assessment for the purpose of complying with another jurisdiction's law or regulation, the assessment shall satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section") ("If a data protection conducted for the purpose of complying with another jurisdiction's law or regulation is not similar in scope and effect… a Controller may submit that assessment with a supplement . . .").

[22] VCDPA § 59.1-580(E).

[23] Cal. Civ. Code § 1798.185(15).

about housing, education, employment, credit, and similarly important decisions.[24] Doing so would encourage "compatib[ility] with privacy laws in other jurisdictions" and focus requirements on those activities that present the most significant risk to consumer privacy.[25]

CalChamber asks the CPPA to draft a rule that recognizes that businesses can use a single privacy assessment to address multiple, similar processing activities. Businesses engage in a multitude of processing activities. Requiring separate privacy risk assessments for each activity would result in a significant operational burden without a corresponding benefit to California consumers' privacy. Instead, and as recognized by other U.S. state privacy frameworks,[26] the CPPA should promote a rule that allows businesses to use an assessment for multiple activities.

B. The CPPA Should Align Regulations With The Statutory Text And Other CCPA Rights And Requirements.

CalChamber supports the development of a principles-based framework for privacy assessments that incentivizes businesses to engage in a meaningful review of its processing activities and clarify how privacy assessments are consistent with other provisions of the statutory text and California law.

The CCPA statutory text is clear that privacy assessments must take into account (1) whether the processing involves sensitive personal information, (2) the benefits of the processing, and (3) the potential risks to the rights of the consumer.[27] Consistent with these instructions, the CPPA should advance a rule that requires businesses to engage in a principles-based balancing test to evaluate the privacy risks involved in processing. A prescriptive list of requirements not only imposes a substantial burden on businesses, but risks creating a process that will grow stale as changes in technology and processing outpace the list of considerations outlined in the regulation. Moreover, a principles-based balancing test allows businesses to tailor the privacy assessment to their industry, taking into account as the CCPA requires, the "size and complexity of the business and the nature and scope of processing activities."[28] For example, this principles-based approach could encourage a business to consider different technical and organizational measures and safeguards to mitigate risks, how reasonable

---

[24] CPA § 6-1-1309 (defining "Decisions that produce legal or similarly significant effects concerning a consumer" as a "decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services").

[25] Californians for Consumer Privacy, *California Privacy Rights Act Text,* Section 3(A)(8), available at: https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/#1798.140(v).

[26] VCDPA § 59.1-580(D).

[27] Cal. Civ. Code § 1798.185(15)(B).

[28] Cal. Civ. Code Ann. §§ 1798.185(15), (15)(A).

consumer expectations might differ, and the context of the relationship between the business and the consumer. Instead of setting forth a list of required considerations, CalChamber urges the CPPA to adopt a framework for privacy assessments that asks the business to reasonably balance the risks of processing personal information against the benefits and safeguards.

In addition, rather than requiring businesses to provide assessments to the CPPA annually, CalChamber asks the CPPA to harmonize assessment requirements with the CPPA's audit right. A business should only be required to provide assessments to the CPPA when specifically requested as part of the CPPA's ability to audit the business.[29]

The regulations should also state explicitly that privacy assessments will not be subject to public disclosure under the California Public Records Act. Under the California Public Records Act, individuals can request access to public records unless an exception applies. Absent an exception, entities may be hesitant to undertake a meaningful and thorough assessment of privacy risks out of concern that such information would become subject to public review. Recognizing this reality, Virginia, Colorado, and Connecticut's privacy statutes specify that privacy assessments will not be subject to public records requests.[30] CalChamber asks the CPPA to align the regulations with existing legal frameworks and clarify that privacy assessments are not subject to public disclosure.

III. Regulations Should Advance Automated Decisionmaking Access & Opt-Out Rights That Promote Consistency With Existing Legal Frameworks, Promote Innovation And Socially Beneficial Technologies, And Protect Trade Secrets.

