
From: Doug Johnson [REDACTED]
Sent: Monday, March 27, 2023 2:37 PM
To: Regulations
Subject: PR 02-2023 - Comments from CTA
Attachments: CTA comments in response to CPPA Invitation for Preliminary Comments on Proposed Rulemaking, 3-27-23.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Attached please find comments from the Consumer Technology Association (CTA) in response to the "PR 02-2023" proceeding. Thank you.

Douglas Johnson
Vice President, Emerging Technology Policy
Consumer Technology Association, producer of CES®
d: [REDACTED]
[CTA.tech](#) | [CES.tech](#)

Disclaimer

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**, an innovator in Software as a Service (SaaS) for business. Providing a **safer** and **more useful** place for your human generated data. Specializing in; Security, archiving and compliance. To find out more [Click Here](#).

**Before the
CALIFORNIA PRIVACY PROTECTION AGENCY**

In the Matter of

**Invitation for Preliminary Comments on
Proposed Rulemaking – Cybersecurity Audits,
Risk Assessments, and Automated Decision
Making**

Proceeding No. 02-2023

COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION

The Consumer Technology Association® (“CTA”) submits this response to the California Privacy Protection Agency’s (“CPPA” or “the Agency”) Invitation for Preliminary Comments on Proposed Rulemaking - Cybersecurity Audits, Risk Assessments, and Automated Decision (“Invitation for Comment”).¹ CTA is North America’s largest technology trade association. Our members are the world’s leading innovators—from startups to global brands—helping support more than 18 million American jobs. CTA owns and produces CES®—the most influential tech event in the world.

The California Privacy Rights Act of 2020 (“CPRA”) directs the CPPA to issue regulations “governing access and opt-out rights with respect to businesses’ use of automated decision making technology, including profiling and requiring businesses’ response to access requests to include meaningful information about the logic involved in those decision making processes, as well as a description of the likely outcome of the process with respect to the

¹ Invitation for Preliminary Comments on Proposed Rulemaking - Cybersecurity Audits, Risk Assessments, and Automated Decision, PR No. 02-2023 (rel. Feb. 10, 2023) (“Invitation for Comment”).

consumer.”²

In response to the Agency’s call for comments CTA urges the CPPA to proceed with caution when considering whether, or what, regulations may be necessary to respond to this directive. Before adopting any new regulations the CPPA should first develop a robust record and undertake sufficient deliberation and consideration of both the benefits and risks presented by the use of automated decision making technology by covered providers. Any new regulations the CPPA adopts should be risk-based, flexible to account for different use cases, and narrowly tailored to avoid imposing undue burdens on small and medium sized enterprises.

In these comments, CTA outlines several factors that the CPPA should consider as it weighs its approach to rulemaking. First, in Part I, CTA describes the nascent development of automated decisionmaking technologies and the need for a flexible approach to regulation. Second, in Part II, CTA urges the CTA to ensure that any regulations of automated decisionmaking systems harmonize with existing state and federal laws and regulations. Third, in Part III, CTA outlines the potential of burdensome regulations to undermine the benefits that can be achieved using AI, especially for small and medium sized enterprises. Fourth, in Part IV, CTA urges the CPPA to adopt a risk-based and flexible approach to regulating AI. Finally, in Part V, CTA highlights the risks of implementing broad opt-out rights for automated decision making systems and suggests that any opt-out requirement should be narrowly tailored.

I. “Automated Decision Making” and the Technologies Underlying Such Systems Are Nascent Technologies Which Require Due Deliberation and Caution Before Adopting New Prescriptive Regulations

As the CPPA moves forward with this proceeding it is important to recognize the nascent nature of automated decision making systems and the technology supporting such systems,

² Codified at CA. Civil Code §1798.185(a)(16).

including artificial intelligence and machine learning (collectively “AI”). Indeed, a recent Federal Trade Commission (FTC) report found that AI is nascent, varied, and not susceptible to one definition.³ This suggests that regulators should proceed with caution in considering new rules that may unduly limit, burden or undermine the many benefits this technology offers to the public.

AI offers tremendous potential for human and societal development: promoting inclusive growth, improving the welfare and well-being of individuals, and enhancing global innovation and productivity. A growing body of research demonstrates that AI can identify and mitigate bias in human decision making.⁴ Perhaps the leading federal agency focused on AI governance and risk management, the National Institute of Science and Technology (“NIST”), has recently commented that “new AI-enabled systems are revolutionizing and benefitting nearly all aspects of our society and economy – everything from commerce and healthcare to transportation and cybersecurity.”⁵

³ See *Combatting Online Harms Through Innovation*, FTC, at 1 (June 16, 2022), available at https://www.ftc.gov/system/files/ftc_gov/pdf/Combatting%20Online%20Harms%20Through%20Innovation%3B%20Federal%20Trade%20Commission%20Report%20to%20Congress.pdf (“Combatting Online Harms Report”) (“AI is defined in many ways and often in broad terms. The variations stem in part from whether one sees it as a discipline (e.g., a branch of computer science), a concept (e.g., computers performing tasks in ways that simulate human cognition), a set of infrastructures (e.g., the data and computational power needed to train AI systems), or the resulting applications and tools.”).

⁴ See, e.g., Jon Kleinberg et al., *Discrimination in the Age of Algorithms*, 10 J. of Legal Analysis 113, 120 (2019), <https://academic.oup.com/jla/article/doi/10.1093/jla/laz001/5476086>; Cass R. Sunstein, *Algorithms, Correcting Biases*, 86 Soc. Rsch.: An Int’l Q. 499, 500 (2019), http://eliassi.org/sunstein_2019_algs_correcting_biases.pdf; Kimberly A. Houser, *Can AI Solve the Diversity Problem in the Tech Industry? Mitigating Noise and Bias in Employment Decision-Making*, 22 Stan. Tech. L. Rev. 290, 352 (2019), https://www-cdn.law.stanford.edu/wp-content/uploads/2019/08/Houser_20190830_test.pdf.

⁵ Moreover, NIST recognizes that AI “is rapidly transforming our world. Remarkable surges in AI capabilities have led to a wide range of innovations including autonomous vehicles and connected Internet of Things devices in our homes. AI is even contributing to the development of a brain-controlled robotic arm that can help a paralyzed person feel again through complex direct human-brain interfaces.” *Artificial Intelligence*, NIST, <https://www.nist.gov/artificial-intelligence> (last visited Oct. 1, 2022). See also *About Artificial Intelligence*, National Artificial Intelligence Initiative Office, <https://www.ai.gov/about/> (last visited Oct. 1, 2022) (explaining that investments in AI technology “have led to transformative advances now impacting our everyday lives, including mapping technologies, voice-assisted smart phones, handwriting recognition for mail delivery, financial trading, smart logistics, spam filtering, language translation, and more. AI advances are also providing great benefits to our social wellbeing in areas such as precision medicine, environmental sustainability, education, and public welfare.”).

Further, CTA members help promote the development of responsible and trustworthy AI through leadership in federated learning, a machine learning (“ML”) approach that learns from a user’s interaction with a given device while keeping all the training data on the device, so that the data does not need to be shared with a server. For example, Google recently published research on Entities as Experts AI, answering text-based questions with less data.⁶ Google has also published guidance for regulators on how to most effectively regulate AI in its *Recommendations for Regulating AI* paper.⁷ Indeed, CTA has supported efforts at the federal level to develop voluntary risk-based frameworks to address potential AI risks, while enabling stakeholders to maximize the benefits of this technology.⁸ In recent comments to NIST concerning the development of that agency’s AI Risk Management Framework (“RMF”), CTA applauded the agency’s work to create a flexible and voluntary risk management framework for managing AI risks, including those that may be implicated by the use of automated decision making systems.⁹

Released in January of this year, NIST’s AI RMF sets forth a voluntary framework to map, measure, manage and govern emerging AI risks.¹⁰ Significantly, in the RMF, NIST acknowledges the nascent nature of this technology,¹¹ and explicitly recognizes that risk mitigation frameworks must measure the benefits offered by AI systems, and that consideration

⁶ Eunsol Choi et al., *Entities as Experts: Sparse Memory Access with Entity Supervision*, Google Research (Oct. 6, 2020), <https://arxiv.org/pdf/2004.07202.pdf>.

⁷ Recommendations for Regulating AI, Google, <https://ai.google/static/documents/recommendations-for-regulating-ai.pdf> (last visited Oct. 3, 2022).

⁸ See, e.g., Consumer Technology Association Comments, RFI - NIST AI Risk Management Framework, Docket No. 21076-01510 (filed Sept. 15, 2021), available at <https://www.nist.gov/system/files/documents/2021/09/16/ai-rmf-rfi-0087.pdf>.

⁹ Comments of the Consumer Technology Association, AI Risk Management Framework, at 2 (filed Sept. 29, 2022), available at <https://www.nist.gov/system/files/documents/2022/11/16/Consumer%20Technology%20Association%20%28CTA%29.pdf>.

¹⁰ National Institute of Science and Technology, AI Risk Management Framework, (rel. Jan. 23, 2023), available at <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>

¹¹ *Id.* at 4.

of such benefits against risks is contextual and depends on “the values at play in the relevant context and should be resolved in a manner that is both transparent and appropriately justifiable.”¹²

NIST’s findings and decision to utilize a voluntary framework suggest it may be premature for the CPPA to move forward with broad restrictions on a nascent technology which offers the potential to dramatically improve consumer well-being. This is especially true given public and private sector efforts to establish voluntary risk management frameworks that are tailored to potential risks while still allowing AI to be deployed in beneficial ways. Given the increased use of these voluntary risk management frameworks and the fast-moving pace of development of this technology, the CPPA should proceed with caution and avoid adopting overly prescriptive rules. Specific restrictions on automated decision making systems’ use of AI or on data that seems unnecessary for those systems to function could undermine the many benefits of AI available now, and in the future.

For the same reason the National Security Commission on Artificial Intelligence’s Final Report did not recommend regulation for AI technologies due, in part, to the “speed of technology development by the private sector”¹³ Moreover, the Agency should refrain from adopting AI regulations that risk further complicating international compliance related to the development and use of this nascent technology.¹⁴ Prescriptive rules would undermine the important work that has been done across the public and private sectors to focus on risk-based

¹² *Id.* at 37.

¹³ See Final Report, National Security Commission on Artificial Intelligence, at 449 (Mar. 19, 2021), *available at* <https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf>.

¹⁴ See Jonathan Keane, *China and Europe are leading the push to regulate A.I. — one of them could set the global playbook*, CNBC (May 26, 2022), <https://www.cnbc.com/2022/05/26/china-and-europe-are-leading-the-push-to-regulate-ai.html> (“In March, China rolled out regulations governing the way online recommendations are generated through algorithms, suggesting what to buy, watch or read. . . . [The European] AI law now seeks to impose an all-encompassing framework based on the level of risk, which will have far-reaching effects on what products a company brings to market.”).

approaches. These findings counsel against the adoption of broad prescriptive rules at this time.

To that end, the emergence of flexible voluntary standards to enable trustworthy AI systems, such as NIST’s AI RMF, should be fully leveraged before the Agency adopts broad prescriptive rules. At a minimum, the CPPA should provide sufficient time for the RMF to be implemented, as organizations work to voluntarily identify and address AI risks. It would be premature to suggest that AI needs onerous rules until such voluntary approaches have been considered (particularly given that existing laws, including antidiscrimination laws, already apply when AI is used).

Additionally, the lack of definitions of key terms, such as “automated decision making”, the absence of any clear contextual framework for interpreting the statute, and no evidence of legislative intent (because the CPRA resulted from voter approval of Proposition 24) offers no foundation for the CPPA to begin its work.¹⁵ That foundation must be established first through the development of a robust record, and only then should the Agency proceed to consider adoption of potentially prescriptive new rules in this area.¹⁶

II. Any Regulation Should Seek to Harmonize with Existing Federal Sectoral Statutes, Rules or Regulations, and Other State AI or Consumer Privacy Laws

When considering the regulation of automated decision-making, the CPPA should recognize that there are a plethora of federal, state, and local laws, rules, and regulations that already exist or which have been proposed. Federal and state regulatory bodies have already invested significant time and resources in developing appropriate risk-based regulatory

¹⁵ Indeed, the CPPA’s Invitation for Comments raises fundamental questions about how to define the term “automated decision making,” the scope of existing law already applicable to such systems, and related foundational questions. CPPA Invitation for Comments at 6-7 (rel. Feb. 10, 2023).

¹⁶ Further, the CPPA should proceed with caution in order to avoid subsequent legal challenges regarding the agency’s rulemaking authority. Overly broad rules or regulations could be subject to challenge if the courts determine the agency has overstepped its authority in this area.

frameworks applicable to those entities using AI that are subject to the jurisdiction of these sector-specific regulators. Adopting broad, general-purpose regulations that may conflict, or be inconsistent, with these sector-specific approaches could create significant uncertainty and confusion in these industries.

As such, the CPPA should consider moving forward with caution to ensure that prior to promulgating any new rules, it is fully informed by a robust and complete record that reflects the new and emerging federal, state, and local rules and regulations applicable to AI-enabled systems. Ultimately, any new regulations that may be promulgated by the CPPA should include express, entity-based, exclusions where federal statutes, regulations, orders or decisions clearly govern specific services, systems or practices.

