Response by the Centre for Information Policy Leadership to the California Privacy Protection Agency's Draft CCPA Updates, Insurance, Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking Technology (ADMT) Regulations

February 19, 2025

I. Introduction and Key Recommendations

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to submit comments in response to the California Privacy Protection Agency's (the Agency) proposed regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies (the Regulations) in accordance with the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA). CIPL's comments focus on the Regulations concerning risk assessments and automated decisionmaking technology.

Since 2001, CIPL has focused on promoting responsible and beneficial uses of data through **organizational accountability**. CIPL welcomes the Agency's focus on risk assessments and transparency—two fundamental elements of organizational accountability—in the Regulations.

In response to the Regulations, CIPL offers the following **general recommendations:**

- **Ensure that the Regulations remain technology-neutral** and **avoid prescriptive classifications, such as those** characterizing certain technologies or processing activities as presenting "significant risk". Technology-specific regulations can become outdated and fail to capture innovative processing activities that may produce significant risk while overregulating low-risk processing.

- **Limit heightened** regulatory **obligations** to the processing of personal information that **"presents significant risk to consumers' privacy or security",** as required by the CCPA.

- **Clarify** that businesses are not required to disclose **trade secrets** and **intellectual property rights** in response to verifiable consumer requests and risk assessment submissions.

- Ensure that the Regulations' use of "personal information" **does not conflict with the CCPA's definition, which specifically excludes** "publicly available information" (unless the publicly available information is "biometric information collected by a business about a consumer without the consumer's knowledge").

- **Align technical terms** and definitions with national and industry standards organizations, such as the National Institute of Standards and Technology (NIST).

---

[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.

- Create regulatory obligations that businesses can **meaningfully operationalize**.

- **Assess compliance** based on demonstrable **due diligence and good faith**, as required by the CCPA.[2]

Regarding **risk assessments**, CIPL offers the following key recommendations:

- **Tailor risk assessment obligations** for processing activities that present actual **significant risk** to consumers' privacy and security.

- Acknowledge that the identification of **risk** and **harm** is largely a **context-specific** exercise.

- **Ensure that regulatory classifications** of significant/high-risk or low-risk be **rebuttable through risk assessments** and **demonstrable** organizational methods and mitigations.

- Provide businesses with a **template** to guide preparation of **abridged risk assessments** and enable submission through the Agency's website.

- **Engage with data protection agencies** and **regulators outside of California** to establish interoperable risk assessment frameworks and templates with guidance to bridge legal and technical differences between legal systems.

Regarding **automated decisionmaking technology and profiling**, CIPL offers the following key recommendations:

- Focus on systems that are **both solely automated** and produce **legal or similarly significant effects**. Ensure that the Regulations are narrowly tailored to govern only access and opt-out rights.

- Recognize that meaningful **ADMT transparency** is **contextual.** Regulations governing ADMT system logic and likely outcomes should be **flexible enough to accommodate different contexts without requiring businesses to disclose trade secrets or intellectual property**.

- Employ **contextual, use-based evaluations** to promote ADMT accuracy and the implementation of appropriate non-discrimination safeguards.

II. General Recommendations

Given the pace of modern technological advancements, and to avoid regulations becoming quickly outdated, CIPL believes that any regulatory approach should avoid imposing technology-specific requirements to the greatest extent possible. Regulations should ideally be technology-neutral, and they should not be unnecessarily prescriptive. They should adopt a principle- and outcome-based approach that enables businesses to progress towards the achievement of specific outcomes (e.g., fairness, transparency, accuracy, human oversight) through risk-based, concrete, demonstrable, and verifiable internal and external measures, regardless of the types and state of technology in use.

[2] Cal. Civ. Code § 1798.199.100 (2018).

Generally speaking, prescriptive classifications of technologies or of processing activities as "significant risk" should be avoided, unless required by the underlying statute. To the extent regulations nevertheless classify a certain technology or processing activity as presenting significant risk (especially in the absence of a statutory mandate), businesses should be able to treat such classifications as rebuttable presumptions (discussed further in Section III).

