Submitted March 27, 2023

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

I. INTRODUCTION AND KEY CONSIDERATIONS

The Centre for Information Policy Leadership (CIPL) welcomes the opportunity to submit comments in response to the California Privacy Protection Agency (CPPA or the Agency)'s invitation for preliminary comments on proposed rulemaking on cybersecurity audits, risk assessments, and automated decisionmaking. CIPL is a global privacy and data policy think tank that works with industry leaders from over 85 members and project participants, regulatory authorities, and policymakers to develop global solutions and best practices for privacy and the responsible use of data.[1] This response focuses on risk assessments and automated decisionmaking (ADM). We use CCPA to refer to the California Consumer Protection Act as amended by the California Privacy Rights Act.

CIPL has a long history of promoting responsible data practices through its efforts regarding organizational accountability. When paired with clear guidance from regulators, organizational accountability supports businesses in achieving effective risk assessments and responsible decisions regarding data uses, including automatic decisionmaking.

Regarding **risk assessments**, CIPL offers the following considerations:

- Regulations or regulatory guidance should set forth the specific harms that should be identified and considered in a risk assessment.

- Prescriptive lists of scenarios, technologies or processing activities that are considered a "significant risk" should be avoided.

- Instead, it would be helpful to provide non-exhaustive lists describing 1) the kinds of high-risk processing operations that may require more detailed and robust risk assessments or data protection impact assessments and 2) the kinds of low-risk processing that likely do not.

- Risk mitigation does not mean the elimination of risk, but the reduction of risk to the greatest reasonable extent, given the desired benefits and reasonable economic and technological parameters. Regulations should help businesses make reasoned and evidence-based decisions on whether to proceed with processing in light of any residual

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

risks and taking into account proportionality.

- While the Agency should provide risk assessment templates detailing minimum requirements, it should maintain a flexible approach so long as all substantive considerations are included based on the context of the processing.

- Promote interoperability between jurisdictions and clarify through guidance how businesses can "bridge" technical differences between legal systems, such as the definition of "personal data".

- Provide businesses with clear guidance on what should be included in a risk assessment summary.

- Assess compliance based on demonstrable good faith and due diligence.

- Clarify that the disclosure of a risk assessment and summary in response to a request from the California Attorney General or the CPPA does not constitute a waiver of any attorney-client privilege or work-product protection that might exist with respect to any information contained in the risk assessment and summary.

- Recognize that identifying risk and harm is largely a **context-specific** exercise.

Regarding **automatic decisionmaking**, CIPL offers the following considerations:

- Instead of prohibiting all or certain categories of ADM while allowing for certain exceptions, focus rules on ADM that produces legal or similarly significant effects.

- For such regulated ADM, establish robust *ex ante* risk assessment and mitigation requirements, as well as other accountability obligations, such as transparency, human review, and robust *ex post* redress rights for erroneous or inappropriate decisions.

- Provide examples of automated decisions producing "similarly significant" effects.

- Examples of ADM producing legal or similarly significant effects should be rebuttable by businesses, as demonstrated through risk assessments.

- Clarify that businesses should find simple ways to inform individuals about the rationale behind or the criteria relied on in reaching the decision without providing a complex explanation of the algorithms used or disclosure of the full algorithm.

- Providing appropriate ADM transparency is contextual and rules on transparency should be flexible enough to accommodate different use cases.

- Clarify the scope of "profiling" by addressing solely automated activities that produce legal or significantly similar effects.

II. OVERVIEW OF THE CIPL ACCOUNTABILITY FRAMEWORK

CIPL's responses to the Agency's specific questions should be understood within the context of CIPL's broader work on how to implement effective and demonstrable organizational accountability. CIPL has developed an accountability framework (the CIPL Accountability Framework),[2] which, at its core, is a blueprint for responsible data practices. (See Figure 1).

The core elements in CIPL's Accountability Framework are: leadership and oversight; risk assessment; policies and procedures (including fairness and ethics); transparency; training and awareness; monitoring and verification; and response and enforcement. By encouraging businesses to implement comprehensive privacy and data governance programs based on CIPL's Accountability Framework (or other similar frameworks), CIPL has sought to ensure that businesses not only comply with applicable legal requirements and best practices but also that businesses demonstrate accountability to improve societal trust in how they use data.

Figure 1: CIPL Accountability Framework – Universal Elements of Accountability

As noted, accountability is a key building block for effective data protection and responsible data use. It operationalizes legal obligations and behavioral goals into concrete data protection controls, policies, procedures, tools and actions within a business. It also places responsibility on businesses to exercise judgment in their regulation of data processing and carry out contextual analyses to establish the level of risk created by their personal data processing and storage. Accountability is an ongoing internal change management process, requiring regular updates to keep pace with evolving laws, regulations, technology, and business practices.

Frequently (and ideally), businesses implement accountability via comprehensive organizational data privacy management programs (DPMPs) addressing all aspects of data governance, privacy law compliance and the data cycle—from collection and generation, to use, processing, and

[2] See CIPL resources and papers on organizational accountability, available here.

deletion. Because a key element of accountability is risk assessment, accountability focuses on, and prioritizes, mitigating the actual data processing risks to individuals. This approach enables businesses to implement legal rules and privacy protections more precisely and effectively. An accountability- and risk-based approach to data governance is a more effective and robust alternative to granular and rigid legal requirements that apply across the board regardless of the risks involved.

Another key element of accountability is that businesses must be able to demonstrate the existence and effectiveness of such DPMPs internally (e.g., to their Boards and senior management) and externally on request (to data protection and enforcement authorities, individuals, business partners, and increasingly, shareholders and investors). Implementing accountability also enables a company to build trust with consumers and business partners and respond to increased calls for digital responsibility.