To illustrate the already complex patchwork of existing and proposed legislation that touches on AI, in the state of California alone, (1) the “Bot Disclosure Law,” SB 1001, prohibits the use of undeclared bots to communicate or interact with another person in California, (2) the California Fair Employment and Housing Council has proposed draft regulations that seek to make unlawful the use of automated-decision systems that “screen out or tend to screen out” applicants or employees (or classes of applicants or employees) on the basis of a protected characteristic, and (3) Attorney General Bonita has launched an inquiry into racial and ethnic bias in healthcare algorithms.¹⁷

States outside of California with consumer privacy statutes have also already proposed or enacted regulations related to the use of automated tools for “profiling.” For example, the Colorado Privacy Act defines “profiling” as “any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable

¹⁷ See Press Release of the Office of California Attorney General, dated Aug. 31, 2022, available at: <https://oag.ca.gov/news/press-releases/attorney-general-bonta-launches-inquiry-racial-and-ethnic-bias-healthcare>.

individual’s economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.”¹⁸ The recently finalized rules implementing the Colorado Privacy Act require companies that employ profiling “for a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services” are required to provide consumers notice of:

1. the decisions that are subject to automated decision making,
2. the categories of data processed as part of the profiling,
3. a non-technical, plain language explanation of how profiling is used in the decision-making process,
4. whether the system has been evaluated for fairness and accuracy,
5. the benefits and potential consequences of the decision based on profiling, and
6. information about how a consumer may choose to opt-out of such decisions.¹⁹

The Colorado regulations also provide consumers the right to opt-out of profiling in furtherance of decisions that produce legal or other “similarly significant” effects concerning a consumer, although businesses are not required to honor such requests if they employ “Human Involved Automated Processing”²⁰ and provide consumers with certain disclosures about the decision that incorporates the profiling process.²¹

Virginia’s consumer privacy law, which came into effect on January 1, 2023, also requires companies to provide consumers the ability to opt-out of profiling in furtherance of

¹⁸ C.R.S. § 6-1-1303(20)

¹⁹ 4 CCR 904-3; 9.03(A)

²⁰ Defined as the automated processing of Personal Data where a human (1) engages in a meaningful consideration of available data used in the Processing or any output of the Processing and (2) has the authority to change or influence the outcome of the Processing.

²¹ 4 CCR 904-3; 9.04(C)

decisions that produce legal or “similarly significant” effects concerning the consumer,²² and also requires companies to conduct data protection assessments when they engage in “processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers.”²³ Connecticut’s consumer data privacy statute contains similar opt-out and impact assessment requirements.²⁴

These state privacy laws also ensure that consumer opt-out and access rights with regard to profiling do not extend to decisions that are only partially automated and incorporate human review within the decision-making process. For example, the profiling opt-out and access rights in Connecticut’s consumer privacy act are restricted to “profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.”²⁵ Similarly, in Colorado, the AG recently finalized regs that create an exemption from the opt-out rules for profiling that is based on “human involved automated processing.”²⁶ These restrictions incentivize companies to adopt innovative automated decisionmaking tools while still maintaining some human oversight of the process.

Federal sector-specific regulations must also be considered before advancing rules that may impact industries that are already highly regulated, such as healthcare and financial services.

²² Va. Code Ann. § 59.1-577(A)(5)

²³ Va. Code Ann. § 59.1-580(A)(3).

²⁴ See CT LEGIS P.A. 22-15, 2022 4(a), 8(a).

²⁵ See CT LEGIS P.A. 22-15, 2022, Section 4(a)(5)(C).

²⁶ See CPA Rules, Rule 9.04(C)

These industries face unique considerations that are likely to be best addressed by regulators that have developed specialized knowledge. For example, the Food and Drug Administration has already been active in addressing concerns related to using automated decision making in “Software as a Medical Device,”²⁷ the Equal Employment Opportunity Commission has published guidance on the Americans with Disabilities Act and its impact on the use of algorithms in the hiring process,²⁸ the FTC has stated that existing laws already apply to the use of AI in credit eligibility decisions under the Fair Credit Reporting Act and the Equal Credit Opportunity Act,²⁹ the Consumer Financial Protection Bureau (“CFPB”) has published guidance for financial and credit institutions who utilize artificial intelligence,³⁰ a collection of federal financial regulators including the Board of Governors of the Federal Reserve, the CFPB, the Office of Comptroller of Currency (“OCC”), and the Federal Deposit Insurance Corporation (“FDIC”) have issued a Request for Information relating to Financial Institutions’ Use of Artificial Intelligence, Including Machine Learning,³¹ and the Department of Transportation has published a comprehensive plan on autonomous vehicles.³²

To avoid confusion and the potential for conflicting obligations for companies that

²⁷ See Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan, Food and Drug Administration (Jan. 2021), <https://www.fda.gov/media/145022/download>.

²⁸ See *The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees*, Equal Employment Opportunity Commission (May 12, 2022), <https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence>.

²⁹ Andrew Smith, *Using Artificial Intelligence and Algorithms*, FTC (Apr. 8, 2020), <https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms>.

³⁰ Consumer Financial Protection Circular 2022-03: Adverse action notification requirements in connection with credit decisions based on complex algorithms, CFPB (May 26, 2022), https://files.consumerfinance.gov/f/documents/cfpb_2022-03_circular_2022-05.pdf.

³¹ *Request for Information and Comment on Financial Institutions’ Use of Artificial Intelligence, Including Machine Learning*, Request for Information and Comment, 86 Fed. Reg. 16837 (Mar. 31, 2021), <https://www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence>.

³² Automated Vehicles Comprehensive Plan, Department of Transportation (Jan. 2021), https://www.transportation.gov/sites/dot.gov/files/2021-01/USDOT_AVCP.pdf.

operate in multiple states, the CPPA should ensure that any similar regulations align with those issued in other states and contain exemptions for companies that fall under sector-specific federal regulations. Interoperability of state laws allows consumers to benefit from consistent protections and avoids a complex patchwork of privacy laws that disproportionately impacts the compliance efforts of small and medium sized businesses.

III. The CPPA Should Avoid Adopting Regulations That Impose Costly Compliance Burdens on Small and Medium Sized Enterprises

As explained above, the benefits of AI systems used across many different industry sectors are numerous. However, those benefits could be eliminated, or undermined, if the costs of complying with extensive new regulations of autonomous decision making systems enabled by AI are adopted by the Agency. For example, the costs of complying with broad new rules of general applicability may stifle innovation and undermine competition in these emerging areas. Further, any new obligations the CPPA may adopt will likely have a disproportionate impact on small-medium sized business, which could force such businesses out of the market. That, in turn, will stifle innovation and reduce competition.

The costs of complying with complex new rules governing access and opt-out rights would likely be significant and could increase compliance costs on entities competing in these sectors. The potential compliance costs associated with complex new regulations is illustrated by the comprehensive proposed new AI regulations currently under consideration in Europe. Notably, the cost of complying with just one of the new duties under the proposed EU AI Act would be an obligation for each covered entity to set up a “quality management system” to ensure compliance with the new rules proposed in the EU. The European Commission has estimated that doing so could cost covered entities as much as €400,000.³³ Other commentators

³³ European Commission, [Study supporting the impact assessment of the AI regulation](#), p. 152 (Apr. 2021).

have estimated significantly greater compliance costs associated with compliance with all of the aspects of the EU AI Act.³⁴ Such estimates do not, of course, reflect potential costs of compliance under any new rules proposed by the CPPA, but they do illustrate the potential impact of any attempt to impose broad, sweeping rules on this emerging area. The CPPA should undertake its own evaluation of the potential costs of any new rules to ensure that an accurate and comprehensive cost-benefit analysis informs any further action in this area.

For these reasons, CTA urges that any substantive limitations on the collection, processing, and use of consumer data related to automated decision-making would need to be, at a minimum, risk-based and highly targeted, as different types of data-driven business models vary widely in how they collect and use data. As such, and given the narrow scope of the proposed rulemaking, CTA encourages the Agency to make any access, opt-out or transparency rules associated with the use of automated decision making systems flexible to account for shifting technologies. Specifically, any rule should be outcome-based rather than prescriptive – the agency should define the goals of regulation as opposed to the methods for regulating.³⁵

Further, the CPPA should refrain from promulgating sweeping and prescriptive access, opt-out or transparency rules at a time when the international and domestic patchwork of laws and regulations surrounding the deployment and use of AI-enabled systems is growing in complexity.

³⁴ See Benjamin Mueller, [How Much Will the Artificial Intelligence Act Cost Europe?](#), Center for Data Innovation (2021) (“We estimate that the Artificial Intelligence Act would cost European businesses €10.9 billion per year by 2025, having cost the economy €31 billion by then. This excludes the opportunity cost of foregone investment into AI.”).

³⁵ This approach is supported by other expert agencies working in this area. For example, NIST explains, for example, that “[f]inding ways to continue to derive benefits from data processing while simultaneously protecting individuals’ privacy is challenging, and not well-suited to one-size-fits-all solutions.” NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0, NIST, at 1 (Jan. 16, 2020), <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf>.

IV. The CPPA Should Consider Adopting a Narrow Focus on Risk-Based Approaches and Leverage Existing Voluntary Standards

One-size-fits-all rules to regulate or discourage AI and algorithmic decision making would stifle innovation, by discounting potential benefits and ignoring options for risk mitigation. Given its widespread applications and uses, regulation of AI in particular is particularly ill-suited to a one-size-fits-all approach. Because it is used in so many types of applications, there are substantial differences between the kinds of risks that consumers may face from mistakes or misuse of AI-enabled systems. For example, health care (e.g., robotic surgery) uses may be more high-risk than media or advertising uses. As explained above, there are significant federal regulations in place that cover industry-specific application of AI. An algorithmic system that uses profiling to make decisions should not receive greater regulatory scrutiny unless a decision has significant legal implications for the consumer. Prescriptive rules that attempt to generally regulate AI technology itself, without accounting for sector-specific applications or actual risks to consumers, will stifle benefits without effectively addressing risks.

When drafting its regulations, the CPPA should look to the NIST AI RMF, which relies on flexible risk-based assessments, and recognizes the importance of proceeding deliberatively to avoid unnecessary burdens on AI development and deployment. NIST solicited input from a wide array of stakeholders to develop its consensus-based approach to providing guidelines for trustworthy AI, and NIST continues to explore and draft guidance on issues such as AI explainability and interpretability. CTA was deeply engaged in the development of NIST's AI RMF and broadly supports NIST's flexible, risk-based approach to developing trustworthy AI systems.³⁶

³⁶ See Comments of the Consumer Technology Association Comments, RFI - NIST AI Risk Management Framework, Docket No. 21076-01510 (filed Sept. 15, 2021), <https://www.nist.gov/system/files/documents/2021/09/16/ai-rmf-rfi-0087.pdf>; Comments of the Consumer

When considering regulations that would require businesses to provide meaningful information about the logic involved in “automated decision making processes,” the CPPA should look to the transparency and explainability guidance that NIST has included in its RMF and should incorporate them as the presumptive standard. The RMF explains that “[t]ransparency reflects the extent to which information about an AI system and its outputs is available to individuals interacting with such a system,” and that “explainable and interpretable AI systems offer information that will help end users understand the purposes and potential impact of an AI system.”³⁷ NIST has also stated that it plans to issue further guidance specifically in the area of AI explainability and transparency and how such characteristics interact with the RMF as a whole. Given the deep, specialized knowledge NIST has and continues to develop with regard to the development of trustworthy AI, the CPPA should defer to NIST and frame any future regulations around NIST’s forthcoming guidance on the issue.

As described above, other state laws regulating the use of automated decision making are limited to decisions that have legal or “similarly significant” effects and are appropriately restricted to higher-risk decisions that may impact an individual’s employment, financial status, or ability to obtain health care.

In line with other states and NIST’s risk-based approach, the CPPA should ensure that proposed requirements are scoped to AI-enabled systems with high impacts on consumers. Similarly, companies that follow the standards developed by NIST should enjoy a safe harbor against state regulatory enforcement.

Technology Association, NIST AI Risk Management Framework: Initial Draft, (filed Apr. 29, 2022), <https://www.nist.gov/document/1st-draft-ai-rmf-comments-consumer-technology-association>; Comments of the Consumer Technology Association, NIST AI Risk Management Framework: Second Draft, Docket No. 21076-01510 (filed Sept. 29, 2022).

³⁷ *AI Risk Management Framework*, NIST, <https://doi.org/10.6028/NIST.AL100-1> (last visited March 20, 2023).

V. Opt-Out and Access Requirements Should Be Narrowly Tailored

Given the lack of clarity and specificity of the nature of proposed opt-out and access requirements, the CPPA should take a narrow, focused approach in developing rules in this area. Overly broad rules or regulations could be subject to challenge if the courts determine the agency has overstepped its authority or did not properly implement the legislature's intent.

Moreover, enacting blanket algorithmic opt-outs, without limitation, would undermine the ability of companies to provide personalized content to consumers generally, and would be impractical because certain integrated product features are provided through the use of AI. Online services routinely make a number of automated decisions in order to provide the services that people sign up for. Specifically, automated recommendations enable personalization, which is the basis for a wide array of online services beneficial to consumers. Rules implementing a broad opt-out of automated decision making technology and profiling, without any limitation, would significantly undermine the ability of companies to provide relevant and personalized services to all users, even those that have not opted out. In addition, a required opt-out could result in implementing human-based manual processes which could introduce bias from human actors in addition to inefficiencies.

Finally, a broad opt-out right could also undermine the utility of training data sets that broadly reflect society, and which help to reduce the potential for bias or discrimination. CTA members seek to reduce the potential for undue outcomes in numerous ways, including through the use of training data sets that are inclusive, draw broadly from different aspects of society, and which reflect our society broadly. Enabling broad opt-out options for individuals could undermine the utility and value of these representative data training sets.

