Comments by the Centre for Information Policy Leadership (CIPL) on the California Privacy Protection Agency's Notice of Modifications to Text of Proposed Regulations and Additional Materials Relied Upon

Submitted June 2, 2025

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the California Privacy Protection Agency's (the Agency)'s Notice of Modifications to Text of Proposed Regulations and Additional Materials Relied Upon.[2] CIPL commends the Agency for the steps it has taken to clarify key concepts, tailor heightened obligations for processing that may present significant risk, and reduce regulatory burdens, while striving to ensure a high level of data privacy and security and enable beneficial data use. CIPL notes with appreciation that the Agency has incorporated many of the key suggestions offered in its comment submitted in February (available here).[3] CIPL's comments below identify opportunities to further strengthen the rules via a risk-based approach grounded in concepts of organizational accountability.[4]

Article 1. General Provisions

§7001 Definitions

- The agency has taken useful steps to clarify the definition of **automated decisionmaking technology (ADMT)** at §7001(e). The application of a risk-based approach to the obligations for ADMT is vital, and the Agency advances this through the associated concept of "**significant decision**." The new definition of significant decision at §7001(ddd) helpfully clarifies circumstances in which ADMT activities will necessitate a risk assessment as per §7150(b)(3) and be subject to the requirements under Article 11. It more clearly focuses on processing activities likely to pose higher risks to individuals than the definition that previously appeared within the

---

[1] **The Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

[2] The Notice of Modifications to Text of Proposed Regulations and Additional Materials Relied Upon can be found here: https://Agency.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_notice.pdf

[3] CIPL Response to the California Privacy Protection Agency's Draft CCPA Updates, Insurance, Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking Technology (ADMT) Regulations, submitted February 25, 2025, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_public_comments_Agency_regulations_risk_assessments_automated_decisionmaking_technology.pdf.

[4] CIPL Report, "What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework" (May 2020), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_mapping_report_27_may_2020__v2.0.pdf.

text of §7150. The exclusion of "advertising to a consumer" from the definition is especially helpful in this regard.

- At the same time, further changes could be helpful for sharpening the focus of the obligations in connection with the Agency's consumer privacy mandate and providing businesses with necessary clarity. The Agency should:

  - Add a materiality threshold to the definition of significant decision, so that it applies to activities that have "material adverse legal or economic effects."

  - Modify §7001(e)(2) to indicate that profiling is included within the definition of ADMT only to the extent that it is used to produce a significant decision.

  - Modify §7001(ddd)(B)(4) to remove "allocation or assignment of work." Allocation of assignments is a lower-risk activity with respect to consumers while constituting an important aspect of businesses' operations.

  - Bind the language on compensation to focus on decisions with material adverse legal or economic effects and to exclude activities that do not meet this threshold, such as routine administrative actions needed to process payroll.

  - Limit "financial and lending services" to a more clearly delineated set of high-risk activities. For example, the "provision" of deposit and checking accounts, transmitting funds, and facilitating installment payments may all capture lower-risk processing to operate existing accounts; the language should focus more specifically on the "opening" of accounts. Greater clarity should also be provided as to how these obligations will work with respect to the Gramm-Leach-Bliley Act (GLBA) exemptions specified in the law.

  - Explicitly exclude from the definition technology and decisions intended to detect and respond to security incidents and resist malicious, deceptive, fraudulent, or illegal actions.

  The concept of "**profiling**" subject to heightened regulatory obligations should be limited to activities that effectuate a significant decision concerning a consumer. The current scope of regulations would extend risk assessment requirements to many beneficial profiling decisions that do not present significant risk to consumers' privacy and security, thereby burdening businesses with compliance processes that do not provide meaningful privacy and security protections to consumers. Importantly, the current approach contravenes the statutory requirement to issue regulations requiring risk assessments for processing that presents significant risk.[5] As currently drafted, businesses would need to complete risk assessments for low-risk profiling decisions such as automated processing that predicts a person's font or music preferences in a particular software or application. The current definition is also likely to capture longstanding, uncontroversial systems that employers and managers use in the workplace. For example, even rudimentary systems that track metrics like production, sales targets, or staffing levels all "analyze" "performance at work," and simple software that tracks whether employees are late to

[5] Cal. Civ. Code § 1798.185(a)(14) (2024).

clock in to work analyzes "reliability." These systems do not replace human decisionmaking, make significant decisions, or pose any consumer privacy risk.