Among other practices covered by the above framework, accountability expressly requires businesses to perform **contextual risk assessments** on their data uses that identify potential harms to individuals and the appropriate mitigation measures to minimize the risks. As noted in CIPL's recent response to the Federal Trade Commission's Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security,[3] contextual risk assessments can also help determine whether a particular use in each context will adversely affect different groups of individuals and how to mitigate such adverse impacts or harms (e.g. discrimination or bias).

An accountability-based framework for data use can enable full compliance with hard legal requirements, as well as enable contextual prioritization of compliance measures and safeguards that are tailored to the specific degree of risk. It also enables mitigations that are consistent with preserving as much as possible the intended beneficial data uses. Thus, organizational accountability focuses on the mitigation of actual risks to individuals and society and helps avoid unnecessary safeguards that undermine legitimate uses while facilitating strong safeguards in high-risk cases. As such, it is an indispensable tool for enabling responsible and beneficial data use. While CIPL's Accountability Framework was initially developed to help mitigate risks related to privacy harms, the framework and the risk assessments it entails can have broader application and can help address a broader range of risks associated with data use.

With respect to profiling and automated decisionmaking (ADM), CIPL acknowledges that the irresponsible use and application of profiling and ADM can directly result in unfair discrimination, financial loss, reputational damage, social disadvantages and potential social and legal consequences for individuals. On the other hand, 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 carried out in a responsible manner, profiling and ADM will ensure effective and appropriate protection for individuals while enabling society, individuals and businesses to reap the benefits of machine learning and other relevant technologies.

[3] Centre for Information Policy Leadership, "*Comments on the FTC's Advanced Notice of Proposed Rulemaking (ANPR) on Commercial Surveillance and Data Security*", November 21, 2022, available here.

III. RESPONSES TO SPECIFIC QUESTIONS

A. Risk Assessments

3. To determine what processing of personal information presents significant risk to consumers' privacy or security under Civil Code § 1798.185(a)(15):

a. What would the benefits and drawbacks be of the Agency following the approach outlined in the European Data Protection Board's Guidelines on Data Protection Impact Assessment?

Key Considerations:

- Regulations or regulatory guidance should set forth the specific harms that should be identified and considered in a risk assessment.
- Providing prescriptive lists of scenarios, technologies or processing activities that are considered a "significant risk" should be avoided.
- Instead, it would be helpful to provide non-exhaustive lists describing 1) the kinds of high-risk processing operations that may require more detailed and robust risk assessments or data protection impact assessments and 2) the kinds of low-risk processing that likely do not.

Risk assessments are designed to assess the likelihood and severity of potential harms associated with data use. Thus, they assess the level of risk that the harm will occur and the severity of the harm if it occurs. As a general matter, this is something that any business should know about all of its processing activities.

By statute, the goal of risk assessments under the CCPA is to restrict or prohibit the processing of personal information where the risks to a consumer's privacy or security outweigh any benefits to the consumer, business, other stakeholders, and the public. In doing so, businesses must specifically identify whether the processing activity includes sensitive personal information as defined by California law. What remains unclear is what kind of processing will, in fact, constitute "significant risk" to a consumer.

Processing that involves such "significant risks" can be identified through contextual risk assessments. Because processing activities range from very low-risks to high- and substantial-risks, it would be helpful to provide businesses guidance on the types of processing activities or examples of processing that might be high-risk or low-risk. Such classifications should be rebuttable through contextual risk assessments. Higher risk activities would require full-blown formal risk assessments, or data privacy impact assessments, and low-risk activities would not. However, rudimentary risk assessments would be required for all processing activities, even presumptively low-risk processing. Such initial, rudimentary risk assessments, coupled with guidance on what might be high-risk activities, could trigger more robust, full-blown data privacy impact assessments where a likelihood of a higher risk is identified or expected.

To conduct effective risk assessments, it would also be helpful if the Agency could provide guidance not only on what kind of processing activities might be high-risk or low-risk, but also on what kinds of harms should be considered and mitigated against through a risk assessment (e.g., financial harms, physical harms, reputational harms, intrusion harms, discrimination, bias, etc.)

All risk assessments, both initial, light-touch risk assessments and full-blown data privacy impact assessments, should consider the likelihood and severity of harms in the context of the processing operations at hand, but with varying degrees of detail and different documentation requirements. Adopting a risk-based approach focusing on how data (including "sensitive" or "high-risk" data) is used in specific contexts enables identification of the actual risk-level in that context as well as the appropriate mitigations for the identified risks. It also enables weighing the benefits of using such data against the risks of processing the data after mitigations have been implemented. All guidance or lists of potentially high-risk processing activities should be rebuttable by actual risk assessments. Similarly, businesses that engage in processing activities normally considered low-risk should be responsible for demonstrating that such activities are, in fact, low risk. Creating pre-determined, categorical lists of what kind of processing activities are always high-risk would result in both overregulating, thereby impeding beneficial processing activities that may not warrant high-risk treatment in a given context, and underregulating, by precluding effective mitigations where high-risk treatment would be warranted. A risk-based approach that provides guidance and guardrails for businesses to make risk assessments practicable and scalable would enable case-by-case risk and mitigation determinations and would help avoid overregulating processing activities that are not, in fact, high-risk in certain contexts, as well as underregulating activities that are, in fact, high risk in a given context.