To avoid these tradeoffs, the CPPA should, as described above, restrict any opt-out requirements to those automated decisions that pose the greatest risk to consumers, specifically, those decisions that create a legal or “similarly significant” impact on the consumer.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: /s/ Douglas K. Johnson
Douglas K. Johnson
Vice President, Emerging Technology Policy

/s/ Rachel Nemeth
Rachel Nemeth
Senior Director, Regulatory Affairs

1919 S. Eads Street
Arlington, VA 22202
(703) 907-7600

Dated: March 27, 2023

From: Craig Erickson [REDACTED]
Sent: Monday, March 27, 2023 2:36 PM
To: Regulations
Subject: PR 02-2023
Attachments: Appendix A - Current Process for Mandatory Independent Security Assessments of California Agencies.docx; Appendix B - California State Legislation related to Cybersecurity, Consumer Privacy Protections, and Public Safety.docx; Appendix C - Proposed Control Set for Initial Risk Assessment Summaries for Identifying High-risk Entities.docx; Appendix C - NIST Control Standards for CCPA Risk Assessments.xlsx; COMMENTS ON PROPOSED CCPA RULEMAKING.docx

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

(all documents are attached, including these comments for the public record)

Commenter: Craig Erickson, a California Consumer residing in Alameda, CA

Contact: [REDACTED]

Date Submitted: 03/27/2023

Craig Erickson's COMMENTS ON PROPOSED RULEMAKING

CYBERSECURITY AUDITS, RISK ASSESSMENTS, AND AUTOMATED DECISIONMAKING

Background

As a California Consumer, I maintain a personal vendor risk program for testing businesses' compliance with the CCPA and governing use of my personal information. In November of 2020, I voted for Proposition 24, the California Privacy Rights Act of 2020 ("CPRA") because I share

"the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public".

Comment 1, Pursuant to Civil Code section 1798.185(a)(15)-(16):

I ask the Agency to consider all stakeholders when issuing regulations **1798.185(a)(15)-(16)**, instead of **only** requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to perform (B) and (A), because consumers and government agencies can also introduce significant risk by their actions or inaction even though they cannot be legally responsible for following the guidance issued by these regulations.

(B) Consumers should be allowed to submit to the California Privacy Protection Agency on an as-needed basis, their own risk assessment findings, compliance test results, or incident reports with respect to their processing of personal information, and that the Agency should help identify and weigh the benefits against potential risks, with the goal of educating the public about which processing activities and organizational entities are deemed “high-risk”.

(A) Based on risk assessments (B) from businesses and consumers which are validated by the Agency, perform a cybersecurity audit on an annual basis, using the State of California’s current process as a model, to ensure that audits are thorough and independent. This proposal is documented in Appendix A.

(a) The *non-exclusive* factors to be considered in determining when processing may result in significant risk to the security of personal information shall include *any one of the following factors*:

a) the size of the business; b) complexity of supply-chain dependencies; c) the nature of processing activities; d) scope in terms of company size; e) sensitivity of personal information; f) vulnerability of targeted populations; g) history of non-compliance, breaches, or unlawful practices; h) absence of, or lack of access to other suppliers providing critical services to consumers.

(16) Consider issuing regulations governing access and opt-out rights with respect to any, and all use of automated decisionmaking technology, because businesses aren’t the only entities using it; government agencies use it in law enforcement; and consumers use it when transmitting opt-out preference signals or using authorized agents to send delete requests to businesses identified in email messages.

Comment 2, I. Cybersecurity Audits; Question 1 (a) (b) (c) (d) (e):

1.a. California State Laws and the California State Constitution require California State Agencies to have mandatory cybersecurity audits, and in some cases, Privacy Impact Assessments. These state agencies serve businesses and consumers. California already has an established Cybersecurity Program including Independent Security Audits for its agencies, which appears to meet the goals and requirements of Civil Code section 1798.185(a)(15)(A), with minimal modifications.

1.b. California’s ISA process, documented in Appendix A, helps agencies comply with other state laws that currently have, or could benefit from, cybersecurity audit requirements. These laws, which are related to security and privacy risks of processing personal information, could be more effective by sharing information and costs from CCPA-mandated risk assessments and cybersecurity audits. These current and pending legislative bills are documented in Appendix B.

1.c. and 1.d. The gaps or weaknesses of any audit or certification is the level of acceptance or validation of the assessment. Obviously, Californians would not vote for mandatory risk assessments and cybersecurity audits if existing ones met the goals and requirements of laws like Civil Code section 1798.185(a)(15)(A). The lack of transparency about what standards and controls are tested, the process, the outcomes, and who this information applies to, greatly impacts consumers’ trust in businesses and enforcement agencies. Laws are ineffective when perceived by businesses or consumers, as being unfairly enforced.

1.e. I recommend using a similar model to the existing ISA process within the State because the CPPA is a state agency, and the State uses NIST SP800-53r4 as its primary standard control framework, according to the Office of Information Security (OIS) in the State’s Information Security Policy.

Comment 3, I. Cybersecurity Audits; Question 2 (a) (b) (c) (d) (e):

2.a. The Agency should consider in its regulations for CCPA's cybersecurity audits pursuant to Civ. Code § 1798.185(a)(15)(A) alignment with cybersecurity audits, assessments, evaluations, and best practices identified in intra-state, inter-state, and federal requirements and standards, and standards from the EU including the GDPR, the EDPB, and NIS 2.

2.b., 2.c. and 2.d. Current cybersecurity audits, assessments, evaluations, or best practices in the US include responding to self-assessment questionnaires from other businesses, and third-party certifications such as SOC2, PCI-DSS, HITRUST, FedRAMP, and ISO. Consumers do not have access to this information, which is both a gap and a weakness which impacts consumers and businesses by eroding public trust that laws are being fairly and effectively enforced.

Comment 4, I. Cybersecurity Audits; Question 2 (e), and Question 3:

2. e. The Agency should consider these cybersecurity audit models, assessments, evaluations, or best practices when drafting its regulations because, when aligned with common controls in other standard control frameworks, the compliance and audit process can facilitate greater acceptance and leverage information from existing best practices. However, due to the wide variety of interpretations and inconsistent audit execution, existing assessments should not be accepted in place of a state agency-initiated audit that sets the control standards and the audit methodology.

Comment 5, I. Cybersecurity Audits; Question 4, and Question 5:

4. and 5. Similar processes from other government agencies help to ensure that these audits, assessments, or evaluations are thorough and independent, by comparing existing cases which are also relevant to the CCPA. The Agency should also consider publishing a "Communicating our Regulatory and Enforcement Activity Policy", as the ICO does in the UK because:

Transparency is often mentioned as a key factor in building and maintaining trust among businesses and consumers. It's also a preventative control mechanism – when businesses and consumers know what enforcement actions are taken, why, and on whom can invoke a sense of fairness, which research has shown tends to encourage compliance.

This topic about transparency relates directly to the Agency's question regarding the scope of cybersecurity audits:

The scope should be dependent upon the classification of business practices and business entities whose management history has been deemed "high-risk" *and should not be concealed from the public.*

For example, the Agency should also consider "trust services" (NIS 2) that are essential to identity verification, or data brokers that operate CDNs or other services that must be resilient for serving the public interest.

Article 2 of The Network and Information Security (NIS 2) Directive, the EU-wide legislation on cybersecurity states: "2. *Regardless of their size, this Directive also applies to entities ... where:*

(a) services are provided by:

(i) providers of public electronic communications networks or of publicly available electronic communications services;

(ii) trust service providers;

(iii) top-level domain name registries and domain name system service providers;

(b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;

(c) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;

(d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;

(e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State;”

Comment 6, II. Risk Assessments; Question 1 (a), and Question 5:

The CCPA directs the Agency to issue regulations requiring businesses “whose processing of consumers’ personal information presents significant risk to consumers’ privacy or security” to regularly submit to the Agency a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits and risks of such processing.

a. The risk assessment itself should determine the necessary scope and submission process for selecting which businesses should be subject to mandated cybersecurity audits. Existing state, federal, and international laws, third-party compliance audits employ a similar approach by using self-assessment questionnaires and other tools to evaluate an entity’s legal requirements and determine if the inherent risk justifies additional scrutiny or controls, even for businesses that make less than \$25 million in annual gross revenue or enjoy other exemptions.

Comment 7, Pursuant to II. Risk Assessments; Question 1 (b) (c) (d) and (e):

Businesses evaluate other businesses through vendor risk management practices, including the use of “ratings” companies and databases such as MITRE’s CVE and US-CERT, to identify product vulnerabilities and data breach histories which can also assist with the CCPA’s risk-assessments requirements. The gaps or weaknesses of these risk assessments include lack of data quality standards in reporting and the lack of participation in sharing information about security and privacy incidents among businesses, consumers, and enforcement agencies. These weaknesses impact consumers by depriving them of critical information they need to make risk-based decisions about their vendors.

Not-for-profit Organizations, with few exceptions, are currently exempt from complying with the CCPA. According to page 2 of “*Findings from ICO information risk reviews at eight charities*”, April 2018, charitable organizations can be large or small, and engage in very high-risk processing. Under the section entitled, “*Typical processing of personal data by charities*”, the ICO writes, “*The charities involved process a limited amount of sensitive personal data as defined by the DPA, including staff sickness records and sometimes donor or service*

user information relating to health and receipt of benefits. Some charities also process information relating to children and vulnerable people.”

This is why I propose the Agency send a risk assessment to every organization registered with the California Secretary of State, not only for the purpose of determining inherent risk but also for increasing the public’s awareness of these new regulations and the standards used in these assessments.

Comment 8, Pursuant to II. Risk Assessments; Question 2:

I cannot predict what harms, if any, particular individuals or communities are likely to experience from a business’s processing of personal information.

Identifying what processing of personal information is likely to be harmful to these individuals or communities, could be discovered through robust reporting process, which would accept input from individual consumers and/or consumer advocacy organizations such as the Identity Theft Resource Center. I recommend not codifying in law or regulations assumptions or current trends which may not hold true in the future, in favor of capturing incident-reporting metrics instead.

Comment 6, Pursuant to II. Risk Assessments; Question 3 (a):

a. To determine what processing of personal information presents significant risk to consumers’ privacy or security under Civil Code § 1798.185(a)(15), the Agency should (a) follow an approach similar to those outlined in the European Data Protection Board’s Guidelines on Data Protection Impact Assessment.

Comment 9, Pursuant to II. Risk Assessments; Question 3 (b) and (e):

b. e. The agency should consider the PIA Methodology from CNIL for Privacy Impact Assessments because of its widespread adoption and online tools for conducting them. The Agency should also consider the ISO/IEC JTC 1/SC 27/WG 5 N1320, WG 5 Standing Document 4 (SD4) – Standards Privacy Assessment (SPA). This document determines whether to apply the SPA process by asking three questions concerning the Standard or Specification Under Review (SUR):

- 1. Will the SUR involve technology that will process PII, or will it involve technology that could link information to an identifiable individual?*
- 2. If the SUR will not process PII or involve technology that could link information to an identifiable individual, will it generate PII?*
- 3. If the SUR will not generate PII, will it involve technology that will be used in a network device by an individual?*

If the answer to any of these questions is affirmative, then the SPA process should be applied to the SUR.

The beauty of this approach lies in its granularity, as applied to an entire product offering or introducing a new feature.

In addition, the ISO/IEC JTC 1/SC 27/WG 5 N1320, WG 5 Standing Document 4 (SD4) – Standards Privacy Assessment (SPA) uses this criteria for defining (e) What processing, if any, does not present significant risk to consumers’ privacy or security:

“This standard [or specification] does not define technology that will process Personally Identifiable Information (PII), nor will it create any link to PII.

Furthermore, the standard [or specification] does not define technology that will be deployed in a network device and used by an individual.”

Comment 10, Pursuant to II. Risk Assessments; Question 3 (c):

The risk assessment should be used initially to determine what personal information is processed by an entity, and what their legal obligations are in complying with the CCPA, so that all stakeholders including businesses, consumers, and the Agency can judge for themselves if a cybersecurity audit should be required based on the design of appropriate controls. To protect trade secrets and security measures, only the resulting status should be reported for each entity when or if the entity’s status is queried by users through an online tool provided by the CPPA.

Comment 11, Pursuant to II. Risk Assessments; Question 4 (a) (b), Question 6 (a) (b):

The minimum content required in risk assessments should be based on a subset of the most fundamental controls in NIST SP 800-53 r5 which are directly applicable to the CCPA Regulations, and can be mapped to controls in other frameworks such as NIST Cybersecurity Framework, NIST Privacy Framework, and the NIST Framework for Improving Critical Infrastructure, Center for Internet Security Controls, OWASP, and ISO.

As a theoretical construct, I have proposed in Appendix C, a subset of selected NIST controls which provide acceptable standards for cybersecurity and information risk practices that are necessary for complying with the CCPA Regulations.

(a) The GDPR and the Colorado Privacy Act are laws which are subject to change, making these a poor choice for the CCPA’s risk assessments. A better choice would be to base risk assessments on standard, mature control frameworks like NIST, which is a commonly used by state and federal government agencies and all companies that do business with these agencies.

(b) Additional content is not required in risk assessments for processing that involves automated decisionmaking, including profiling because several controls included in my proposed NIST subset covers underlying dependencies like data quality and provenance, which are marked with an asterisk in Appendix C. Additional content may be required for mandated cybersecurity audits according to relevant risk factors.

Comment 12, Pursuant to II. Risk Assessments; Question 6 (a):

Businesses should only submit summary risk assessments formatted as a self-assessment questionnaire issued by the Agency, for the purpose of identifying risk factors ascribed to their company.

The Agency should not accept any other risk assessment conducted by the business because most other assessments will likely be outdated and not aligned with CPPA standards which are not yet defined.

These summaries should include a relevant subset of controls based on the NIST standard, similar to my Comment 11, which is documented in Appendix C. They should be submitted at least once annually, or within 90 days of a change in ownership.

Comment 13, Pursuant to II. Risk Assessments; Question 6 (b):

Businesses should designate a company officer that attests to the completeness, accuracy, *and currency* of risk assessment summaries, signed by the designated officer under penalty of perjury, like NIS 2 attestations in the EU, or Sarbanes Oxley in the US.

Combined with other proposals I've made in these comments, these summaries can be verified or refuted by incident reporting and complaints from consumers and other enforcement agencies.