CalChamber appreciates the opportunity to provide input on the scope of access and opt-out rights for automated decisionmaking. Automated decisionmaking technologies offer tremendous opportunities to improve lives and tackle a diverse array of societal challenges, from disaster recovery and resilience[31] to reducing climate impact.[32] At the same time, CalChamber appreciates that businesses should act as trustworthy stewards of automated decisionmaking

---

[29] California Consumer Privacy Act Regulations, § 7304(a)-(c) (providing the CPPA with the right to at any time, announced or unannounced, audit the business, contractor, of service provider for compliance with the CCPA).

[30] *See* VCDPA § 59.1-580(C); CPA § 6-1-1309(4); CTDPA § 8(c).

[31] *See* Ashley van Heteren, et al., *Natural disasters are increasing in frequency and ferocity. Here's how AI can come to the rescue*, World Economic Forum (Jan. 14, 2020), https://www.weforum.org/agenda/2020/01/natural-disasters-resilience-relief-artificial-intelligence-ai-mckinsey/#:~:text=AI%20algorithms%20could%20instantaneously%20assess,and%20isolated%20from%20escape%20routes.

[32] *See, e.g.*, Karen Hao, *Here are 10 ways AI could help fight climate change*, MIT Technology Review (Jun. 20, 2019), https://www.technologyreview.com/2019/06/20/134864/ai-climate-change-machine-learning/.

technologies, including by taking steps to help "consumers understand more fully how their information is being used and for what purposes."[33]

A. Regulations Should Define Automated Decisionmaking To Promote Coherence Across Legal Frameworks And To Promote Consumer Privacy And Innovation.

Regulations related to automated decisionmaking should apply to the use of technology that: (1) results in profiling in furtherance of decisions with legal or similarly significant effects concerning the consumer; (2) makes a final decision; and (3) is not subject to human involvement. Not only would a definition of automated decisionmaking that reflects these components promote goals of interoperability and consistency across existing legal frameworks,[34] but it would also strike the appropriate balance between promoting consumer privacy and facilitating the development of socially beneficial innovation. Under this approach, the regulations would address those activities that present a heightened risk of harm to California consumers. Additionally, the definition of automated decisionmaking should be scoped to final decisions, as automated decisionmaking tools often serve as the components of a larger system or set of decisions, and requiring an opt-out for any and all intermediary outputs before a final decision is reached would be unworkable and significantly disrupt consumers' use of such technologies. Additionally, rights related to automated decisionmaking technology should be scoped to those decisions made without human involvement. Clarifying in the regulations that consumer rights apply to "solely" automated decisionmaking would create consistency with existing global privacy frameworks,[35] further the statute's goals of encouraging innovation,[36] and focus legal requirements on processing likely to result in a heightened risk of harm to consumers.

---

[33] Californians for Consumer Privacy, *California Privacy Rights Act Text,* Section 2(G), available at: https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/#1798.140(v).

[34] All other comprehensive U.S. state privacy laws that address automated decisionmaking limit the opt-out right to profiling in furtherance of legal or similarly significant effect. *See, e.g.*, VCDPA § 59.1-577(A)(5)(iii)); CPA § 6-1-1306(1)(a)(C)) (hereinafter "CPA"); CTDPA § 4(A)(5)(C). Additionally, the GDPR provides a right to opt-out of automated decisionmaking that "produces legal effects concerning him or her or similarly significantly affects him or her." *See* General Data Protection Regulation, Article 22.

[35] *See, e.g.*, VCDPA § 59.1-577(A)(5)(iii)); CPA § 6-1-1306(1)(a)(C)); CTDPA § 4(A)(5)(C); GDPR Article 22.

[36] *See* Californians for Consumer Privacy, *California Privacy Rights Act Text,* Section 2(G), available at: https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/#1798.140(v).