Where a business cannot resolve or come to a decision around residual risk after all available mitigations have been considered and its processing activity appears to remain high-risk, consulting with the Agency may be helpful. In such consultations, the Agency would be able to limit or ban the processing, or, where the Agency deems the risks sufficiently mitigated or the benefits of the processing sufficiently valuable, to authorize the processing.

b. What other models or factors should the Agency consider? Why? How?

Key Considerations:

- Risk mitigation does not mean the elimination of risk, but the reduction of risk to the greatest reasonable extent, given the desired benefits and reasonable economic and technological parameters. Regulations should help businesses make reasoned and evidence-based decisions on whether to proceed with processing in light of any residual risks and taking into account proportionality.

The purpose of a risk assessment is not to establish whether there is any risk in the processing—almost all uses of personal data involve some kind of risk, and, generally, it is not possible to eliminate all risks. Instead, the purpose of a risk assessment, as acknowledged by California law, is to consider the severity of risk and to reduce it as much as is reasonable and practicable considering the intended benefits and the available mitigations and controls (e.g., state-of-the-art technology, cost of implementation, and best practices).

In CIPL's 2014 white paper *A Risk-based Approach to Privacy: Improving Effectiveness in Practice*, we offered a preliminary matrix of tangible and intangible harms that might be considered.[4] (*See* Annex). With respect to the risk assessment process itself, a "threshold", "light touch" or triage assessment is usually appropriate as early as possible in the product or service development stage and throughout development to establish whether a more detailed risk assessment is required for uses that may involve heightened risk.

As discussed in the answer to Question 3(a), risk assessments should consider the likelihood and severity of harms that individuals may experience, as well as the benefits of the intended data use to individuals, the business, and third parties or society, as the CCPA does. This enables the preservation of the desired benefits when implementing any necessary mitigations to address the identified risks.

As with harm, the assessment of benefits should include both the magnitude of benefit and its likelihood of occurring. The range of benefits should include benefits to individuals (e.g., ability to complete a transaction, obtain a desired good or service, be protected from fraud, etc.) and to the business (e.g., ability to attract customers, deliver goods or services more efficiently, and reduce fraud and other losses). They should also include benefits likely to be enjoyed by society more broadly (e.g., use of data for social good such as reducing the spread of infectious diseases, reducing environmental waste, delivering services to the public with greater efficiency and fairness, etc.).

Although this approach provides businesses with flexibility, it also requires sound judgment and a thorough understanding of the potential impact of the business's activities. A **key difficulty** is deciding in a consistent and repeatable manner what risks, harms, and benefits to individuals to consider, how to weigh them, and how to assess the likelihood and severity of the harm. Frameworks like the matrix in *Annex* are helpful for addressing this difficulty.

To facilitate standardizing risk assessments as much as possible (and desirable) and to avoid unnecessary risk assessments, it may be useful for the Agency to facilitate engagement and discussions on the risk taxonomy and methodologies to assess severity and likelihood of risk. The Agency should also produce guidance on the most common high-risk use cases and, where possible, provide a standard set of mitigating measures that businesses could apply. Businesses could still be entitled to depart from this guidance and implement different mitigating measures on the basis of a formal contextual risk assessment.

4. What minimum content should be required in businesses' risk assessments?

Key Considerations:

- While the Agency should provide risk assessment templates detailing minimum requirements, it should maintain a flexible approach so long as all substantive considerations are included based on the context of the processing.

The methodologies used to carry out a risk assessment are generally not formalized, though some regulators have released templates or tools that businesses may use or base their own

[4] CIPL, "*A Risk-based Approach to Privacy: Improving Effectiveness in Practice*", June 19, 2014, available here.

methodologies on. The CPPA should promote a format that allows it to prioritize review of conduct that may create the most harm to individuals or to democratic and social values.

The GDPR does not prescribe a particular format. Instead, it requires that an assessment contain, at a minimum, a systematic description of the proposed processing and the purposes of the processing, including, where applicable, the legitimate interest pursued by the business. In addition, it must include an assessment of the necessity and proportionality of the processing operations, an assessment of the risks to the rights and freedoms of individuals and the measures, safeguards, security measures and mechanisms implemented to ensure the protection of personal data and to demonstrate compliance with the GDPR, considering the rights and legitimate interests of the affected individuals. [5] The CPPA should also adopt an approach that provides flexibility in format around certain required elements.

Regulators do not generally expect businesses to carry out a new risk assessment for every new processing activity. Instead, businesses can rely on a single assessment to cover a set of similar and interconnected processing activities.

5. What would the benefits and drawbacks be for businesses and consumers if the Agency accepted businesses' submission of risk assessments that were completed in compliance with GDPR's or the Colorado Privacy Act's requirements for these assessments? How would businesses demonstrate to the Agency that these assessments comply with CCPA's requirements?

Key Considerations:

- Promote interoperability between jurisdictions and clarify through guidance how businesses can "bridge" technical differences between legal systems, such as the definition of "personal data".

The benefits, for companies that must comply with both the GDPR or the CCPA, include the ability to leverage existing templates, systems, policies, and procedures to streamline compliance. The purpose of risk assessments is to prevent harm. The Agency should accept risk assessments completed in compliance with other jurisdictions so long as the content and substance of the risk analysis and any potential mitigation procedures meet California requirements. To do so in a demonstrable way, the Agency should issue guidance detailing the specific potential harms to individuals that a risk assessment should consider.

Further, because of differences between legal systems, which include varying scopes for key definitions, including personal data, and varying triggers for when a risk assessment is required as a result of the different definitions, the Agency should provide guidance on how to bridge or address these differences in such submissions. For example, California law defines "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household". This definition is likely broader than Colorado's law, which defines "personal data" as "information that is linked or reasonably linkable to an identified or identifiable individual".