- The concept of "**automated processing**" appears several times throughout the modified rules and is important in the definition of profiling (§7001(ii)) as well as the rules for determining when a risk assessment must be completed (§7150(4) and (5)). The phrase appears intended to address instances where processing is *solely* automated. The text should clarify this scope accordingly.

- The Agency should align the definition of "**penetration testing**" (§7001(bb)) with the most current definition provided by the U.S. National Institute of Standards and Technology (NIST).[6] This modification would foster interoperability with other data privacy and security rules and standards, consistent with the CCPA's instruction to "cooperate with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections."[7]

- The revised definition of "**physical or biological identification or profiling**" at §7001(ee) should be further tailored by introducing an intent standard, so that the obligations apply to systems intended to be used to identify individuals and exclude systems not used for identification purposes. The intent requirement should consider whether developers and deployers of biometric technologies take reasonable measures (e.g., technical, organizational, and contractual) to ensure that the processing of biometric characteristics cannot be used for identifying purposes.[8] Adding this intent standard would align this definition with the statutory definition of "biometric information", where data is in scope if it is "is used or is intended to be used" for identifying purposes.[9] Furthermore, emotion recognition should only be within scope to the extent that it is used to make a significant decision or to identify or recognize a consumer.

- The definition of "**systematic observation**" at §7001(eee) should be revised to clarify that it applies to truly systematic recordings, such as CCTV and video surveillance, which present a greater degree of risk then other types of recording (such as recording of business meetings).

§7004 Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent

- The symmetry in choice requirement (§7004(a)(2)(A)) should reflect that there may be a different number of steps needed for a consumer to opt in (e.g., through a single click) versus opt out of sharing information – which could, for example, necessitate follow-on verifications. The regulations should require symmetry as a general principle but not limit opt outs to the "same or fewer" steps in all instances.

---

[6] NIST has provided different definitions in different publications; the most recent dates from November 2022 and is based on the definition from ISO/IEC 19989-3:2020. See https://csrc.nist.gov/glossary/term/penetration_testing.

[7] Cal. Civ. Code § 1798.199.40.

[8] For more on this topic, please see CIPL, *Enabling Beneficial and Safe Uses of Biometric Technology Through Risk-Based Regulations*, April 2024.

[9] Cal. Civ. Code § 1798.140(c).

- The Agency should take care to ensure that the proposed prohibition on "general or broad terms of use" (§7004(a)(4)(C) within choice architecture is not in tension or conflict with the broader requirements of the law for business to provide Notice at Collection.

Article 3. Business Practices for Handling Consumer Requests

- With respect to the requirement in §7020(e) to provide consumers the ability to specify a date range for "requests to know", the regulations should acknowledge that a business should only be expected to respond with respect to information that the business continues to maintain.
- With respect to obligations related to Requests to Correct, the Agency should restore the "implement measures to" language stricken from §7023(c) in the most recent version. Doing so would appropriately task the business with striving to keep corrected information accurate but recognize that its ability to do so may be affected by factors outside its control.
- The Agency should add language indicating that where illustrative examples are provided, such as under §7023(m)(2) and (3), those examples are not meant be exhaustive.

Article 10. Risk Assessments

CIPL appreciates the Agency's effort to clarify and simplify the risk assessment requirements using an approach tiered to the level of likely risk. The updated draft regulations are more aligned with the statutory requirement to produce risk assessments when processing may pose significant risk.

- The regulations include some requirements that add administrative burden without corresponding privacy benefits for consumers. For example, the obligation set forth in § 7157(b)(3) to submit to the Agency information about the number of risk assessments conducted or updated *for each processing activity* would require businesses to link each risk assessment to individual processing activities, even though processing activities may cross over multiple risk assessments and a single risk assessment may cover multiple processing activities. In addition, the obligation set forth in § 7155(a)(2) to review and update as necessary all risk assessments would impose undue burden in light of the obligation to update the assessment where there are material changes in processing practices set forth in § 7155(a)(3).