As noted below, CIPL believes that the Agency's Regulations appear to unduly broaden many concepts from the CCPA, thereby creating more expansive compliance obligations for regulated businesses. To the extent possible, the Agency should tighten definitions so as not to impede beneficial and low-risk processing activities. Overly broad regulations can hinder businesses from prioritizing and focusing resources on privacy-enhancing measures that minimize risks. Overly broad regulations can also burden the Agency itself by unnecessarily (and improperly) expanding its remit and forcing it to devote resources to activities that do not present significant risks to consumers' privacy and security.

CIPL submits that the following concepts appear to be unduly broad and/or inappropriately addressed by the draft Regulations, particularly when read in conjunction with the CCPA:

- The definition of "artificial intelligence" (AI) as proposed in § 7001(c) is unnecessary and outside the CCPA's statutory mandate to issue regulations governing ADMT access and opt-out rights.[3] The CCPA already acknowledges that personal information exists in various formats, including "artificial intelligence systems that are capable of outputting personal information".[4] The Agency's proposed definition is overbroad because it could, based on some interpretations, include non-AI technology that infers outputs from inputs.

- To the extent the Regulations propose to add and define technical terms—such as "artificial intelligence,"[5] "multi-factor authentication,"[6] and "penetration testing"[7]—CIPL recommends aligning its definitions with those drafted by national standards bodies, such as the National Institute of Standards and Technology (NIST), to prevent potential gaps and/or conflicts-of-law issues for businesses.

- The definition of "automated decisionmaking technology" (ADMT), as proposed in § 7001(f), is overbroad to the extent it covers technology used to generate a value or a score that is then used as a "key factor in a human's decisionmaking" or as a "primary factor to make a significant decision."[8] As drafted, it is not clear how to determine what a "key" or "primary" factor is. A list of non-exhaustive examples clarifying what may constitute a key/primary factor would be useful for effective compliance. In our previous submission to the Agency in March 2023,[9] we recommended that the Agency limit the scope of its regulations to ADMT and

---

3 Cal. Civ. Code § 1798.185(a)(15).
4 *Id.* at § 1798.140(v)(4)(C).
5 Cal. Code Regs. tit. 11, § 7001(c) (as proposed).
6 *Id.* at § 7001(w) (as proposed).
7 *Id.* at § 7001(dd) (as proposed).
8 Cal. Code Regs. tit. 11, § 7001(f) (as proposed).
9 CIPL Response to CPPA Invitation for Preliminary Comments on Proposed Rulemaking on Cybersecurity Audits, Risk Assessments and Automated Decision-making, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_cppa_invitation_for_preliminary_comments_on_proposed_rulemaking_on_cybersecurity_audits_risk_assessment_and_adm_-_march_27_2023.pdf.

profiling that *produce legal or similarly significant effects*. Such an approach would apply the CCPA's general requirements to low-impact or low-risk ADMT and profiling activities, but impose heightened regulatory requirements for activities that have legal or similarly significant effects. By adding "produces legal or similarly significant effects" to the definition of ADMT, the Agency can enforce heightened regulatory obligations on processing activities that pose the most significant risks or harms to consumers. As proposed, § 7001(f)(3)'s reference to "profiling" without the "legal or similarly significant effects" limitation will inadvertently capture many low-risk processing activities and overburden both businesses and the Agency.

- As proposed, the Regulations impose special requirements on businesses that use ADMT for "extensive profiling"[10] of a consumer—which specifically refers to work or educational profiling,[11] public profiling,[12] and profiling for behavioral advertising.[13] The concept of "extensive profiling," however, is unnecessary and beyond the scope of the statutory mandate. CIPL urges removal of this concept from the Regulations. The CCPA specifically defines profiling (without the modifier "extensive") and directs the Agency only to issue access and opt-out rights related to ADMT "including profiling."[14] Introducing the term "extensive profiling" expands the Agency's remit regarding profiling and includes many processing activities that may present low risk to consumers' privacy and security, especially as it relates to behavioral advertising. Behavioral advertisements include a wide range of beneficial targeted advertising practices based on a consumer's needs and preferences, such as whether she prefers to support small businesses, is in the market for a certain product (like furniture), or lives within the geographic area of a business. Furthermore, the proposed term's inclusion of "public profiling"—defined as profiling a consumer through systematic observation of a publicly accessible place—contradicts the exclusion of publicly available information from the scope of the CCPA.[15] As proposed in the Regulations, a "publicly accessible place" includes private businesses and areas where consumers do not have a reasonable expectation of privacy.[16]