[5] Article 35 GDPR.

Colorado's definition is closer to the GDPR, which defines "personal data" as "information relating to an identified or identifiable natural person".

In sum, where similar processing activities must be assessed under various laws, the Agency should accept assessments submitted in other jurisdictions where the actual content and substance of the assessment is comparable between jurisdictions. The agency should provide guidance that enables interoperability between other risk-assessment frameworks and permit use of "bridging mechanisms", such as addenda, to address novel aspects of California law vis-à-vis the GDPR and the Colorado Privacy Act.

6. In what format should businesses submit risk assessments to the Agency? In particular:

a. If businesses were required to submit a summary risk assessment to the Agency on a regular basis (as an alternative to submitting every risk assessment conducted by the business):

i. What should these summaries include?

ii. In what format should they be submitted?

iii. How often should they be submitted?

The CCPA requires regulated businesses to submit risk assessments to the CPPA on a "regular basis". An appropriate interpretation of this requirement would avoid overwhelming both the Agency and regulated entities. A reasonable interpretation could be that a business must submit a risk assessment, preferably in summary form, for processing activities that meet a certain risk-level threshold once and then again in the event of any material changes to the processing, which could include changes in business models, risk, law, technology and other external and internal factors.

The Agency should provide an optional online template that businesses can use to submit their risk assessment summaries. This will give businesses notice regarding what is expected in the summary and help ensure consistent responses and ease of review for the Agency.

b. How would businesses demonstrate to the Agency that their summaries are complete and accurate reflections of their compliance with CCPA's risk assessment requirements (*e.g.*, summaries signed under penalty of perjury)?

Key Considerations:

- Provide businesses with clear guidance on what should be included in a risk assessment summary.
- Assess compliance based on demonstrable good faith and due diligence.
- Clarify that the disclosure of a risk assessment and summary in response to a request from the California Attorney General or the CPPA does not constitute a waiver of any attorney-client privilege or work-product protection that might exist with respect to any information contained in the risk assessment and summary.

One way for the CPPA to ensure complete and accurate summaries of risk assessments is through clear guidance on what should be included in a risk assessment summary. Additionally, regulated businesses should be assessed by reference to demonstrable good faith and due diligence in complying with such guidance. Moreover, organizational accountability generally, and any robust risk-assessment regime, requires businesses to maintain records of their accountability and compliance measures, as well as of their risk assessments. Thus, in the event of a concern with the processing operations of a particular regulated entity, the Agency should be able to go beyond the submitted summaries and obtain the full risk assessments related to that processing. This ability serves as an incentive to provide accurate and complete risk assessment summaries. Further, the Agency might clarify that preparing risk assessment summaries in good faith and in compliance with the requirements can serve as a mitigating factor in an enforcement context, which would serve as an additional incentive for providing complete and accurate risk assessment summaries. Finally, the CCPA appropriately provides that businesses that violate the law, including by submitting inaccurate or incomplete risk assessment summaries, should be held accountable through "vigorous administrative and civil enforcement". However, in order not to undermine good faith compliance efforts, punitive sanctions should mainly target non-compliant activity that is deliberate, wilful, seriously negligent, repeated or particularly serious.

The Agency should also clarify that the disclosure of a risk assessment in response to a request from the California Attorney General or the CPPA does not constitute a waiver of any attorney-client privilege or work-product protection that might exist with respect to the risk assessment and any information contained in the assessment.

In sum, the agency's powers to investigate, audit, and impose fines, coupled with clear statements on how good faith and due diligence in compliance can serve as mitigating factors in enforcement, provide businesses with a strong and effective incentive to submit complete and accurate risk assessment summaries.

8. What else should the Agency consider in drafting its regulations for risk assessments?

Key Considerations:

- Recognize that identifying risk and harm is largely a **context-specific** exercise.

Given the importance of the notion of heightened risk in the CCPA, and as discussed in the answers to Question 3, the Agency should create non-exhaustive, illustrative lists describing 1) the kinds of high-risk processing operations that may require more detailed and robust risk assessments and 2) the kinds of low-risk processing that likely do not. This would substantially aid and streamline the risk assessments process enable businesses to demonstrate, through risk assessments, that their particular use cases are not high risk, but would also require them to ensure that potentially low-risk processing activities included in such guidance are, in fact, low risk in their specific contexts. In other words, inclusion in a high-risk or low-risk list would be rebuttable by regulated entities based on context-specific risk assessments, and the burden to ensure an accurate assessment of risk would ultimately be on businesses.

As noted, the Agency should also issue guidance on the harms to be considered in a risk assessment. There is a wide range of possibilities for what might constitute cognizable harm.

There is some consensus that the term must include not only a wide range of tangible injuries (including financial loss, physical threat or injury, unlawful discrimination, identity theft, loss of confidentiality and other significant economic or social disadvantage), but also intangible harms (such as damage to reputation or goodwill, or excessive intrusion into private life). See Annex.

The notion of harm may also potentially include broader societal harms (such as contravention of national and multinational human rights instruments, loss of societal trust, damage to democratic institutions or any aggregate impact of harms to individuals). In such cases, difficult issues concerning the definition, identification, and concreteness of such harms and whether businesses are well placed to assess them, must be resolved, for example by identifying criteria and proxies for such societal harms that are objective and measurable. In addition, it must be clear that any consideration of societal impacts and harms must remain grounded in concrete risk to individuals, which, in turn, may have wider societal implications. What matters most is that the meaning of harm is defined through a transparent, inclusive process and with sufficient clarity to help guide the risk analyses of data users and that of regulators.