Comment 14, Pursuant to II. Risk Assessments; Question 7:

All organizational entities registered with the California Secretary of State should be required to submit an initial risk assessment, which consists of no more than 100 self-assessment questions designed to identify high-risk processing and high-risk entities. These self-assessment questions are provided alongside the NIST controls I mapped to CCPA Regulations in Appendix C.

Comment 15, Pursuant to III. Automated Decisionmaking; Question 3 and Question 4:

Automated Decisionmaking, and any privacy risks associated with its use is not limited to CCPA-covered entities. Businesses which are exempt from the CCPA due to revenue thresholds have been reluctant to acknowledge their status, which effectively defrauds consumers regarding their CCPA rights according to controlled privacy experiments I have conducted over a two year period. I anticipate that business start-ups, who are eager to accelerate their market positions but less eager to implement privacy controls, will claim to use AI, ML, Deep Neural Networks, etc. This is problematic because it could be nearly impossible for the Agency to determine who is using this technology, especially if companies make false representations or fall under the revenue threshold to avoid public embarrassment AND regulatory scrutiny.

Comment 16, Pursuant to III. Automated Decisionmaking; Question 3 (a) (d) (e) (f) and Question 5:

The Agency should consider all regulatory frameworks regarding the use of Artificial Intelligence (AI) because AI is the baseline technology underlying Automated Decisionmaking technologies. In particular, the Agency should consider:

- [Regulatory framework proposal on artificial intelligence | Shaping Europe's digital future \(europa.eu\)](#)
- [explaining-decisions-made-with-artificial-intelligence-1-0.pdf](#) from the ICO
- [guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf](#) from the ICO

The Agency should also consider which AI systems the EU has identified as high-risk in its [Regulatory framework proposal on artificial intelligence](#), for inclusion in its criteria for defining high-risk factors:

- critical infrastructures (e.g. transport), that could put the life and health of citizens at risk;
- educational or vocational training, that may determine the access to education and professional course of someone's life (e.g. scoring of exams);
- safety components of products (e.g. AI application in robot-assisted surgery);
- employment, management of workers and access to self-employment (e.g. CV-sorting software for recruitment procedures);

- essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan);
- law enforcement that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence);
- migration, asylum and border control management (e.g. verification of authenticity of travel documents);
- administration of justice and democratic processes (e.g. applying the law to a concrete set of facts).

3. a. The Agency should use the ICO definition because it's the most concise:

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/>

For related terms, I also recommend <https://publications.jrc.ec.europa.eu/repository/handle/JRC126426> which provides an "operational definition" consisting of an iterative method providing a concise taxonomy and list of keywords that characterise the core domains of the AI research field.

3. d. e. f. I recommend the Agency analyze how its own regulations on ADM would or would not apply to use cases in the EU, in light of the other conflicting US laws which could circumvent these protections. Existing GDPR case law, and associated privacy risks can be found in the following report, <https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf>.

For example, one consumer complaint I filed with the California Office of Attorney General applies directly to case law, *3.3 Credit Scoring*, which is justified on "contractual necessity" only if it relies on relevant information. I was denied access to my business banking account due to their use of an identity provider which is a credit rating agency exempt from the CCPA, is a registered data broker, and also has a history of data breaches involving my compromised answers to security questions pertaining to another individual which I have no right to correct. In my case there was no automated decisionmaking using machine-learning or artificial intelligence algorithms: just me and my US passport standing in front of the bank branch manager who opened my account but could not authenticate me for online-banking because of a simple "automated process" consisting of a flawed lookup table maintained by an untrustworthy identity provider exempt from the CCPA.

Closing Comment

I want to thank the CPPA for providing this opportunity to participate in its rulemaking process through these public comments. For brevity's sake, my Appendices are attached (if possible) to this submission, and published in my PrivacyPortfolio for peer review and collaboration with my professional colleagues.

Like laws and audits, my own assumptions and proposals need to be tested. Therefore, as a follow-up to this public comment I will be conducting these tests on my personal vendors and sending my findings to my vendors and the appropriate enforcement agencies and publishing the results of my experiment in my public data catalog.

As a California Consumer who exercises my own rights, I hope that the CPPA succeeds in providing independent assurance to all stakeholders that critical assets and citizen data are protected, which is the stated goal of Mandatory Independent Security Assessments of California Agencies.

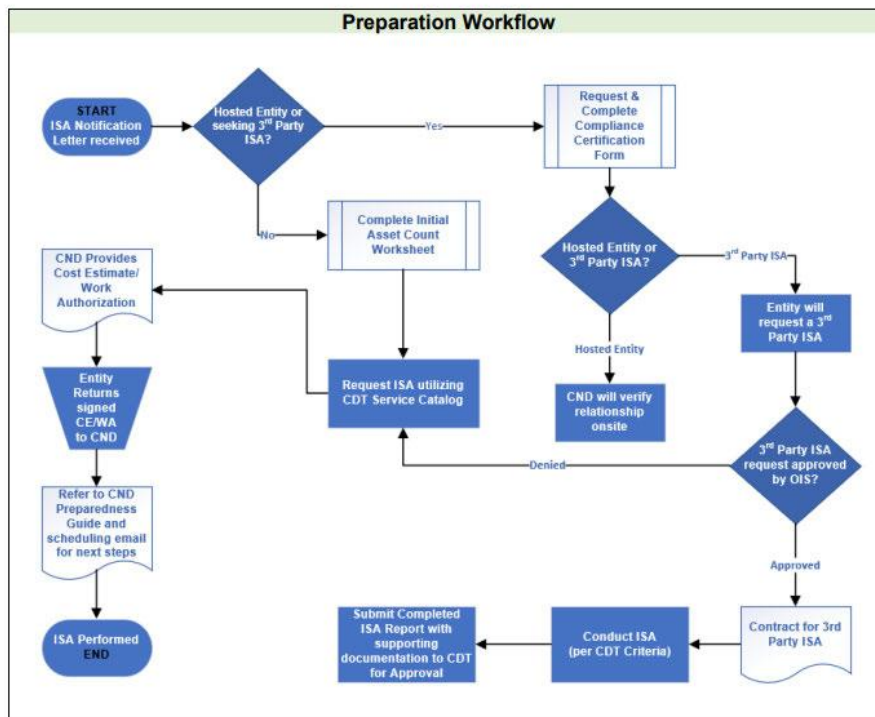
Sincerely,

Craig Erickson, a California Consumer

Appendix A

Current Process for Mandatory Independent Security Assessments of California Agencies

Use this as a process model for CCPA risk assessments, based on output from CCPA cybersecurity audits:



1. Entities begin the ISA process when they receive a formal notification letter from California Department of Technology (CDT) Office of Information Security (OIS) advising them that it is their year to undergo an ISA.
 - a. Entities can seek approval to undergo a commercial, 3rd party ISA by attaching a copy of the proposed Statement of Work for the contract to the ISA Compliance Certification Form. The completed ISA report must meet the ISA Criteria* EXACTLY and follow the SAME FORMAT.

Note: All businesses and organization registered with the California Secretary of State should receive a “Welcome Packet” promoting awareness of the new CCPA Regulations and Resource Guide to help them comply with the Regulations and additional reporting requirements.

Note: Businesses and Consumers can use an online service to determine which classification status applies to the entity as 1) CCPA-Exempt; 2) CCPA-Covered; 3) Data Brokers; 4) Large Businesses; 5) High-Risk Processors. This tool also informs the user which obligations apply to each entity class. For a CCPA-Exempt entity, it would state the entity has no legal obligations under the CCPA, and advise that a consumer may reasonably expect them to comply with the CCPA unless told otherwise.

Note: All CCPA-covered entities must complete a Risk Assessment Questionnaire. This is designed to confirm or address any discrepancies in their classification status and assess their awareness of the CCPA

through simple tests anyone could conduct. For example, all CCPA-covered entities must have a published privacy policy, but if the policy predates the passage of the new CPRA-amended CCPA Regulations, it's more likely than not that they are non-compliant and recommend they consult the Resource Guide.

Note: All CCPA-covered entities classified as Data Brokers, Businesses Collecting Large Amounts of Personal Information, and High-Risk Processors would be required to fill out an Initial Asset Count Worksheet. This worksheet is designed to identify assets critical to the scope of an audit. It includes registered domains, websites, IoT devices, brand names, subsidiaries, parent companies. It would also include estimated counts of employees, consumer profiles, service providers, contractors, and third parties involved in collecting or processing PI. Counting the average number of sensitive data elements and attributes stored or processed helps the Agency designate which entities meet the criteria for mandatory risk assessments and audits.

Note: Audits and assessments are verified through testing controls, and the controls which are tested must be sampled from a finite population. Without making the entire inventory of system asset public information, input from consumers and other agencies can use other sources to verify or refute the scope of assets tested.

2. Entities begin the ISA scheduling process by completing the Initial Asset Count Worksheet. (Appendix A)
3. Create the ISA Case from the CDT IT Services Portal catalog within 30 days of the date of official notification.
4. Receive Confirmation of ISA Dates and Cost Estimate/Work Authorization and return the signed CE/WA to the Cyber Network Defense (CND) Engagement Manager who officially schedules the entity's assessment dates.
5. Entity receives a copy of the CND Preparedness Guide from the CND Engagement Manager with an email confirming the schedule for their ISA. The Preparedness Guide will enable the entity to be as prepared as possible for CND's arrival on site and to ensure the best possible outcome and benefits from the ISA.

The ISA is conducted using a two-team approach. The Risk Analysis (RA) team conducts (BLUE TEAM) tasks related to the defensive controls assessed (task sections 10-15). The Penetration Test (Pen Test) team conducts (RED TEAM) activities related to the offensive simulation operations portion of the assessment (task sections 16-17).

If the Pen Test Team detects a Significant Risk, it will initiate a "Hard Pause" if delayed disclosure is likely to result in network compromise by a real-world threat actor. The Pen Test Team provides the Entity Liason with information pertaining to the detected risk, impacted host(s), and recommended course of action to reduce the risk to the enterprise.

If the CND detects the potential presence of Illegal Activity (external threat actor compromise, insider threat activities, etc.) the ISA will initiate a "Hard Stop". The Pen Test Team, working with the entity's management team, perform the required initial reporting to Cal-CSIRS as well as facilitate any interim evidence preservation process for red team actions.

Areas within the current ISA include host vulnerability assessments, firewall analysis, host hardening analysis, phishing susceptibility, network penetration testing, and snap-shot analysis of network traffic for signs of threat actor compromise.

Note: This proposal is not suggesting that CMD conducts all risk assessments, but that standards and guidelines for third-party assessors be aligned with CMD standards to a reasonable degree.

Appendix B

California State Legislation related to Cybersecurity, Consumer Privacy Protections, and Public Safety.

Proposal

The benefits to the CPPA and OAG by leveraging existing policies, programs, procedures, and resources within California State agencies that align with intended objectives of mandated cybersecurity audits and risk assessments include:

- Reducing the cost/effort of auditors and auditees required to comply with legal mandates.
- The harmonization of laws and regulations at an inter-state and federal level based on established standards for cybersecurity.
- Independent verification and validation of cybersecurity audits and risk assessments.

Note: Other significant laws relevant to the CCPA can also leverage this audit, assessment, and reporting process to help supplement and verify findings of non-compliance and high-risk activities.

Bill	Subject	Latest Bill Version	Lead Authors Status	Last History Action
AB 254	Confidentiality of Medical Information Act: reproductive or sexual health application information	Introduced 1/19/2023	Bauer-Kahan	Active Bill – In Committee Process 2/2/2023 – Referred to Assembly Health Committee and Privacy and Consumer Protection Committee
AB-327	Existing law establishes the California Cybersecurity Integration Center (Cal-CSIC) within the Office of Emergency Services, the primary mission of which is to reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or computer networks in the state.			
AB 362	Data brokers: registration	Introduced 2/8/2023	Becker	

AB 386	California Right to Financial Privacy Act	Introduced 2/2/2023	Nguyen	
AB 677	Confidentiality of Medical Information Act	Introduced 2/13/2023	Addis	4/14/2021, now relates to COVID-19 vaccination status and prohibitions on disclosure. covid vaccinations
AB- 694	1798.140. Definitions			10/5/2021 – Approved by the Governor. Chaptered by Secretary of State – Chapter 525, Statutes of 2021.
AB 707	Information Practices Act of 1977: commercial purposes	Introduced 2/13/2023	Patterson	
AB- 1712	Personal information: data breaches.		Irwin	Active Bill – Pending Referral
AB 726	Information Practices Act of 1977: definitions	Introduced 2/13/2023	Patterson	Active Bill – Pending Referral 2/14/2023 – From printer. May be heard in committee March 16.
AB 733	Invasion of privacy	Introduced 2/2/2023	Fong, Hart	Active Bill – Pending Referral 2/14/2023 – From printer. May be heard in committee March 16
AB- 749	State agencies: information security: uniform standards.		Irwin	Active Bill - In Committee Process
AB 793	Privacy: reverse demands	Introduced 2/13/2023	Bonta	Active Bill – Pending Referral 2/15/2023 – From printer. May be heard in committee March 16.