- The *training* of automated decisionmaking technology should not be considered as a *use of ADMT*, as proposed in § 7200(a)(3), because the training of ADMT systems does not "execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking."[17] While the use of personal information to train ADMT is already covered by the general provisions of the CCPA, it should not fall within the scope of the Regulations, which focus on the use of the technology itself.

---

[10] Cal. Code Regs. tit. 11, § 7200(a)(2) (as proposed).

[11] "Profiling a consumer through systematic observation when they are acting in their capacity as an applicant to an educational program, job applicant, student, employee, or independent contractor ('work or educational profiling')," Cal. Code Regs. tit. 11, § 7200(a)(2)(A) (as proposed).

[12] "Profiling a consumer through systematic observation of a publicly accessible place ('public profiling')," Cal. Code Regs. tit. 11, § 7200(a)(2)(B) (as proposed).

[13] "Profiling a consumer for behavioral advertising," Cal. Code Regs. tit. 11, § 7200(a)(2)(C) (as proposed).

[14] Cal. Civ. Code § 1798.185(a)(15).

[15] Cal. Civ. Code § 1798.140(2)(A).

[16] Cal. Code Regs. tit. 11, § 7001(*ll*) (as proposed)

[17] "'Automated decisionmaking technology' or 'ADMT' means any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking." Cal. Code Regs. tit. 11, § 7001(f) (as proposed).

III. Risk Assessments

Risk assessments are key to organizational accountability and the responsible use of data. CIPL believes that accountable organizational governance must include contextual risk assessments to identify potential harms, mitigate risks, and promote beneficial and safe uses of personal information.

In addition, the purpose of a risk assessment is to assess the likelihood and severity of potential risks and harms associated with data use. Processing that involves "significant risk" is best measured through contextual risk assessments. Contextual risk assessments are especially useful for identifying and distinguishing significant, higher risks from lower risks. As such, CIPL encourages businesses to conduct basic risk assessments on all processing activities, even presumptively low-risk processing. A basic risk assessment, coupled with rebuttable guidance from regulators as to which types of processing activities are likely to involve significant risk, can identify processing activities that may potentially pose higher risk and therefore trigger the need for a more robust risk assessment (such as the type detailed in § 7152 of the Regulations[18]).

Importantly, any regulatory classification of processing activities presenting "significant risk," as proposed in § 7150(b) of the Regulations, should be able to be rebutted by an organization's comprehensive and contextual risk assessment. By creating a pre-determined, categorical list of the kinds of processing activities that present significant risk,[19] the Regulations may impede beneficial processing activities that do not warrant significant risk treatment in a given context (thereby resulting in overregulation), and may preclude effective mitigations where significant risk treatment would be warranted (resulting in under-regulation).

For example, as drafted, the Regulations classify all profiling related to behavioral advertising as involving significant risk (§ 7150(b)(3)(B)(iii)). This is concerning because in many cases, profiling a consumer for behavioral advertising will not involve significant risk to that consumer's privacy or security. For example, a business may "profile" a consumer as someone who is interested in furniture and process that consumer's personal information to display to them advertisements related to furniture providers. Businesses should be able to complete risk assessments to rebut the presumption that this kind of processing involves significant risk, and risk assessment submissions to the Agency should not be required when these determinations are made. However, businesses should maintain records of these risk assessments and submit them to the Agency or Attorney General when requested to do so.