B. Automated Decisionmaking (ADM)

3. With respect to the laws and other requirements, frameworks, and/or best practices identified in response to questions 1 and 2,

d. What gaps or weaknesses exist in these laws, other requirements, frameworks, and/or best practices for automated decision making? What is the impact of these gaps or weaknesses on consumers?

f. Would you recommend that the Agency consider these laws, other requirements, frameworks, or best practices when drafting its regulations? Why, or why not? If so, how?

8. Should access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling, vary depending upon certain factors (e.g., the industry that is using the technology; the technology being used; the type of consumer to whom the technology is being applied; the sensitivity of the personal information being used; and the situation in which the decision is being made, including from the consumer's perspective)? Why, or why not? If they should vary, how so?

The following considerations, i.e., adopting the "legal or similarly significant effects" standard, explainability and transparency, and scope of profiling regulation, respond to aspects of Questions 3(d), 3(f), and 8.

Key Considerations – Adopting The "Legal or Similarly Significant Effects" Standard:

- Instead of prohibiting all or certain categories of ADM while allowing for certain exceptions, focus rules on ADM that produces legal or similarly significant effects.
- For such regulated ADM, establish robust *ex ante* risk assessment and mitigation requirements, as well as other accountability obligations, such as transparency, human review, and robust *ex post* redress rights for erroneous or inappropriate decisions.
- Provide examples of automated decisions producing "similarly significant" effects.
- Examples of ADM producing legal or similarly significant effects should be rebuttable by businesses, as demonstrated through risk assessments.

One of the most significant questions for ADM regulation is whether to require individual consent or limited other grounds for automated decisions, **or** to focus on ensuring accountable ADM, transparency, and effective remedies in the event of a problematic decision, particularly in the context of ADM that produces legal effects or similarly significant effects. CIPL strongly recommends the latter approach. The GDPR has been interpreted to prohibit ADM that produces legal or other similarly significant impacts unless it is based on consent, contractual necessity, or is authorized by law.[6] CIPL believes that enabling individual choice and consent in relation to ADM is too restrictive to ensure that the rules remain future-proof in light of the wide-spread reliance on ADM, machine learning, and artificial intelligence. Moreover, given the prevalence of ADM, a consent-based approach would further contribute to consent fatigue.

The GDPR approach of enabling ADM through a prohibition coupled with a range of exceptions seems unstainable in the long run. The exceptions currently provided in the GDPR for automated processing do not reflect all valid reasons for deploying and carrying out ADM, including a broad range of established and accepted processing practices where consent (opt-in or opt-out) is impracticable and the other current exceptions do not apply. For example, although Article 22(2) GDPR lists three processing grounds as exceptions to the prohibition, i.e., processing necessary for the performance of a contract, compliance with legal obligation, and consent, these exceptions may not be better or more relevant grounds for ADM processing than any of the other grounds for processing included in the GDPR, such as legitimate interest, public interest, and vital interest as valid bases, nor are they necessarily more protective of individuals' rights.[7] However, Article 22 GDPR does not recognize these other grounds for processing as exceptions to the prohibition of covered ADM. CIPL believes that a robust *ex ante* risk assessment coupled with appropriate mitigations and other accountability measures, including transparency and robust *ex post* remedial options in the case of erroneous or inappropriate automated decisions would be

[6] Article 29 Working Party, "*Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679*", Adopted on October 3, 2017, page 19. The Article 29 Working Party, is data protection advisory body in the EU and was replaced by the European Data Protection Board on May 25, 2018.
[7] CIPL White Paper, "*Recommendations for Implementing Transparency, Consent and Legitimate Interest Under the GDPR*", May 19, 2017, available here.

more effective in protecting and empowering individuals while also enabling ADM in line with the demands of the digital economy and society.

The CPPA's mandate to issue regulations under the CCPA may be interpreted broadly and is not currently limited to ADM with legal or similar effects. Significant benefits offered by ADM to consumers and business could be undermined or completely lost if consumers are granted overly broad opt-out rights. Thus, CIPL recommends that the Agency provide more guidance and clarity on the scope of the term "automated decisionmaking". In particular, the Agency should limit the reach of ADM regulation to *solely* automated decisionmaking that produces *legal or similarly significant effects* on individuals. Automated decision making that does not result in legal or similar effects would still be subject to the privacy protections and safeguards prescribed under the CCPA, but any additional ADM-related protections would only apply to solely ADM that have legal or similar effects on individuals.

Adopting the "legal or similarly significant effects" standard will have significant benefits that are workable and practical for individuals and businesses. First, the standard promotes interoperable solutions for businesses that have to comply with other domestic and global frameworks such as the Virginia Consumer Data Protection Act,[8] Colorado Privacy Act,[9] Connecticut Data Privacy Act,[10] EU GDPR,[11] UK GDPR[12] (also United Kingdom's draft Data Protection and Digital Information Bill),[13] and Brazil's LGPD.[14] Second, reading the standard in conjunction with the risk-based approach addressed above, businesses would bear the responsibility to identify and mitigate potential risks and harms associated with the covered ADM process. Mitigations could include human review of the ADM before deploying a new profiling or solely ADM process. Further, if a risk assessment shows that an ADM tool yields biased results, the business can recalibrate the specific ADM model to ensure fair outcomes. The "legal or similarly significant effects" standard has the benefit of capturing high(er)-risk use cases (e.g. automated processing based on race, gender, heath data), while providing greater leeway for automated decisions that do not rise to the level of having legal or similar effects on individuals (e.g., use of training data to build, improve, and enhance algorithms).