AB 801	Student privacy: online personal information	Introduced 2/13/2023	Patterson	Active Bill – Pending Referral 2/14/2023 – From printer. May be heard in committee March 16.
AB-825	Personal information: data breaches: genetic data.		Levine	10/5/2021 – Approved by the Governor. Chaptered by Secretary of State – Chapter 527, Statutes of 2021.
AB 947	California Consumer Privacy Act of 2018: Amends the law to require all five members of the California Privacy Protection Agency’s governing board to have qualifications, experience and skills in consumer rights, in addition to those in privacy, technology and other currently required areas.	CPPA Introduced 2/14/2023	Gabriel	Active Bill – Pending Referral 2/15/2023 – From printer. May be heard in committee March 17.
AB 1034	Biometric information: law enforcement: surveillance	Introduced 2/15/2023	Wilson	Active Bill – Pending Referral 2/14/2023 – From printer. May be heard in committee March 18.
AB 1102	Telecommunications: privacy protections: 988 calls	Introduced 2/15/2023	Patterson	Active Bill – Pending Referral 2/14/2023 – From printer. May be heard in committee March 18
AB 1194	California Privacy Rights Act of 2020: exemptions: abortion services	Introduced 2/16/2023	Carrillo	Active Bill – Pending Referral 2/16/2023 – Read first time. To print.
AB-1194	California Privacy Rights Act of 2020: exemptions: abortion services.		Carrillo	Active Bill – Pending Referral
AB-1352	Independent information security assessments: Military Department: local educational agencies.		Chau	

AB 1394	Commercial sexual exploitation: civil actions	Introduced 2/17/2023	Wicks	Active Bill – Pending Referral 2/18/2023 – From printer. May be heard in committee March 20
AB 1463	Information Practices Act of 1977	Introduced 2/17/2023	Lowenthal	Active Bill – Pending Referral 2/17/2023 – Read first time. To print.
AB 1546	California Consumer Privacy Act of 2018: statute of limitations	Introduced 2/17/2023	Gabriel	Active Bill – Pending Referral 2/17/2023 – Read first time. To print.
AB 1552	Student privacy: online personal information	Introduced 2/17/2023	Reyes	Active Bill – Pending Referral 2/17/2023 – Read first time. To print.
AB 1552	Student privacy: online personal information	Introduced 2/17/2023	Reyes	Active Bill – Pending Referral 2/18/2023 – From printer. May be heard in committee March 20
AB- 1651	Labor statistics: annual report. Worker rights: Workplace Technology Accountability Act.		Kalra	Inactive bill – Died 11/30/2022 – From committee without further action.
AB- 1711	An act to amend Section 1798.29 of the Civil Code, relating to Privacy: breach		Seyarto	
AB 1712	Personal information: data breaches	Introduced 2/17/2023	Irwin	Active Bill – Pending Referral 2/18/2023 – From printer. May be heard in committee March 20
AB 1721	California Consumer Privacy Act of 2018	Introduced 2/16/2023	Ta	Active Bill – Pending Referral 2/17/2023 – Read first time. To print.
AB- 2089	Privacy: mental health digital services: mental health application information.		Bauer-Kahan.	
AB- 2355	School cybersecurity.		Salas	

AB-2958	Committee on Judiciary. State Bar of California.			
SB-41	Privacy: genetic testing companies.		Umberg	
SB 287	Features that harm child users: civil penalty	Introduced 2/2/2023	Skinner	Active Bill – In Committee Process 2/15/2023 – Referred to Senate Judiciary Committee and Appropriations Committee
SB 296	In-vehicle cameras	Introduced 2/2/2023	Dodd	Active Bill – In Committee Process 2/15/2023 – Referred to Senate Judiciary Committee.
SB 611	Information Practices Act of 1977	Introduced 2/15/2023	Menjivar	Active Bill – Pending Referral 2/16/2023 – From printer. May be heard in committee March 18.
SB 793	Insurance: privacy notices and personal information	Introduced 2/16/2023	Glazer	Active Bill – Pending Referral 2/17/2023 – Read first time. To Senate Rules Committee for assignment. To print.
SB 845	Let Parents Choose Protection Act of 2023	Introduced 2/17/2023	Stern	Active Bill – Pending Referral 2/21/2023 – From printer. May be heard in committee March 20
SB 875	Referral source for residential care facilities for the elderly: duties	Introduced 2/17/2023	Glazer	Active Bill – Pending Referral 2/17/2023 – Read first time. To Senate Rules Committee for assignment. To print.
SB-1059	Privacy: data brokers.		Becker.	Inactive bill – Died 11/30/2022 – From committee without further action
SB-1140	Public social services: electronic benefits transfer cards.		Umberg.	

SB-1454	California Privacy Rights Act of 2020: exemptions.		Archuleta.	Inactive bill – Died 11/30/2022 – From committee without further action.
---------	--	--	------------	--

Appendix C

Proposed Control Set for Initial Risk Assessment Summaries for Identifying High-risk Entities.

Proposal Use this smaller subset of common controls from NIST, ISO, CIS, and OWASP to establish a minimum standard nearly all businesses can meet. If more stringent standards are needed due to significantly greater risk exposure or harm, they can be layered on top of the baseline, much like PCI-DSS or HITRUST is structured. This control subset is documented in this Excel Workbook, published in my public data catalog accessible from this link:

<https://query.data.world/s/iohi7b7aao4bb5on6bjvifvwfbj3le?dws=00000>

Note: The methodology I used to create a smaller subset was:

- 1) select the greatest number of common controls from all standards
- 2) select the controls most relevant to CCPA test cases and mandated cybersecurity audits and assessments.

Note: NIST 800-53r4 is the current standard for California Office Information Security. This proposed control set uses Revision 5 which incorporates many controls from the Privacy Framework and Cybersecurity Framework for Improving Critical Infrastructure. It represents a baseline canonical model, which all other standard control frameworks are mapped to.

National Institute of Standards and Technology Special Publication 800-53, Revision 5

<https://doi.org/10.6028/NIST.SP.800-53r5>

This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk. The controls address diverse requirements derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines. Finally, the consolidated control catalog addresses security and privacy from a functionality perspective (i.e., the strength of functions and mechanisms provided by the controls) and from an assurance perspective (i.e., the measure of confidence in the security or privacy capability provided by the controls). Addressing functionality and assurance helps to ensure that information technology products and the systems that rely on those products are sufficiently trustworthy.

Self-Assessment Questionnaire for Risk Assessment Summaries	NIST Control Family	NIST SP 800-53, Revision 5 Controls	Related NIST Controls
Who has access to my online account?		AC-1: Policy and Procedures	AU-2: Event Logging; AU-3: Content of Audit Records; AC-6: Least Privilege
Who accessed my online account for what purpose?		AC-2: Account Management	AU-2: Event Logging; AU-3: Content of Audit Records; AC-6: Least Privilege; PT-3: Personally Identifiable Information Processing Purposes
Which enforcement mechanisms are used? (ACL, firewall rule, LDAP, Oauth, JWT, Kerberos, etc.)		AC-3: Access Enforcement	SC-7: Boundary Protection; AU-2: Event Logging; AU-3: Content of Audit Records

Which internal and external
processes is my PI shared
with?

Access Control
(AC)

AC-4: Information Flow
Enforcement

AU-2: Event Logging;
AU-3: Content of Audit
Records;
RA-8: Privacy Impact
Assessments;

How many internal and external users accessed my PI?		AC-6: Least Privilege	AU-2: Event Logging; AU-3: Content of Audit Records; PT-3: Personally Identifiable Information Processing Purposes
Are security or privacy key value attribute labels, markers, or tags applied to assets for enforcing		AC-16: Security and Privacy Attributes	PM-5: System Inventory; RA-8: Privacy Impact Assessments;
Are appropriate enforcement mechanisms used for each type of remote access?		AC-17: Remote Access	AC-3: Access Enforcement; AU-2: Event Logging; AU-3: Content of Audit Records; IA-2: Identification and Authentication (organizational Users);
How well do remote access controls on external systems match controls on internal systems?		AC-20: Use of External Systems	IA-2: Identification and Authentication (organizational Users); IA-8: Identification and Authentication (non-organizational Users); SR-1: Policy and
Where can all the privacy controls and procedures be found?		AT-1: Policy and Procedures	CA-1: Policy and Procedures

	Awareness and Training (AT)		
What are all employees required to know about information security and data privacy best practices?		AT-2: Literacy Training and Awareness	CA-1: Policy and Procedures
Who is responsible and accountable for specific aspects of information security and data privacy?		AT-3: Role-based Training	PM-13: Security and Privacy Workforce; PM-15: Security and Privacy Groups and Associations; PM-20: Dissemination of Privacy Program

Where can all the audit logs and procedures be found?	Audit and Accountability (AU)	AU-1: Policy and Procedures	AU-1: Policy and Procedures; AU-2: Event Logging; AU-3: Content of Audit Records; AU-6: Audit Record Review, Analysis, and Reporting; RA-8: Privacy Impact Assessments; PT-3: Personally Identifiable Information Processing Purposes
Where are audit logs required and which events are logged?		AU-2: Event Logging	
Which fields in each event are required to capture necessary audit log details?		AU-3: Content of Audit Records	
When are audit logs reviewed, by whom, and for what purpose?		AU-6: Audit Record Review, Analysis, and Reporting	

Which systems or processes consume information about control status?	Assessment, Authorization, and Monitoring (CA)	CA-1: Policy and Procedures	PM-5: System Inventory
How are controls evaluated?		CA-2: Control Assessments	RA-3: Risk Assessments;
Which assets are monitored for control risks?		CA-7: Continuous Monitoring	PM-5: System Inventory
How are control assessments verified?		CA-8: Penetration Testing	RA-3: Risk Assessments;



	Configuration Management (CM)	CM-1: Policy and Procedures	
Minimum configuration requirements for each asset		CM-2: Baseline Configuration	
Configuration change events are detected and reported		CM-3: Configuration Change Control	
When are Privacy Impact Analyses required for new or modified assets that involve PII?		CM-4: Impact Analyses	SI-2: Flaw Remediation; RA-8: Privacy Impact Assessments;
What changed in the configuration of each asset?		CM-6: Configuration Settings	
What essential business purpose does this asset fulfill and why is it technically required to be functional?		CM-7: Least Functionality	PT-3: Personally Identifiable Information Processing Purposes

Which assets are components or dependancies of other assets, and which common controls are inherited?		CM-8: System Component Inventory	
Where in the system and in what jurisdiction are data assets collected, stored, and processed?		CM-12: Information Location	SC-42: Sensor Capability and Data; SC-7: Boundary Protection



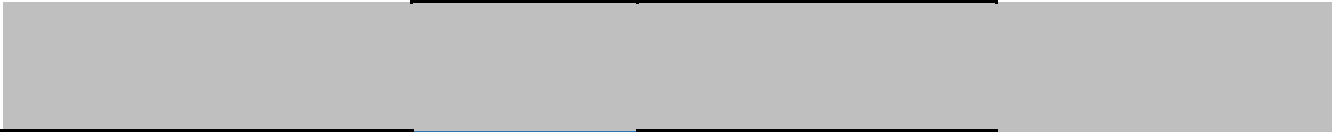
which policies and procedures are essential to maintaining business continuity?		CP-1: Policy and Procedures	SC-5: Denial-of-service Protection
Which assets and resources are included in Contingency Plans?		CP-2: Contingency Plan	
Where are CP test results reported?	Contingency Planning (CP)	CP-4: Contingency Plan Testing	
What controls protect the security and integrity of data backups?		CP-9: System Backup	
How much time elapses before a system is fully recovered?		CP-10: System Recovery and Reconstitution	



which policies and procedures are essential to ensuring all authorized users can access a system?		IA-1: Policy and Procedures	

How well does user IA controls match asset access controls?		IA-2: Identification and Authentication (organizational Users)	AC-20: Use of External Systems
Do system or service account identifiers contain PI or public information?		IA-4: Identifier Management	SI-19: De-identification
Which authenticators are used for which purpose to access a specific asset?		IA-5: Authenticator Management	PM-5: System Inventory; AC-20: Use of External Systems; PT-3: Personally Identifiable Information Processing Purposes
	Identification and Authentication (IA)		
What measures disassociate user attributes or identifier assertion relationships among individuals, credential service providers, and relying parties?		IA-8: Identification and Authentication (non-organizational Users); RA-8: Privacy Impact Assessments;	

--	--



Which policies, procedures, and events involve incident response controls?	Incident Response (IR)	IR-1: Policy and Procedures	
Where are IR test results reported?		IR-3: Incident Response Testing	
Who is involved in IR and what are their roles?		IR-4: Incident Handling	PS-7: External Personnel Security
Which events require IR, and where can IR reports be found?		IR-6: Incident Reporting	SI-5: Security Alerts, Advisories, and Directives; RA-3: Risk Assessment

Which assets and resources are included in Incident Response Plans?		IR-8: Incident Response Plan	PM-5: System Inventory; SC-1: Policy and Procedures
Which assets and resources require periodic changes, like patches, licenses, and information updates?	Maintenance (MA)	MA-1: Policy and Procedures	PM-5: System Inventory
Are laptops, tablets, and mobile phones classified as removable media?	Media Protection (MP)	MP-1: Policy and Procedures	
		MP-5: Media Transport	
		MP-7: Media Use	
	Physical and Environmental Protection (PE)	PE-1: Policy and Procedures	
Which physical access authenticators are used, and what PI is collected or processed by these controls?		PE-6: Monitoring Physical Access	RA-8: Privacy Impact Assessments;
Which critical assets and resources require a redundant, alternative power source?		PE-11: Emergency Power	
Which products and processes require security and privacy considerations?	Planning (PL)	PL-1: Policy and Procedures	PM-1: Information Security Program Plan; PM-5: System Inventory

What are the product and process requirements for protecting the confidentiality, integrity, and availability of	Planning (PL)	PL-8: Security and Privacy Architectures	PM-1: Information Security Program Plan; RA-8: Privacy Impact Assessments
Which internal programs and common controls implement Information Security policies?	Program Management (PM)	PM-1: Information Security Program Plan	SC-28: Protection of Information at Rest; SC-8: Transmission Confidentiality and Integrity; SA-8: Security and Privacy Engineering Principles;
How are remediation actions prioritized, scheduled, and evaluated?		PM-4: Plan of Action and Milestones Process	SI-2: Flaw Remediation
Is there an inventory of systems, applications, and projects that process personally identifiable information?		PM-5: System Inventory	PM-21: Accounting of Disclosures
Does your industry play a role in Critical Infrastructure, and if so is there a plan for		PM-8: Critical Infrastructure Plan	
what action relation demonstrates that risk management processes are established, managed, and		PM-9: Risk Management Strategy	RA-1: Policy and Procedures; RA-3: Risk Assessments; RA-8: Privacy Impact
Are there role-based workforce development and improvement programs which		PM-13: Security and Privacy Workforce	AT-3: Role-based Training
include defining the		PM-15: Security and Privacy Groups and Associations	AT-3: Role-based Training
How does your security and privacy workforce stay current on recommended security and privacy practices, techniques		PM-20: Dissemination of Privacy Program Information	PT-5: Privacy Notice
where can internal and external users learn more about your privacy and data protection practices?			