B. Regulations Should Clarify That Certain Automated Decisionmaking Is Not Subject to Opt-Out and Access Rights.

Regulations addressing access and opt-out rights for automated decisionmaking should identify that certain activities are not subject to the rule. Failure to do so would make the regulations unworkable with respect to certain technologies and services. For example, although some consumers could exercise a right to opt-out of engaging with an automated vehicle that incorporates automated decisionmaking, a bystander may not be able to do so. Moreover, not recognizing certain exceptions could undermine consumer privacy and safety. For example, automated detection tools protect consumers online from fraud and help organizations root out future fraudulent activities.[37] Similarly, automated decisionmaking tools help identify and defend against cybersecurity attacks.[38] The statutory text contemplates a number of exceptions that echo the principles behind these exclusions – processing to comply with legal requirements and to exercise and defend legal claims, as examples.[39] Of course, these exceptions would continue to apply, though CalChamber requests that the CPPA also clarify specific activities that would be out of the scope of the automated decisionmaking rights, such as efforts to detect and prevent fraud, promote security, protect the safety of individuals, and promote fairness.[40] These exemptions are necessary to protect consumer privacy and wellbeing and should not be subject to an opt-out right, which would hinder a business's ability to further goals of safety, fairness, and security.

C. Regulations Should Permit Businesses To Provide "Meaningful Information" Through Its Conspicuously Posted Privacy Policy Or Other Conspicuous Resources And Should Not Require Disclosure Of Trade Secrets.

CalChamber shares the CPPA's goals of promoting transparency and helping California consumers understand how their personal information is collected, processed, and disclosed. To achieve this objective, the CPPA should clarify that "meaningful information" about automated decisionmaking is informed by the statutory text and prioritizes providing consumers with information that will be most useful to them. The CPPA need not invent new categories for disclosure and can look instead to the ingredients required to be disclosed by the

---

[37] *See, e.g.*, Darrell M. West, *Using AI and machine learning to reduce government fraud,* Brookings (Sept. 10, 2021), https://www.brookings.edu/research/using-ai-and-machine-learning-to-reduce-government-fraud/.

[38] *See, e.g.*, Victor Dey, *How AI cybersecurity tools tackle today's top threats*, Venture Beat (Dec. 15, 2022), https://venturebeat.com/ai/how-ai-security-enhances-detection-and-analytics-for-todays-sophisticated-cyberthreats/.

[39] Cal. Civ. Code § 1798.145(a)(1), (5).

[40] *See, e.g.*, American Data Privacy Protection Act (H.R. 8152) (2022) (recognizing that activities related to "diversifying an applicant, participant, or customer pool" would not be subject to the statute's prohibition on discrimination).

statutory text and regulations: categories of personal information collected to make the decision, as well as identification of whether the business uses or discloses sensitive personal information as part of the automated decisionmaking.[41] This approach is consistent with the Findings and Declarations accompanying the statute, which note that "[i]n the same way that ingredient labels on food help consumers shop more effectively, disclosure around data management practices will help consumers become more informed counterparties in the data economy, and promote competition."[42] Technical jargon about the interworkings of the automated decisionmaking tool is unlikely to provide consumers with meaningful information. Instead, and like an ingredient label, a disclosure that prioritizes the component parts of the processing already recognized in the statute would provide consumers information in a digestible format.

Regulations also should clarify that businesses can provide information about automated decisionmaking in the location where consumers review information about the business's privacy practices – their conspicuous privacy policy required under the statute. Additionally, CalChamber encourages the CPPA to recognize that businesses have latitude to determine where the disclosure would be most effective for a consumer, such as the privacy policy or another resource where a consumer is likely to encounter it.

Moreover, CalChamber asks the CPPA to take the opportunity in the regulations to clarify that access requirements for automated decisionmaking and related obligations should not be construed to require the business to disclose trade secrets. In coordination with Section 1798.185(a)(3), which requires the CPPA to establish exceptions necessary to comply with intellectual property rights and trade secrets,[43] recognizing this exception would "giv[e] attention to the impact on business and innovation" and strike an appropriate balance between providing consumers with meaningful information about the use of their personal information and facilitating businesses' ability to continue to develop socially beneficial technology and services.

---

[41] *See* California Consumer Privacy Act Regulations, § 7011.

[42] *See* Californians for Consumer Privacy, *California Privacy Rights Act Text,* Section 2(G), available at: https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/#1798.140(v).

[43] *See* Cal. Civ. Code § 1798.185(a)(3); *see also* Cal. Civ. Code § 1798.100(f).

* * *

CalChamber looks forward to an ongoing dialog with the CPPA on these important topics throughout the next stage of the rulemaking process.

Sincerely,

/s/

Lindsey Tonsager
Jayne Ponder
Hensey Fenton
Counsel for CalChamber