Furthermore, it is crucial to have the correct understanding of what constitutes a "legal" effect and a "similarly significant" effect. The concept of "legal effect" is relatively straightforward and can be defined as any impact on someone's rights or something that affects a person's legal status or their rights under a contract. The term "similarly significant" is more difficult. It implies that the effect of a decision based on solely automated processing must be similar in its significance

---

[8] § 59.1-573. (Personal data rights; consumers) A(5) of Consumer Data Protection Act, available here.
[9] Section 6-1-1306 (Consumer Personal Data rights) 1(a)(1)(c) of Colorado Privacy Act, available here.
[10] Section 4 (5) Connecticut Data Privacy Act, Senate Bill No 6, Public Act No 22-15 An Act Concerning Personal Data Privacy and Online Monitoring, available here. Please note that Virginia and Colorado privacy rules only allow opt-out rights for profiling in furtherance of decisions that product legal or similarly significant effects concerning the consumer. Thus, there is no opt-out right is provided if profiling not involved even if there is solely automated processing. Nevertheless, Connecticut provides opt out rights limited to solely automated decision-making that result in legal or similarly significant effects.
[11] Article 22 GDPR.
[12] Article 22 of the UK GDPR.
[13] Data Protection and Digital information (No 2) Bill, Article 22A-D, available here.
[14] Article 20 of the Brazilian Data Protection Law (LGPD) Law No 13853/2019, available here.

to a legal effect, hence, requiring similar additional safeguards such as risk assessments and appropriately tailored mitigations and redress rights. Although the determination of what constitutes a "similarly significant" effect is highly contextual, the following non-exhaustive criteria could assist in making the determination in cases where it is not clear if the automated decision produces such effects, keeping in mind the high threshold that needs to be reached:

- The duration of impact (temporary vs. permanent) of the automated decision on individuals;
- The severity and likelihood of risks and harms to individuals; and
- The impact of the automated decision at different stages of a decisionmaking process (i.e., does an initial or intermediary automated decision in a process produce a similarly significant effect or only the ultimate automated decision in that process).[15]

CIPL encourages the Agency to provide illustrative examples of legal and similarly significant effects and parameters for the threshold to be reached. This will provide clarity and consistency to businesses, especially to be considered during their internal risk assessment procedures. However, businesses should be able to rebut those examples in practice through risk assessments. The table below includes examples on automated decisions producing legal and similarly significant effects.[16]

CIPL Table on the Application Threshold	
Legal Effects	• Decisions affecting the legal status of individuals; • Decisions affecting accrued legal entitlements of a person; • Decisions affecting legal rights of individuals; • Decisions affecting public rights — e.g., liberty, citizenship, social security; • Decisions affecting an individual's contractual rights; • Decisions affecting a person's private rights of ownership.
Similarly Significant Effects *Some of these examples may also fall within the category of legal effects depending on the applicable*	• Decisions affecting an individual's eligibility and access to essential services — e.g., health, education, banking, insurance; • Decisions affecting a person's admission to a country, their residence or citizenship; • Decisions affecting school and university admissions; • Decisions based on educational or other test scoring – e.g., university admissions, employment aptitudes, immigration; • Decision to categorize an individual in a certain tax bracket or apply tax deductions;

[15] The UK ICO noted that certain factors may assist in this determination, such as the psychological effects of the decision and whether an individual knows that his or her behavior is being monitored. The Office of the Australian Information Commissioner (OAIC) has commented that the notion of a "similarly significant effect" under Article 22 is quite vague and believes that it should apply in the context of "bigger" decisions. The OAIC believes that some of the current draft privacy legislation in the United States could provide additional clarification in this context. For example, some draft laws propose a non-exhaustive list of "significant effects" which include, denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities and health care services.

[16] This table is based on one provided in our submission to the Article 29 Data Protection Working Party's "*Guidelines on Individual Decision-Making and Profiling*", on December 1, 2017, available here.

legal regime and the specific decision in question	• Decision to promote or pay a bonus to an individual; • Decisions affecting an individual's access to energy services and determination of tariffs.
Decisions <u>Not</u> Producing Legal or Similarly Significant Effects *CIPL believes these automated decisions do not typically produce such effects. Instances where they might produce such effects are contextual and should be determined on a case-by-case basis.*	• Decisions ensuring network, information and asset security and preventing cyber-attacks; • Decisions to sandbox compromised devices for observation, restrict their access to or block them from a network; • Decisions to block access to malicious web addresses and domains and delivery of malicious emails and file attachments (e.g., identifying child sex abuse material and content that is objectionable or inappropriate for minors); • Decisions for fraud detection and prevention (e.g., anti-fraud tools that reject fraudulent transactions on the basis of a high fraud score); • Decisions of automated payment processing services to disconnect a service when customers fail to make timely payments; • Decisions based on predictive human resources analytics to identify potential job leavers and target them with incentives to stay; • Decisions based on predictive analytics to anticipate the likelihood and nature of customer complaints and target appropriate proactive customer service; • Normal and commonly accepted forms of targeted advertising; • Web and device audience measurement to ensure compliance with advertising agency standards (e.g., requirements not to advertise foods high in fat, sugar and sodium when the audience consists of more than 25 % of children).

Key Considerations – Explainability & Transparency:

- Clarify that businesses should find simple ways to inform individuals about the rationale behind or the criteria relied on in reaching the decision without providing a complex explanation of the algorithms used or disclosure of the full algorithm.

- Providing appropriate AI transparency is contextual and rules on transparency should be flexible enough to accommodate different use cases.