Are individuals permitted to learn to whom their personally identifiable information has been disclosed, and if so, how?		PM-21: Accounting of Disclosures	AU-6: Audit Record Review, Analysis, and Reporting;
How do you confirm and disseminate the accuracy and relevance of personally identifiable information throughout the information life cycle?		PM-22: Personally Identifiable Information Quality Management	IA-2: Identification and Authentication (organizational Users); IA-8: Identification and
Are public individuals permitted to file complaints, questions, or concerns, and if so, are they provided with the		PM-26: Complaint Management	IR-6: Incident Reporting; RA-8: Privacy Impact Assessments;
Are there any reporting mechanisms which document progress in meeting privacy compliance requirements, and if so who receives these reports?		PM-27: Privacy Reporting	IR-6: Incident Reporting; RA-8: Privacy Impact Assessments;
Which roles are stakeholders in managing risk across the enterprise?		PM-28: Risk Framing	PT-1: Policy and Procedures; RA-3: Risk Assessments

What factors are evaluated in personnel screening that pertain directly to security and privacy risks?	Personnel Security (PS)	PS-1: Policy and Procedures	RA-3: Risk Assessments
Which systems, resources or processes require access agreements with signed acknowledgments that		PS-6: Access Agreements	PT-4: Consent; PT-3: Personally Identifiable Information Processing Purposes
How is provider compliance with personnel security requirements monitored?		PS-7: External Personnel Security	AC-20: Use of External Systems; IR-4: Incident Handling

<p>Who is ultimately responsible for ensuring that Personally Identifiable Information Processing is transparent to all stakeholders?</p>	<p>Personally Identifiable Information Processing and Transparency (PT)</p>	<p>PT-1: Policy and Procedures</p>	<p>PM-21: Accounting of Disclosures</p>

What legal or contractual authority is granted for processing PII?		PT-2: Authority to Process Personally Identifiable Information	SR-1: Policy and Procedures
What purposes are authorized for processing PII?		PT-3: Personally Identifiable Information Processing Purposes	PM-21: Accounting of Disclosures
What consents authorized for processing PII?		PT-4: Consent	PM-21: Accounting of Disclosures
Where can individuals find more information about privacy practices and risks?		PT-5: Privacy Notice	Dissemination
Is there a vulnerability management plan or program that implements policies and procedures and evaluates?		RA-1: Policy and Procedures	PM-9: Risk Management Strategy
Which stakeholders review risk assessment results, and how frequently?		RA-3: Risk Assessment	PT-1: Policy and Procedures; IR-6: Incident Reporting

Is there documentation of which assets must be scanned for vulnerabilities, including how frequently?	Risk Assessment (RA)	RA-5: Vulnerability Monitoring and Scanning	SR-1: Policy and Procedures; SA-9: External System Services
Is there a record of when Privacy Impact Assessments are performed for new system acquisitions, changes in		RA-8: Privacy Impact Assessments	SR-1: Policy and Procedures; SA-9: External System Services
Is there documentation of mission-critical system components used to determine essential assets for		RA-9: Criticality Analysis	PM-5: System Inventory

Is there documentation showing when, according to policy, new assets are tested for functionality?	System and Services Acquisition (SA)	SA-1: Policy and Procedures	SR-1: Policy and Procedures;
Are security tests or scans routinely performed at appropriate stages in the SDLC?		SA-3: System Development Life Cycle	CM-8: System Component Inventory
Is there documentation of onboarding, evaluating, and offboarding suppliers?		SA-4: Acquisition Process	SR-1: Policy and Procedures; RA-8: Privacy Impact Assessments
Are security and privacy engineering principles documented for assets in the system inventory?		SA-8: Security and Privacy Engineering Principles	PM-5: System Inventory
How are audits, test results, or other forms of evaluations shared with stakeholders for assuring that suppliers are meeting their contractual obligations?		SA-9: External System Services	AC-20: Use of External Systems; SR-1: Policy and Procedures; SC-8: Transmission Confidentiality and Integrity
How are configuration changes documented, managed, and approved within the SDLC?		SA-10: Developer Configuration Management	CM-8: System Component Inventory

How are stakeholders, in accordance with policy, notified when an event requires their action or showing how 'adequate capacity' is calculated for each critical asset, and whether it is	System and Communications Protection (SC)	SC-1: Policy and Procedures	AI-3: Role-based Training; PT; PM-9: Risk Management Strategy
Are any assets and resources in the system inventory classified as endpoints requiring boundary protection controls?		SC-5: Denial-of-service Protection	CP-1: Policy and Procedures
Are data protection controls selected in accordance with risk assessments, data sensitivity, and local or		SC-7: Boundary Protection	AC-3: Access Enforcement; PM-5: System Inventory; CM-12: Information Location
what internet, local, or process is used to scan all traffic for security and privacy attributes, which could be		SC-8: Transmission Confidentiality and Integrity	RA-8: Privacy Impact Assessments; SA-9: External System Services
is there documentation on which data assets and system components require controls for confidentiality, integrity		SC-16: Transmission of Security and Privacy Attributes	scans
Does the system inventory identify sensors in devices that can collect and record data about the user or the		SC-28: Protection of Information at Rest	PM-5: System Inventory; RA-8: Privacy Impact Assessments;
		SC-42: Sensor Capability and Data	CM-12: Information Location; SC-7: Boundary Protection
Is there documentation of every flaw remediated, in accordance with all Risk Assessment (RA), Program Management (PM), and		SI-2: Flaw Remediation	PM-4: Plan of Action and Milestones Process; CM-4: Impact Analyses; RA-3: Risk Assessments
Are all internal and external system monitoring activities reviewed for privacy impacts?		SI-4: System Monitoring	RA-8: Privacy Impact Assessments
Is there documentation showing which system security alerts, advisories, and directives are received		SI-5: Security Alerts, Advisories, and Directives	IR-6: Incident Reporting; RA-3: Risk Assessment
Are data management and			

retention requirements documented in the system inventory that covers the full life cycle of information?	System and Information Integrity (SI)	SI-12: Information Management and Retention	PT-3: Personally Identifiable Information Processing Purposes
Do you have a routine process for validating the accuracy of personally identifiable information which may be used to make determinations about the rights, benefits, or privileges of individuals?		SI-18: Personally Identifiable Information Quality Operations *	* Automated Decision-Making; SR-4: Provenance *
Do you test for re-identification as a residual risk over time with de-identified data?		SI-19: De-identification	IA-8: Identification and Authentication (non-organizational Users); IA-4: Identifier Management

who or what role is designated to be responsible for managing the development, documentation, and maintain chronological provenance information on the origin, development, ownership, location, and changes to a system or system component and associated	Supply Chain Risk Management (SR)	SR-1: Policy and Procedures	SA-9: External System Services; RA-8: Privacy Impact Assessments
Do you document, monitor, and maintain chronological provenance information on the origin, development, ownership, location, and changes to a system or system component and associated		SR-4: Provenance *	SI-18: Personally Identifiable Information Quality Operations *

Regulation Section	Section Title	ROLE	GOAL OR STRATEGY	ISSUE	Referenced Civil Codes
§ 7060.	General Rules Regarding Verification.	Consumer	DISCOVER HIGH-RISK VERIFICATION	Match Identifying Information	1798.105, 1798.106, 1798.110,
§ 7060.	General Rules Regarding Verification.	Consumer	DISCOVER HIGH-RISK VERIFICATION	PI Not Necessary for Verification	1798.105, 1798.106, 1798.110,
§ 7060.	General Rules Regarding Verification.	Consumer	DISCOVER HIGH-RISK VERIFICATION	Process Not Stringent For High Risk PI	1798.105, 1798.106, 1798.110,
California Consumer Privacy Act of	Information Security Breaches	Consumer	SECURITY RISK ASSESSMENT TO AGENCY	Implement and Maintain Reasonable	1798.150.
§ 7060.	General Rules Regarding Verification.	Consumer	DISCOVER HIGH-RISK VERIFICATION	Match Identifying Information	1798.105, 1798.106, 1798.110,
§ 7060.	General Rules Regarding Verification.	Consumer	DISCOVER HIGH-RISK VERIFICATION	PI Not Necessary for Verification	1798.105, 1798.106, 1798.110,
§ 7060.	General Rules Regarding Verification.	Consumer	DISCOVER HIGH-RISK VERIFICATION	Process Not Stringent For High Risk PI	1798.105, 1798.106, 1798.110,
California Consumer Privacy Act of	Information Security Breaches	Consumer	SECURITY RISK ASSESSMENT TO AGENCY	Implement and Maintain Reasonable	1798.150.
§ 7002	the Collection and Use of Personal	Business	COMPLIANCE WITH CONSUMER'S	Inconsistent With Consumer's	1798.106, 1798.121, 1798.130,
§ 7002	the Collection and Use of Personal	Business	DISCLOSED PURPOSE AT TIME OF	Purpose Incompatible With Context	1798.106, 1798.121, 1798.130
§ 7012	Collection of Personal Information.	Consumer	CHOOSE TO ENGAGE	Notices to Consumers	1798.100, 1798.115, 1798.120
§ 7012	Collection of Personal Information.	Consumer	CHOOSE TO ENGAGE	Compliant Notice of Collection	1798.100, 1798.115, 1798.120,
§ 7012	Collection of Personal Information.	Consumer	CHOOSE TO ENGAGE	Compliant Notice of Collection	1798.100, 1798.115, 1798.120,

§ 7011	Privacy Policy.	Business	VERIFY CHOICE	Compliant Disclosure of Categories of	1798.105, 1798.106, 1798.110,
§ 7011	Privacy Policy.	Business	VERIFY CHOICE	Compliant Disclosure of Specific	1798.105, 1798.106, 1798.110,
§ 7011	Privacy Policy.	Business	VERIFY CHOICE	of CCPA Request Methods	1798.105, 1798.106, 1798.110,
§ 7011	Privacy Policy.	Business	VERIFY CHOICE	of CCPA Request Methods	1798.105, 1798.106, 1798.110,
§ 7020.	Submitting Requests to Delete,	Business	MINIMUM REQUIREMENTS	Execute Request Methods	1798.105, 1798.106, 1798.110,
§ 7020.	Submitting Requests to Delete,	Business	DELETIONS; AVOID PROCESSING	Erroneous Treatment of Requests	1798.105, 1798.106, 1798.110,
§ 7024	Requests to Know.	Consumer	DISCOVER PI	Undisclosed Collection	1798.115, 1798.130, 1798.140,
§ 7024	Requests to Know.	Consumer	DISCOVER PROCESSING ERRORS	Treatment of Requests to Know	
§ 7023	Requests to Correct.	Consumer	DISCOVER CORRECTION OVERRIDES	Information Overridden By Inaccurate	1798.130 1798.185, 1798.81 5
§ 7027	Limit Use and Disclosure of Sensitive	Consumer	DISCOVER NECESSARY SENSITIVE PI	No Meaningful Control	1798.135, 1798.140, 1798.185
§ 7025.	Opt-Out Preference Signals.	Consumer	UNAUTHORIZED USE OF PREFERENCE	Unauthorized Use	1798.135, 1798.140, 1798.185
§ 7022	Requests to Delete.	Consumer	THIRD PARTY NOTIFICATIONS	Notification Failure	1798.105, 1798.130 and 1798.185
§ 7022	Requests to Delete.	Consumer	DISCOVER PROCESSING ERRORS	Treatment of Requests to Delete	
§ 7063.	Authorized Agents.	Authorized Agents	FULLFILLMENT , VERIFICATION,	Prohibited Use of Consumer's PI	1798.105, 1798.106, 1798.110,

§ 7050.	Service Providers and Contractors.	Service Providers and Contractors.	DISCOVER EXCEPTIONS FOR USE OF PI	Non-Compliant Use of PI	1798.105, 1798.106, 1798.110,
§ 7101	Record-Keeping.	Business	SHARED WITH THIRD PARTIES ARE	Request Records Improperly	1798.106, 1798.110, 1798.115,
California Consumer Privacy Act of	Information Security Breaches	Consumer	SECURITY RISK ASSESSMENT TO AGENCY	Implement and Maintain Reasonable	1798.150.
§ 7027	Limit Use and Disclosure of Sensitive	Consumer	EXCEPTIONS FOR NO NOTICE	Exception For Posting Notice To Limit	1798.135, 1798.140, 1798.185
§ 7061.	Password-Protected Accounts	Consumer	DISCOVER SECURITY ISSUES	Malicious Activity Suspected	1798.105, 1798.106, 1798.110,
§ 7061.	Password-Protected Accounts.	Consumer	DISCOVER SECURITY ISSUES	Re-authentication Not Required	1798.105, 1798.106, 1798.110,
§ 7050.	Service Providers and Contractors.	Service Providers and Contractors.	DISCOVER EXCEPTIONS FOR USE OF PI	Non-Compliant Use of PI	1798.105, 1798.106, 1798.110,
§ 7060.	General Rules Regarding Verification.	Consumer	DISCOVER HIGH-RISK VERIFICATION	Match Identifying Information	1798.105, 1798.106, 1798.110,