- In our previous submission, CIPL noted that §7050(h)(2) and §7153(a) appropriately acknowledge that service providers may have a role to play in assisting customers ("recipient-businesses") with meeting their risk assessment compliance obligations. The Agency has taken useful steps to adjust the language in these sections to avoid misaligned expectations between recipient-businesses and service providers on roles and responsibilities with regards to risk assessments. The Agency should amend the language further to ensure that the obligations under §7050(h)(2) and §7153(a) do not pose an undue and unintended burden on service providers. Because service providers may have a high number of customers needing support for their risk assessments, the regulations should explicitly enable service providers to share information with their business customers in a standardized and readily replicable way about how their products and services work. Additionally, service providers should not be required to disclose trade secrets or intellectual property when complying with these obligations (see below).

- §7150(b)(6), which enumerates when processing poses a significant risk to consumers' privacy, includes training of ADMT for a list of enumerated purposes "or profiling of a consumer." The "or" introduces uncertainty as to the intended scope of the provision. CIPL

recommends that profiling be included only to the extent that it is associated with activities that make a significant decision concerning a consumer, consistent with the suggestion regarding the definition of profiling above.

- The draft regulations would require the participation of a number of individuals to conduct risk assessments that are not always needed. For example, § 7151(a) states that employees whose job duties include participating in the processing of personal information that would be subject to a risk assessment must be included in the risk assessment process for the relevant activity. Section 7152(a)(8) further states that risk assessment must identify and document individuals who provided the information for the risk assessment, barring only legal counsel from this obligation. Many employees may have "job duties" that include participating in the processing of personal information or determining the methods whereby it will be processed. Requiring businesses to seek the feedback of every such person could require large expenditures of time and resources that would not necessarily enhance the quality of the risk assessment. As an alternative the Agency should require that businesses consult with an individual who is primarily responsible for the processing activity in question. The Agency should similarly revise the regulations such that businesses need not provide the name of every individual who provided information for the risk assessment and instead include, for example, the individual who has the authority to participate in deciding whether the business will initiate the processing that is the subject of the risk assessment.

- The draft regulations would prohibit the use of the phrase "to improve our services" in risk assessments (e.g., §7152(a)(1)) as well as in communications to consumers (§7222(b)(1)). CIPL urges the Agency to provide organizations flexibility to identify a range of potential improvements without identifying them granularly. The potential for new and unforeseen needs for product improvement to arise as technology and consumer interactions with products and services evolve necessitates greater flexibility.

- The Agency takes useful steps in §7156 to clarify interoperability mechanisms with risk assessment requirements in other states. The Agency should consider a more flexible approach that would allow a business to more readily rely on a single risk assessment to cover a set of similar and interconnected processing activities across states, provided that all substantive elements are included. Interoperability mechanisms for risk assessment obligations are extremely impactful as they allow businesses to harmonize compliance and technical processes and avoid procedural burdens, without impacting the level of privacy and security afforded to individuals.

- The Agency has added helpful language clarifying that ADMT Pre-use Notice Requirements (§ 7220(d)) and responses to Requests to Access ADMT (§ 7222(c)) are not required to include trade secrets or information that would compromise a business's ability to combat fraud or prevent and address security, safety, and illegal behavior. As CIPL suggested in its previous submission, the Agency should extend the same protections to risk assessments, e.g., with respect to requirements to describe the "logic" of ADMT at § 7152 (a)(3)(G) and required disclosures to "recipient businesses" of ADMT at §7153(a). Furthermore, the regulations should provide assurances that the Agency will protect the confidentiality of materials submitted by businesses related to risk assessments.

- The requirement that a member of the business's executive management team with specialist knowledge of risk assessments must attest, under penalty of perjury, that risk assessment information submitted to the Agency is true and correct (§ 7157(b)(5)) could have the unintended effect of deterring otherwise qualified individuals from leading data privacy management programs. The Agency could address this concern while preserving accountability by requiring attestation that the information is correct "to the best of [the individual's] knowledge" and removing the reference to perjury.

Article 11. Automated Decisionmaking Technology

The Agency has taken useful steps to tailor the ADMT requirements to situations more clearly meeting the proposed definition of the technology and posing higher risks while enabling beneficial uses of the technology. The removal of training from the list of uses in §7200 is especially important in this regard. The Agency has also helpfully simplified and clarified the rules on opt-out and requests to access.

- The Agency should restore and expand language in § 7221(b) indicating that a business is not required to provide consumers the ability to opt out of ADMT when the use of ADMT is necessary "to resist, prevent, and detect malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions," consistent with the language of ADMT pre-use notices (§ 7220(d)) and responses to Requests to Access ADMT (§ 7222(c)).