Explainability is an essential principle for developing trustworthy automated decisionmaking models. In line with the NIST's Four Principles of Explainable AI,[17] CIPL recommends that the

[17] The National Institute of Standards and Technology prescribes the following principles for explainable AI systems: (i) explanation – a system delivers or contains accompanying evidence or reason for outputs and/or processes, (ii) meaningful – a system provides explanations that are understandable to the intended consumers,

Agency avoid providing access rights that require businesses to provide overly detailed descriptions of complex algorithms behind automated decisionmaking processes. This is particularly important to ensure that businesses can provide "meaningful" information to average consumers about the underlying automated decisions and its logics. Full transparency of algorithms (i.e., disclosure of source code or extensive descriptions of the inner workings of algorithms) is not meaningful to users and does not advance their understanding of how their data is being handled in ADM processes.

In addition, consumer access rights must be balanced with businesses' legitimate interests in protecting their trade secrets and similar types of information, e.g., intellectual property rights, that would be put at risk through detailed disclosure requirements. Further, if businesses are required to provide information regarding the use of ADM that constitutes a low-risk (e.g. decisions to block access to malicious addresses), it would create unnecessary burdens on businesses that do not benefit consumers. In that regard, transparency requirements should be both risk-based and principles-based, given that there are countless ADM contexts and appropriate transparency may look very different for one ADM application when compared with another. A principles- and outcomes-based regulatory approach allows businesses to decide how to achieve the required outcomes through a wide range of contextual mitigations and controls. Meanwhile, the Agency should encourage businesses to develop best practices for ADM transparency, as part of organizational accountability and responsible and ethical development and use of technology. Finally, the Agency should take an inclusive approach related to consumer access rights, for instance, by taking into account the needs of non-English speakers or people with inconsistent internet connection, so that all residents can seek access information related to the use of high-risk ADM.

Key Considerations – Scope of Profiling Regulation:

- Clarify the scope of "profiling" by addressing solely automated activities that produce legal or significantly similar effects.

CIPL believes that profiling and automated decisionmaking are distinct concepts although they are related and have the potential to impact individuals' rights and freedoms if carried out irresponsibly.[18] The CPRA defines "profiling" as any automated processing of personal information to evaluate personal aspects related to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preference, interests, reliability, behavior, location, and movements.[19] In that regard,

(iii) explanation accuracy – an explanation correctly reflects the reason for generating the output and/or accurately reflects the system's process, and (iv) knowledge limits – a system only operates under conditions for which it was designed and when it reaches sufficient confidence in its output. See NIST, "*Four Principles of Explainable Artificial Intelligence*", September 2021, Available here.

[18] While profiling effectively means collecting personal information and evaluating patters to analyze and make predictions, automated decision-making involves further action by taking decisions impacting the individuals.

[19] Section 1798.140 of the Civil Code, Section 14 Definitions (z).

the defined concept is aligned with international frameworks, such as Article 4(4) GDPR.[20] The definition suggests that in order for an activity to qualify as a profiling, it must consist of "any form of automated processing". CIPL suggests that the Agency clarify the concept and exclude processing from the scope if the actual use of the data to evaluate, analyze, or predict personal aspects is carried out with human involvement. For example, where data is collected by automated means, e.g., in online forms, and the subsequent evaluation, analysis or predictions are conducted manually, this should not equate to profiling, as the core activity (i.e., evaluation) is not automated processing. This does not mean such activity is not protected at all; rather, it will still be subject to all CCPA requirements and safeguards but not subject to additional requirements related to automated processing prescribed by the Agency.

In addition, as highlighted in our first recommendation above, the Agency's ADM regulation should specifically address profiling that results in solely automated decisions that produce legal effects or similarly significant effects on an individual. In that regard, different types of profiling would be proportionately and sufficiently protected, i.e., (i) general profiling, which can include non-solely automated decisionmaking and profiling that does not produce legal or similarly significant effects, that are subject to all the requirements and safeguards of the CCPA, and (ii) profiling that results in solely automated decisions producing legal effects or similarly significant effects on an individual, that is subject to all requirements and safeguards of the CCPA, *and* additional provisions that will be prescribed by the Agency.

4. How have businesses or businesses been using automated decisionmaking technologies, including algorithms? In what contexts are they deploying them? Please provide specific examples, studies, cases, data, or other evidence of such uses when responding to this question, if possible.

Please find below an illustrative table of examples of beneficial uses of standard data processing activities that include ADM and/or profiling.

Sector	ADM and/or profiling is used for:
Banking and Finance	• Credit scoring and approval; • Ensuring responsible lending; • Customer segmentation to ensure appropriate product offerings and protections; • Initiatives to know-your-customer; • Preventing, detecting, and monitoring of financial crimes; • Debt management; • Credit and risk assessments; • Fraud prevention; • Anti-money laundering efforts; • Preventing the financing of terrorism; • Detecting tax evasion; • Countering bribery and corruption;

[20] Article 4(4) GDPR defines profiling as "'*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements".*

	• Preventing cybercrimes.
Health	• Greater efficiency and precision in delivery of healthcare and medicines; • Increasing the accuracy of diagnoses; • Understanding syndromes and preventing recurrence; • Understanding links between particular symptoms and medicines; • Ensuring quality performance of physicians and medical staff.
Information and Network Security	• Cyber-incident prevention and diagnostics; • Network and information protection; • Personalization of Internet browsing sessions.
Insurance	• Underwriting risks and allocating premiums.
Human Resources	• Recruitment and the objective analysis of job applications; • Examining employee retention patterns; • People development and promotion; • Unlocking unused employee skills and abilities; • Obtaining insights into employee performance drivers; • Monitoring compliance with internal policies, codes of conduct and business ethics; • Screening for compliance with export control and economic sanctions laws; • Promotion of workplace diversity and inclusion.
Energy	• Predicting energy consumption; • Forecasting demand and supply levels; • Understanding usage peaks; • More efficiently detecting and responding to utility outages.
Education	• School and university admissions; • Promoting policies of affirmative action; • Using analytics to optimize learning environments.
Marketing	• Providing recommendations based on profiles, previous and peer purchases; • Loyalty programs – retail, hotel, travel services, etc.; • Customer segmentation.
Non-profit	• Identifying potential supporters and patterns of charitable behaviors.
Public Sector	• Detection of tax evaders; • Detection of social security and benefits fraud; • Focusing resources on appropriate cases for investigation; • Policing and law enforcement; • Public health and safety – predicting trends and preventing accidents.