CIPL recommends a risk-based approach supplemented with guidance to make risk assessments practicable and scalable, enabling case-by-case risk and mitigation determinations. Such an approach will avoid overregulating processing activities that do not present significant risk in certain contexts, and will avoid underregulating activities that do. The rebuttable presumption approach to the classification of significant risk and risk assessment submissions will also ensure that the Agency is monitoring processing activities that actually present significant risk (and not those that address only low-risk processing activities).

As drafted, § 7154 of the Regulations prohibits a business from processing personal information "*if the risks to consumers' privacy outweigh the benefits* to the consumer, the business, other stakeholders, and the public from the processing."[20] Thus, the Regulations do not suggest that risky

---

18 Cal. Code Regs. tit. 11, § 7152 (as proposed).
19 Cal. Code Regs. tit. 11, § 7150(b) (as proposed).
20 Cal. Code Regs. tit. 11, § 7154(a) (as proposed) [emphasis added].

processing is unlawful *per se*. Indeed, CCPA § 1798.185(14)(B) seeks to "restrict" *or* "prohibit" processing if the risks outweigh the benefits. Consistent with the statute, however, the Agency should acknowledge that risks assessments must include an assessment of the intended benefits, to be weighed against the identified risks, and should create a mechanism for businesses to seek guidance from the Agency when the outcome is unclear, close, or when risks may outweigh important benefits. Section 7154's outright prohibition of processing activity in all circumstances in which risks could potentially outweigh benefits is overbroad when read in light of the CCPA.

Sections 7050(h)(2) and 7153(a) rightly acknowledge that service providers may have a role to play in assisting customers ("recipient-businesses") with meeting their risk assessment compliance obligations.[21] As proposed, service providers must provide "all facts necessary" to support recipient-businesses conducting risk assessments.[22] As drafted, this may create misaligned expectations between recipient-businesses and service providers on roles and responsibilities with regards to risk assessments. CIPL recommends amending this language so that recipient-businesses and service providers can tailor expectations based on the nature of their relationship and the underlying processing. Specifically, the Agency should consider the GDPR's approach, which requires service providers to assist recipient-businesses complying with their obligations, "taking into account the nature of processing and the information available to the processor…".[23]

CIPL welcomes the Agency's regulation regarding a business's submission of abridged risk assessments for processing that involves significant risk and the ability to submit a certification of conduct when there are no material changes to the underlying processing activity. To encourage effective compliance with the requirements for submission of risk assessments, the Agency should provide businesses with a template to submit abridged risk assessments through the Agency's website.

The Regulations should also incorporate language reaffirming that businesses are not required to divulge trade secrets when submitting risk assessments to California public authorities, as stated in Section 1798.185(14)(B) of the CCPA. Relatedly, the Regulations should clarify that the disclosure of risk assessments in abridged and unabridged form does not constitute a waiver of any confidentiality, attorney-client privilege, or work-product protection that might exist with respect to any information contained within the risk assessment.

Finally, to promote efficiency and effective compliance, the Agency should engage with data protection agencies and regulators outside of California to establish interoperable risk assessment frameworks. This should also include the creation of templates to guide businesses when they must bridge legal and technical differences between legal systems and different risk assessment requirements. Completing comprehensive and contextual risk assessments is a resource-intensive

---

[21] *See* CIPL Report "Building Accountable AI Programs: Mapping Emerging Best Practices to the CIPL Accountability Framework" Sections 3.5 and 4.1 (Feb. 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_building_accountable_ai_programs_23_feb_2024.pdf.

[22] "In conducting the business's risk assessment pursuant to Article 10, including by making available to the business all facts necessary to conduct the risk assessment and not misrepresenting in any manner any fact necessary to conduct the risk assessment." Cal. Code Regs. tit. 11, § 7050(h)(2) (as proposed). *See also* "A business that makes automated decisionmaking technology or artificial intelligence available to another business ("recipient-business") for any processing activity set forth in section 7150, subsection (b), must provide all facts necessary to the recipient-business for the recipient-business to conduct its own risk assessment." Cal. Code Regs. tit. 11, § 7153(a) (as proposed).