§ 7012	Collection of Personal Information.	Consumer	CHOOSE TO ENGAGE	Compliant Link to Notice of Collection	1798.100, 1798.115, 1798.120
§ 7012	Collection of Personal Information.	Consumer	CHOOSE TO ENGAGE	Compliant Link to Notice of Collection	1798.100, 1798.115, 1798.120
§ 7012	Collection of Personal Information.	Consumer	CHOOSE TO ENGAGE	Compliant Link to Notice of Collection	1798.100, 1798.115, 1798.120
§ 7012	Collection of Personal Information.	Consumer	CHOOSE TO ENGAGE	Notices to Consumers	1798.100, 1798.115, 1798.120
§ 7012	Collection of Personal Information.	Consumer	CHOOSE TO ENGAGE	Notices to Consumers	1798.100, 1798.115, 1798.120,

§ 7012	Collection of Personal Information.	Consumer	CHOOSE TO ENGAGE	Notices to Consumers	1798.100, 1798.115, 1798.120
§ 7012	Collection of Personal Information.	Consumer	CHOOSE TO ENGAGE	Notices to Consumers	1798.100, 1798.115, 1798.120
§ 7012	Collection of Personal Information.	Consumer	CHOOSE TO ENGAGE	Notices to Consumers	1798.100, 1798.115, 1798.120,
§ 7100	Training.	Business	Compliant Handling of Requests	Staff not informed of all requirements	1798.105, 1798.106, 1798.110,
§ 7100	Training.	Business	Compliant Handling of Requests	Staff unaware of sale / share	
§ 7100	Training.	Business	Compliant Handling of Requests	Staff not informed of all requirements	1798.105, 1798.106, 1798.110,
§ 7011	Privacy Policy.	Business	VERIFY CHOICE	of CCPA Request Methods	1798.105, 1798.106, 1798.110,

§ 7101	Record-Keeping.	Consumer	PROVE SECURITY ISSUES	No Records of Consumer Requests	1798.106, 1798.110, 1798.115,
§ 7101	Record-Keeping.	Consumer	PROVE RETENTION ISSUES	Consumer Requests Not Maintained	1798.106, 1798.110, 1798.115,
§ 7101	Record-Keeping.	Business	SECURE CUSTOMER RECORDS	Security Not Maintained For Consumer	1798.106, 1798.110, 1798.115,
§ 7101	Record-Keeping.	Business	DISCREPANCIES BY DISPERSING	Records of Consumer Requests	1798.106, 1798.110, 1798.115,
§ 7024	Requests to Know.	Consumer	THIRD PARTIES PI DISCLOSED TO	Categories of PI Disclosed for Business	1798.115, 1798.130, 1798.140,



§ 7011	Privacy Policy.	Business	VERIFY CHOICE	of CCPA Request Methods	1798.105, 1798.106, 1798.110,
--------	-----------------	----------	---------------	-------------------------------	-------------------------------------

§ 7070.	Consumers Less Than Under 13 Years of Age	Consumer	CHOOSE TO ENGAGE	Compliant Guardian Verification	1798.120, 1798.135, 1798.185
§ 7024	Requests to Know.	Consumer	VERIFIABLE REQUEST FOR SPECIFIC PI	Compliant Verification Procedures	1798.115, 1798.130, 1798.140,
§ 7024	Requests to Know.	Business	DO NOT DISCLOSE SPECIFIC PI	Non-Verifiable Requests	1798.115, 1798.130, 1798.140,
§ 7024	Requests to Know.	Consumer	VERIFIABLE REQUEST FOR CATEGORIES	Compliant Verification Procedures	1798.115, 1798.130, 1798.140,
§ 7024	Requests to Know.	Business	REQUEST FOR CATEGORIES OF PI	Non-Verifiable Requests	1798.115, 1798.130, 1798.140,
§ 7023	Requests to Correct.	Consumer	SUBMIT VERIFIABLE REQUEST	Compliant Verification Procedures	1798.130 1798.185, 1798.81 5
§ 7023	Requests to Correct.	Business	DO NOT CORRECT SPECIFIC PI	Non-Verifiable Requests	1798.130 1798.185, 1798.81 5
§ 7063.	Authorized Agents.	Authorized Agents	SIGNED PERMISSION FROM	No Agent Signed Permission	1798.105, 1798.106, 1798.110,
§ 7063.	Authorized Agents.	Authorized Agents	FULLFILLMENT , VERIFICATION,	Prohibited Use of Consumer's PI	1798.105, 1798.106, 1798.110,

§ 7060.	General Rules Regarding Verification.	Consumer	DISCOVER REASONABLE VERIFICATION	Compliant Verification Procedures	1798.105, 1798.106, 1798.110,
§ 7060.	General Rules Regarding Verification.	Consumer	DISCOVER HIGH-RISK VERIFICATION	Match Identifying Information	1798.105, 1798.106, 1798.110,
§ 7060.	General Rules Regarding Verification.	Consumer	DISCOVER HIGH-RISK VERIFICATION	PI Not Necessary for Verification	1798.105, 1798.106, 1798.110,
§ 7060.	General Rules Regarding Verification.	Consumer	DISCOVER IMPEDIMENTS	Inaccurate Data Used For Verification	1798.105, 1798.106, 1798.110,
§ 7061.	Password-Protected Accounts	Consumer	DISCOVER SECURITY ISSUES	Re-authentication Not Required	1798.105, 1798.106, 1798.110,
§ 7062.	Non-Accountholders.	Consumer	DISCOVER DATA POINTS	Unreliable Degree of Certainty	1798.105, 1798.106, 1798.110,
§ 7062.	Non-Accountholders.	Consumer	DISCOVER HIGH-RISK VERIFICATION	Unreliable High Degree of Certainty	1798.105, 1798.106, 1798.110,

§ 7027	Limit Use and Disclosure of Sensitive	Consumer	MALICIOUS ACTION EXCEPTIONS	Exception For Posting Notice To Limit	1798.135, 1798.140, 1798.185
--------	---------------------------------------	----------	-----------------------------	---------------------------------------	------------------------------

California Consumer Privacy Act of	Information Security Breaches	Consumer	SECURITY RISK ASSESSMENT TO AGENCY	Implement and Maintain Reasonable	1798.150.
--	-------------------------------------	----------	--	---	-----------

§ 7027	Limit Use and Disclosure of Sensitive	Consumer	PHYSICAL SAFETY EXCEPTIONS	Exception For Posting Notice To Limit	1798.135, 1798.140, 1798.185
--------	---	----------	----------------------------------	---	------------------------------------

California Consumer Privacy Act of	Information Security Breaches	Consumer	SECURITY RISK ASSESSMENT TO AGENCY	Implement and Maintain Reasonable	1798.150.
--	-------------------------------------	----------	--	---	-----------

§ 7011	Privacy Policy.	Business	VERIFY CHOICE	Compliant Description of Information	1798.105, 1798.106, 1798.110,
California Consumer Privacy Act of	Information Security Breaches	Consumer	SECURITY RISK ASSESSMENT TO AGENCY	Implement and Maintain Reasonable	1798.150.

§ 7002	the Collection and Use of Personal	Business	DISCLOSED PURPOSE DEFENSE	Purpose Incompatible With Context	1798.106, 1798.121, 1798.130,
§ 7002	the Collection and Use of Personal	Business	UNDISCLOSED COLLECTION AND USE	Collection Not Disclosed or Incompatible	1798.106, 1798.121, 1798.130,
§ 7024	Requests to Know.	Consumer	DISCOVER PI	Undisclosed Collection	1798.115, 1798.130, 1798.140,
§ 7024	Requests to Know.	Consumer	DISCOVER PI	Incomplete Categories of PI Collected	1798.115, 1798.130, 1798.140,

§ 7100	Training.	Business	Compliant Handling of Requests	Staff not informed of all requirements	1798.105, 1798.106, 1798.110,
§ 7100	Training.	Business	Compliant Handling of Requests	Staff not informed of all requirements	1798.105, 1798.106, 1798.110,
§ 7011	Privacy Policy.	Business	VERIFY CHOICE	of CCPA Request Methods	1798.105, 1798.106, 1798.110,

§ 7010	Overview of Required Disclosures.	Business	AVOID PROVIDING NOTICE	No Notice at Collection	1798.105, 1798.106, 1798.110,
§ 7024	Requests to Know.	Consumer	THIRD PARTIES PI DISCLOSED TO	Categories of PI Disclosed for Business	1798.115, 1798.130, 1798.140,
§ 7023	Requests to Correct.	Consumer	TEST FOR DENIALS	Denied Due To Totality of Circumstances	1798.130 1798.185, 1798.81 5
§ 7023	Requests to Correct.	Business	DENY REQUEST	Denied Due To Totality of Circumstances	1798.130 1798.185, 1798.81 5
§ 7060.	General Rules Regarding Verification.	Consumer	DISCOVER HIGH-RISK VERIFICATION	Match Identifying Information	1798.105, 1798.106, 1798.110,
§ 7011	Privacy Policy.	Business	VERIFY CHOICE	of CCPA Request Methods	1798.105, 1798.106, 1798.110,
§ 7102	for Businesses Collecting Large Amounts	Agency	NON-COMPLIANT BUSINESSES	Metrics Not Disclosed By July 1	1798.106, 1798.110, 1798.115,
§ 7011	Privacy Policy.	Business	VERIFY CHOICE	No Required Data Reporting	1798.105, 1798.106, 1798.110,

§ 7070.	Consumers Less Than Under 13 Years of Age	Consumer	CHOOSE TO ENGAGE	Required Links for Minors	1798.120, 1798.135, 1798.185
§ 7071.	Consumers at Least 13 Years of Age and Less Than 16	Consumer	CHOOSE TO ENGAGE	Required Links for Minors	1798.120, 1798.135, 1798.185
§ 7072.	Notices to Consumers Less Than 16 Years of Age	Consumer	CHOOSE TO ENGAGE	Required Links for Minors	1798.120, 1798.135, 1798.185
§ 7013	to Opt-Out of Sale/Sharing and the “Do	Consumer	CHOOSE TO OPT-OUT	Missing Opt-out Notice	1798.120, 1798.135, 1798.185
§ 7014	to Limit and the “Limit the Use of My	Consumer	CHOOSE TO LIMIT	No Limit Request Instructions	1798.121, 1798.135, 1798.185
§ 7015	Alternative Opt-Out Link.	Consumer	CHOOSE TO LIMIT & OPT-OUT	Missing Opt-out Notice	1798.121, 1798.135 and 1798.185
§ 7011	Privacy Policy.	Business	VERIFY CHOICE	of CCPA Request Methods	1798.105, 1798.106, 1798.110,
§ 7024	Requests to Know.	Consumer	DISCOVER PROCESSING ERRORS	Treatment of Requests to Know	
§ 7026	Requests to Opt-Out of Sale/Sharing.	Consumer	DISCOVER PROCESSING ERRORS	Treatment of Requests to Opt-out	
§ 7027	Limit Use and Disclosure of Sensitive	Consumer	DISCOVER PROCESSING ERRORS	Treatment of Requests to Opt-out	
§ 7022	Requests to Delete.	Consumer	DISCOVER PROCESSING ERRORS	Treatment of Requests to Delete	
§ 7062.	Non-Accountholders.	Consumer	DISCOVER HIGH-RISK VERIFICATION	Requires Reasonably High Degree of	1798.105, 1798.106, 1798.110,
§ 7002	the Collection and Use of Personal	Business	COMPLIANCE WITH PURPOSE	Unnecessary Collection or Purpose	1798.106, 1798.121, 1798.130,
§ 7027	Limit Use and Disclosure of Sensitive	Consumer	DISCOVER NECESSARY SENSITIVE PI	No Meaningful Control	1798.135, 1798.140, 1798.185

§ 7027	Limit Use and Disclosure of Sensitive	Consumer	RIGHT TO LIMIT EXCEPTIONS	Exception For Posting Notice To Limit	1798.135, 1798.140, 1798.185
§ 7050.	Service Providers and Contractors.	Service Providers and Contractors.	DISCOVER EXCEPTIONS FOR USE OF PI	Non-Compliant Use of PI	1798.105, 1798.106, 1798.110,
§ 7050.	Service Providers and Contractors.	Service Providers and Contractors.	AVOID NOTIFICATION OF DENIAL	No Notification of Denial	1798.105, 1798.106, 1798.110,
§ 7002	the Collection and Use of Personal	Business	COMPLIANCE WITH CONSUMER'S	Inconsistent With Consumer's	1798.106, 1798.121, 1798.130,
§ 7002	the Collection and Use of Personal	Business	COMPLIANCE WITH CONSUMER'S	Inconsistent With Consumer's	1798.106, 1798.121, 1798.130,
§ 7023	Requests to Correct.	Consumer	CONFIRMATION OF CORRECTION	Confirmation Inaccurate Information	1798.130 1798.185, 1798.81 5
§ 7101	Record-Keeping.	Business	NON-CCPA PURPOSE FOR RETAINING PI	Requests to Delete Denied	1798.106, 1798.110, 1798.115,
§ 7024	Requests to Know.	Consumer	DISCOVER PI SOLD	Purpose of Collection or Sale	1798.115, 1798.130, 1798.140,
§ 7002	the Collection and Use of Personal	Business	CONSENT FOR OTHER PURPOSES	Consent Not Obtained For Each Purpose	1798.106, 1798.121, 1798.130,
§ 7010	Overview of Required Disclosures.	Business	AVOID ENFORCEMENT	No Privacy Policy	1798.105, 1798.106, 1798.110,
§ 7011	Privacy Policy.	Consumer	VERIFY CHOICE	Non-Compliant Privacy Policy	1798.105, 1798.106, 1798.110,

California Consumer Privacy Act of	Information Security Breaches	Consumer	SECURITY RISK ASSESSMENT TO AGENCY	Implement and Maintain Reasonable	1798.150.
------------------------------------	-------------------------------	----------	------------------------------------	-----------------------------------	-----------