C. CONCLUSION

An appropriately implemented risk-based approach to data use, automated decision making and profiling is vital for ensuring that the CCPA remains future proof and thus capable of delivering

effective privacy and data protection to individuals in the long run. Rather than creating one-size-fits-all rules and obligations that may soon be outdated, the risk-based approach provides a process with outcomes that can change with context and adapt to changing technologies and business practices. Thus, decisions about whether and how to proceed with certain processing operations will always be tailored exactly to the circumstances and thus more likely to be appropriate for the protection of the rights and freedoms of individuals. Such context-specific solutions are a prerequisite for facilitating and ensuring technological and business innovation and societal progress, as well as protecting individuals. This risk-based approach will also be most effective if there is an ongoing and open dialogue between regulated businesses, the CPPA, and law and policymakers about the constantly evolving technologies and business practices as well as the needs and expectations of individuals and society. The suggestions and recommendations in this paper are intended to highlight the substantial promise of the risk-based approach to data protection and privacy.

DRAFT - Risk Matrix

ANNEX

Risks	Unjustifiable Collection			Inappropriate Use Inaccuracies Not expected by individual Viewed as Unreasonable Viewed as Unjustified			Security Breach Lost Data Stolen Data Access Violation			Aggregate
	Likely	**Serious**	**Score**	**Likely**	**Serious**	**Score**	**Likely**	**Serious**	**Score**	**Risk Rank**
Tangible Harm										
Bodily Harm	0	0	0	0	0	0	0	0	0	**0**
Loss of liberty or freedom	0	0	0	0	0	0	0	0	0	**0**
Financial loss	0	0	0	0	0	0	0	0	0	**0**
Other tangible loss	0	0	0	0	0	0	0	0	0	**0**
Intangible Distress										
Excessive surveillance	0	0	0	0	0	0	0	0	0	**0**
Suppress free speech	0	0	0	0	0	0	0	0	0	**0**
Suppress associations	0	0	0	0	0	0	0	0	0	**0**
Embarrassment/anxiety	0	0	0	0	0	0	0	0	0	**0**
Discrimination	0	0	0	0	0	0	0	0	0	**0**
Excessive state power	0	0	0	0	0	0	0	0	0	**0**
Loss of social trust	0	0	0	0	0	0	0	0	0	**0**

Legend:

Rank 'Likely' from 10 (high) to 1 (low) based on the highest score for any component
Rank 'Serious' from 10 (high) to 1 (low) based on the highest score for any component

Aggregate Risk Rank:

Highest score is 300
Lowest score is 0

Proposed Processing:	THREATS						
	Unjustifiable Collection of Data	Inappropriate Use of Data				In Wrong Hands	
		Storage or use of inaccurate or outdated data	Use of data beyond individuals' reasonable expectations	Unusual use of data beyond societal norms, where any reasonable individual in this context would object	Unjustifiable inference or decision-making, that the organisation cannot objectively defend	Lost or stolen data	Data that is unjustifiably accessed, transferred, shared or published
Tangible Harm							
Bodily harm	how likely?	how likely?	how likely?	how likely?	how likely?	how likely?	how likely?
	how serious?	how serious?	how serious?	how serious?	how serious?	how serious?	how serious?
Loss of liberty or freedom of movement	how likely?	how likely?	how likely?	how likely?	how likely?	how likely?	how likely?
	how serious?	how serious?	how serious?	how serious?	how serious?	how serious?	how serious?

ANNEX

Damage to earning power	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
	how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	
Other significant damage to economic interests	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
	how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	
Intangible Distress														
Detriment arising from monitoring or exposure of identity, characteristics, activity, associations or opinions	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
	how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	
Chilling effect on freedom of speech, association, etc.	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
	how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	

ANNEX

Reputational harm	how likely?	how likely?	how likely?	how likely?	how likely?	how likely?	how likely?	
	how serious?	how serious?	how serious?	how serious?	how serious?	how serious?	how serious?	
Personal, family, workplace or social fear, embarrassment or anxiety	how likely?	how likely?	how likely?	how likely?	how likely?	how likely?	how likely?	
	how serious ?	how serious ?	how serious ?	how serious ?	how serious ?	how serious ?	how serious ?	
Unacceptable intrusion into private life	how likely?	how likely?	how likely?	how likely?	how likely?	how likely?	how likely?	
	how serious?	how serious?	how serious?	how serious?	how serious?	how serious?	how serious?	
Discrimination or stigmatization	how likely?	how likely?	how likely?	how likely?	how likely?	how likely?	how likely?	
	how serious?	how serious?	how serious?	how serious?	how serious?	how serious?	how serious?	

ANNEX

Societal Harm														
Damage to democratic institutions (e.g. excessive state or police power	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
	how serious ?		how serious ?		how serious ?		how serious ?		how serious ?		how serious ?		how serious ?	
Loss of social trust (Who knows what about whom?)	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
	how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	

ANNEX