[23] GDPR Article 28(f).

exercise and public authorities should provide businesses with as much consistency, support, and clarity as possible to encourage compliance. Ultimately, the Agency should maintain a flexible approach to risk assessment submissions so long as all substantive elements are included based on the context of the underlying processing. Businesses should also be allowed to rely on a single risk assessment to cover a set of similar and interconnected processing activities.

IV. Automated Decisionmaking Technology

With respect to profiling and automated decisionmaking technology (ADMT), CIPL acknowledges that the irresponsible use and application of profiling and ADMT can directly result in unfair discrimination, financial loss, reputational damage, social disadvantages and potential social and legal consequences for individuals. At the same time, both practices have the potential to provide great benefits for individuals, society, businesses and the economy – examples can be found in both public and private sectors, including healthcare, education, banking, insurance and marketing. Thus, if organizations carry out ADMT and profiling in a responsible manner, they can ensure effective and appropriate protection for individuals while enabling society, individuals and businesses to reap the benefits of machine learning and other relevant technologies.

The CCPA directs the Agency to issue regulations "governing access and opt-out rights with respect to a business's uses of automated decisionmaking technology, including profiling." (See Section 1798.185(15)). This is a narrow statutory directive; it does not authorize regulations addressing *all* aspects of ADMT and profiling. Indeed, the CCPA itself already addresses the processing of personal information, regardless of the circumstances or purposes.

As proposed, the Regulations cast a wide net for uses of ADMT. Consistent with CIPL's previous comment[24] to the Agency, the Regulations should focus on uses of ADMT and profiling that involve solely automated processing and produce legal or similarly significant effects. The Regulations' inclusion of training uses of ADMT as a *use of automated decisionmaking technology* under § 7200(a)(3) directly contradicts the definition of automated decisionmaking technology in § 7001(f) because the training of ADMT does not "execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking." In other words, the training of ADMT does not involve any decisions impacting consumer privacy and security.

Additionally, § 7200(a)(1) as drafted targets entire sectors rather than specific, high-risk activities. For example, instead of "financial or lending services," it should more narrowly address "credit or lending decisions." Rather than "healthcare services," it should address "diagnostic, planning, or care decisions." In short, the terminology used in this section is too broad to facilitate meaningful and risk-based compliance by covered businesses.

Moreover, § 7200 as drafted creates time- and resource-intensive requirements on businesses engaged in common and low-risk processing activities, which, in turn, would overburden the enforcement efforts of the Agency. For these reasons, the Regulations should focus principally on uses of ADMT that involve solely automated processing and produce legal or similarly significant effects.

---

[24] Response by the Centre for Information Policy Leadership to the CPPA's Invitation for Preliminary Comments on Proposed Rulemaking on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking, March 27, 2023, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_cppa_invitation_for_preliminary_comments_on_proposed_rulemaking_on_cybersecurity_audits_risk_assessment_and_adm_-_march_27_2023.pdf.

The inclusion of training uses of ADMT (as proposed in § 7200(a)(3)) is impracticable because ADMT developers are not always able to identify (or predict) the specific capabilities of ADMT. The regulations should instead encourage developers, given their resources and monitoring abilities, to identify the range of applications or tasks well suited for the technology, the applications or tasks for which it is not well suited, and any applications or tasks considered inappropriate.

Section 7221(b), as proposed, lists exceptions to the ADMT right to opt-out, e.g., when a significant decision is subject to appeal by a human reviewer; when ADMT is used for security, fraud prevention, and safety purposes; and when it is used for certain admission, acceptance, and hiring purposes, certain allocation of work and compensation purposes, and certain work and education profiling purposes. While these exceptions are welcome and allow businesses to execute necessary functions, they nevertheless can be overly prescriptive by limiting beneficial ADMT uses that do not pose significant risk to consumers. For example, the Regulations should not overly limit or constrict the security, fraud prevention, and safety exception. Section 7221(b)(1)(B) should be amended to expand its reach to include the **prevention** and **detection** of malicious actions. CIPL accordingly suggests that § 7221(b)(1)(B) be rephrased to say: "to resist***, prevent, and detect*** malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions."

Additionally, CIPL recommends including a catch-all exception to § 7221 for cases where a business can demonstrate a compelling reason not to provide consumers with the ability to opt-out of its use of ADMT, especially where the use does not pose a significant risk to the consumer's privacy and security.

Finally, the Agency should provide more guidance about how a business can comply with § 7221's opt-out rights when using personal information to train ADMT. In some cases, depending on the underlying technology, it may be unreasonable for a developer to erase personal information from a model. However, a developer should be permitted to apply technical solutions like output filters to satisfy an individual's opt-out request.[25] The Regulations should acknowledge these technical complexities. Further, in some cases, businesses should be able to comply with ADMT related opt-out rights by subjecting consumers that opt-out to manual processes instead of ADMT systems.

Due to the processing complexity surrounding some ADMT systems, the CCPA rightly acknowledges that the Regulations should establish meaningful access rights about ADMT logic.[26] Consumer access rights can help promote ADMT explainability, an essential principle for developing trustworthy ADMT. However, as written, the Regulations require businesses to provide overly detailed descriptions of ADMT processes that may go beyond what is required by the CCPA—at times contradicting language in the CCPA—and may require businesses to divulge trade secrets and intellectual property.

For example, the CCPA defines a "business purpose" to include, among other necessary activities, "[u]ndertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business". (See Section 1798.140(e)(8)).[27] Yet, §§ 7220(c)(1) and 7222(b)(1) of the Regulations prohibit

---

[25] CIPL Discussion Paper, "Applying Data Protection Principles to Generative AI: Practical Approaches for Organizations and Regulators" Dec. 2024, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_applying_data_protection_principles_genai_dec24.pdf.

[26] Cal. Civ. Code § 1798.185(a)(15).

[27] Cal. Civ. Code § 1798.140(e)(8) [emphasis added].

businesses from describing a business purpose with the terms, "to improve our services". This overly prescriptive and contradictory language could present serious compliance challenges for businesses seeking to protect trade secrets, intellectual property, and internal security and safety mechanisms. The Regulations should clarify that no ADMT-related regulations shall be construed as requiring a business to disclose trade secrets or intellectual property.

Additionally, §§ 7220(c)(5)(A) and 7222(b)(4) require businesses to explain the "key parameters" of the logic and the "intended output" of an ADMT system. This language is also overly prescriptive and could be construed as requiring businesses to divulge trade secrets. The Regulations should take care to safeguard businesses' legitimate interest in protecting their trade secrets and intellectual property rights while upholding consumer rights.

The Regulations exempt businesses from conducting direct evaluations to ensure that their use of ADMT works as intended and does not discriminate based upon protected classes if the business: 1) obtained the ADMT from another entity, 2) reviewed that entity's evaluation, and 3) implemented accuracy and non-discrimination safeguards.[28] However, where a business is deploying ADMT developed by another entity, the developer-entity's evaluation and safeguards cannot substitute for the business-deployer's own evaluation in the field under the proper use-case context. The accuracy and bias risks that may be associated with ADMT are extremely context-specific and will depend on the use case and underlying data. While CIPL encourages transparency and cooperation between developers and deployers in many cases, effective evaluation and accuracy and anti-discrimination safeguards must remain the responsibility of both developers and deployers. Moreover, the Regulations should acknowledge that businesses will at times need to test ADMT systems using representative samples to ensure their use of ADMT does not discriminate.

V. Conclusion

CIPL applauds the Agency for addressing important public policy concerns through the Regulations and the multiple rounds of public input that the Agency has facilitated. Our above comments and recommendations are meant to foster future proof and effective measures that promote a risk-based approach. CIPL believes that context-specific solutions are a prerequisite for facilitating and ensuring technology and business innovation and societal progress, while protecting the rights of individuals. Thank you for your consideration.

[28] Cal. Code Regs. tit. 11, §§ 7201(a)(1)(A); 7221(b)(3)(B)(i); 7221(b)(4)(B)(i); 7221(b)(5)(B)(i) (as proposed).