§ 7060.	General Rules Regarding Verification.	Consumer	DISCOVER HIGH-RISK VERIFICATION	Process Not Stringent For High Risk PI	1798.105, 1798.106, 1798.110,
§ 7102	for Businesses Collecting Large Amounts	Agency	BUSINESSES SUBJECT TO REQUIREMENT	Required Metrics Not Compiled	1798.106, 1798.110, 1798.115,

California Consumer Privacy Act of	Information Security Breaches	Consumer	SECURITY RISK ASSESSMENT TO AGENCY	Implement and Maintain Reasonable	1798.150.
§ 7050.	Service Providers and Contractors.	Service Providers and Contractors.	DISCOVER EXCEPTIONS FOR USE OF PI	Non-Compliant Use of PI	1798.105, 1798.106, 1798.110,
§ 7050.	Service Providers and Contractors.	Service Providers and Contractors.	DISCOVER EXCEPTIONS FOR USE OF PI	Non-Compliant Use of PI	1798.105, 1798.106, 1798.110,

California Consumer Privacy Act of	Information Security Breaches	Consumer	SECURITY RISK ASSESSMENT TO AGENCY	Implement and Maintain Reasonable	1798.150.
------------------------------------	-------------------------------	----------	------------------------------------	-----------------------------------	-----------

California Consumer Privacy Act of	Information Security Breaches	Consumer	SECURITY RISK ASSESSMENT TO AGENCY	Implement and Maintain Reasonable	1798.150.
§ 7027	Limit Use and Disclosure of Sensitive	Consumer	QUALITY OF SERVICE EXCEPTIONS	Exception For Posting Notice To Limit	1798.135, 1798.140, 1798.185

§ 7061.	Password-Protected Accounts.	Consumer	DISCOVER SECURITY ISSUES	Malicious Activity Suspected	1798.105, 1798.106, 1798.110,
California Consumer Privacy Act of	Information Security Breaches	Consumer	SECURITY RISK ASSESSMENT TO AGENCY	Implement and Maintain Reasonable	1798.150
§ 7012	Collection of Personal Information.	Consumer	CHOOSE TO ENGAGE	Noncompliant Retention Disclosures	1798.100, 1798.115, 1798.120,

§ 7022	Requests to Delete.	Consumer	DISCOVER THIRD PARTY COLLECTIONS	Unauthorized Use	1798.105, 1798.130 and 1798.185
§ 7101	Record-Keeping.	Business	NON-CCPA PURPOSE FOR RETAINING PI	Requests to Delete Denied	1798.106, 1798.110, 1798.115,
§ 7023	Requests to Correct.	Consumer	TEST FOR DENIALS	Denied Due To Totality of Circumstances	1798.130 1798.185, 1798.81 5
§ 7023	Requests to Correct.	Business	DENY REQUEST	Denied Due To Totality of Circumstances	1798.130 1798.185, 1798.81.5
§ 7022	Requests to Delete.	Consumer	DISCOVER CONFIRMATION METHOD	No Confirmation of Delete	1798.105, 1798.130 and 1798.185
§ 7060.	General Rules Regarding Verification.	Consumer	DISCOVER REASONABLE VERIFICATION	Compliant Verification Procedures	1798.105, 1798.106, 1798.110,
§ 7022	Requests to Delete.	Consumer	DISCOVER THIRD PARTY COLLECTIONS	Unauthorized Use	1798.105, 1798.130 and 1798.185

§ 7060.	General Rules Regarding Verification.	Consumer	DISCOVER HIGH-RISK VERIFICATION	Match Identifying Information	1798.105, 1798.106, 1798.110,
§ 7002	the Collection and Use of Personal	Business	COMPLIANCE WITH CONSUMER'S	Inconsistent With Consumer's	1798.106, 1798.121, 1798.130,
§ 7024	Requests to Know.	Consumer	DISCOVER PI SOURCES	Incomplete Categories of Sources	1798.115, 1798.130, 1798.140,

Code Title	Subdivision	Description	Test Case Title	Test Case Pre-Reqs	Standard	Guidance
	(c) (1)	determining the method by which the	Matching Method		shall implement reasonable	Verification for Password-Protected
	(c) (2)	determining the method by which the	Sensitive PI Matching		shall implement reasonable	Verification for Password-Protected
	(c) (3)	(c) In determining the method by	Verification Process Requirements		shall implement reasonable	Verification for Password-Protected
Information Security Breaches	(a) (1) (2)	(a) (1) Any consumer whose	Implement and Maintain Reasonable			
	(c) (1)	determining the method by which the	Matching Method		shall implement reasonable	Verification for Password-Protected
	(c) (2)	determining the method by which the	Sensitive PI Matching		shall implement reasonable	Verification for Password-Protected
	(c) (3)	(c) In determining the method by	Verification Process Requirements		shall implement reasonable	Verification for Password-Protected
Information Security Breaches	(a) (1) (2)	(a) (1) Any consumer whose	Implement and Maintain Reasonable			
	(b) (5)	purpose(s) for which the personal	Service Providers, Contractors,	i. List of Third Parties	i. Consumer's Reasonable Expectations	the consumer likely expects an online
	(c) (3)	another disclosed purpose is	Disclosed Purpose At Time of	Context; ii. Other Disclosed	Purpose listed in Civil Code section	strong link exists between the
	(a) (b) (c)	purpose of the Notice at Collection is to	Any Collection Notice	evidence of each step in the process;	the point of collection; ii. Categories	Definitions. (q) "Notice at Collection"
	(g) (1)	(g) Third Parties that Control the	Joint Collection Notice	of first-party origin page; ii. Screenshot	for all parties with a link to each party's	examples follow. (A) Business F
	(g) (2)	Parties that Control the Collection of	Transferred Collection Notice	of third-party privacy policy on first-party	i. conspicuous;	

	(e) (1) (I)	(e) The privacy policy shall include the	Third Parties PI Was Disclosed To		Definitions. (f) "Categories of third parties"	
	(e) (1) (K)	(e) The privacy policy shall include the	Business or Commercial Purpose For		Definitions. (f) "Categories of third parties"	
	(e) (3) (D)	(e) The privacy policy shall include the	Disclosure of Sensitive PI For Other			
	(e) (3) (F)	(e) The privacy policy shall include the	How an Opt-out Preference Signal Will Be			
	(c)	shall consider the methods by which it	Execute Request Methods		Requirements for Methods for Submitting	5) Illustrative examples follow
	(d)	may use a two-step process for online	Delete Request Methods		section 7004	a delete request from being treated
	[none]	[none]	Document Undisclosed PI			
		process the request as a request to	Erroneous Treatment of Request			
	(k)	(k)Whether a business, service	Third Party Compliance			business, service provider, or
	(a)	(a) The unauthorized use or	Necessary to Perform or Provide		Definitions. (aa) "Request to limit"	
	(d)	(d) The business and the platform,	Repurposed Use			
	(b) (3)	(3) Notifying all third parties to whom the	Third Party Shared Delete			
		process the request as a request to	Erroneous Treatment of Request			
	(d)	authorized agent shall not use a	Prohibited Use			

	(a) (5)	provider or contractor shall not	Other Purposes			examples follow. (A) An email
	(d)	(d) Information maintained for	Non-Compliant Record Sharing			
Information Security Breaches	(a) (1) (2)	(a) (1) Any consumer whose	Implement and Maintain Reasonable			
	(m) (2)	(m) The purposes for which a	Security Incidents			
	(b)	(b) If a business suspects	Malicious Activity			
	(a)	business maintains a password-	Reauthentication Verification Method		i. section 7060	
	(a) (4)	provider or contractor shall not	Security			examples follow. (A) An email
	(c) (1)	determining the method by which the	Matching Method		shall implement reasonable	Verification for Password-Protected

	(c) (1)	business collects consumers'	Passive Collection Notice	capture; ii. Tracking pixels, fonts,		
	(c) (2)	business collects consumers'	Online Collection Notice	Safari, Firefox, Edge, Bravo browsers;	i. conspicuous; ii. Close proximity	
	(c) (3)	business collects personal	Mobile Collection Notice	Samsung, AppleStore, GooglePlay;		
	(c) (4)	business collects consumers'	In-Person Collection Notice	Location; ii. Printed forms that		
	(c) (4)	business collects consumers'	Mail Collection Notice	Mail with printed form to submit PI;		

	[none]	[none]	Email Collection Notice	i. email with tracking URLs	[none]	
	(c) (5)	(5) When a business collects personal	Telephone Collection Notice	Contemporaneous Notes; ii. Telephone	i. Oral Notice	
	[none]	[none]	IoT Collection Notice	without website / landing page		
	(a)	(a) All individuals responsible for	Trained Staff			
	(b)	(b) A business that knows or reasonably	Special Requirements			
	(a)	(a) All individuals responsible for	Trained Staff			
	(e) (3) (J)	(e) The privacy policy shall include the	Concerns Contact Method			enforced by OAG; ii. Often the

	(a)	(a) A business shall maintain records of	Records Integrity		retained at least 24 months	
	(a)	(a) A business shall maintain records of	Request-Response Categories			
	(a)	(a) A business shall maintain records of	Deidentification, Encryption, Access			
	(b)	(b) The records may be maintained in	Record-keeping Sources		for required fields, not for the sources	
	(k) (6)	(k) In responding to a verified	Response Disclosed For Business			





	(e) (3) (E)	(e) The privacy policy shall include the	Verification Methods for CCPA Requests			
--	-------------------	--	--	--	--	--

	(c)	(c) A business shall establish, document, and comply with a	Guardian Opt-in Identity Verification	less than 13 years old AND Legal	(a) (2)	
	(a)	(a) For requests that seek the	Required For Specific Pieces of PI		Definitions. (z) "Request to know" means	
	(a)	(a) For requests that seek the	Required For Specific Pieces of PI		Definitions. (z) "Request to know" means	
	(b)	(b) For requests that seek the	Required For Categories of PI			
	(b)	(b) For requests that seek the	Identity Proof Required For ategories of PI			
	(a)	requests to correct, if a business	Identity Proof Required		Definitions. (x) "Request to correct"	General Rules Regarding Verification.
	(a)	requests to correct, if a business	Identity Proof Required		Definitions. (x) "Request to correct"	General Rules Regarding Verification.
	(a)	(a) When a consumer uses an authorized	Agent Authorization Proof		Definitions. (d) "Authorized agent" means	
	(d)	authorized agent shall not use a	Prohibited Use			

	(a)	shall establish, document, and comply with a	Method For Verifying		i. reasonable	Definitions. (mm) "Verify" means to
	(c) (1)	determining the method by which the	Matching Method		shall implement reasonable	Verification for Password-Protected
	(c) (2)	determining the method by which the	Sensitive PI Matching		shall implement reasonable	Verification for Password-Protected
	(h)	(h) For requests to correct, the	Inaccurate Verification Data			
	(a)	business maintains a password-	Reauthentication Verification Method		i. section 7060	
	(b)	(b) A business's compliance	Request to Know Categories			
	(c)	(c) A business's compliance with a request	Request to Know Specific PI		high degree of certainty may include	Definitions. (ii) "Signed" means that

	(m) (3)	(m) The purposes for which a	Malicious Actions			
--	-------------	------------------------------	-------------------	--	--	--

Information Security Breaches	(a) (1) (2)	(a) (1) Any consumer whose	Implement and Maintain Reasonable			

--	--	--	--	--	--	--

	(m) (4)	(m) The purposes for which a	Physical Safety			
--	-------------	------------------------------	-----------------	--	--	--

Information Security Breaches	(a) (1) (2)	(a) (1) Any consumer whose	Implement and Maintain Reasonable			

		policy shall include the following	Description of Information Practices		Comprehensive; ii. Online and	Definitions. (o) "Information Practices"
Information Security Breaches	(e) (1) (a) (1) (2)	(a) (1) Any consumer whose	Implement and Maintain Reasonable			

	(c) (2)	another disclosed purpose is	Other Disclosed Purpose	Context; ii. Other Disclosed	Definitions. (k) "Employment-related	application requires a Job Applicant to
	(f)	shall not collect categories of	Undisclosed Collection and Use	Provided by Consumer; ii. PI	i. section 7012	intends to collect additional
	[none]	[none]	Document Undisclosed PI			
	(k) (1)	(k) In responding to a verified	Request Response Categories			

	(a)	(a) All individuals responsible for	Trained Staff			
	(a)	(a) All individuals responsible for	Trained Staff			
	(e) (3) (J)	(e) The privacy policy shall include the	Concerns Contact Method			enforced by OAG; ii. Often the

	(b)	that controls the collection of a	No Notice at Collection	i. business	i. section 7012	[None]
	(k) (6)	(k) In responding to a verified	Response Disclosed For Business			
	(b)	(b) In determining the accuracy	Consumer Data Quality Baseline		Definitions. (x) "Request to correct"	
	(b)	(b) In determining the accuracy	Business Data Quality Baseline		Definitions. (x) "Request to correct"	
	(c) (1)	determining the method by which the	Matching Method		shall implement reasonable	Verification for Password-Protected
	(e) (3) (J)	(e) The privacy policy shall include the	Concerns Contact Method			enforced by OAG; ii. Often the
	(a) (2)	(a) A business that knows or reasonably	Data Reporting Disclosure			
	(e) (5)	policy shall include the following	Privacy Policy Data Reporting Requirements		(a) A business that knows or reasonably	



	(a)	(a) Process for Opting-In to Sale or Sharing of Personal Information	Guardian Opt-in Consent	less than 13 years old AND Legal	Definitions. (bb) "Request to opt-in to	Definitions. (h) "COPPA" means the
	(a)	(a) A business that has actual knowledge that it sells or	Guardian Opt-in Consent	less than 16 years old AND at least 13	i. section 7028	
	(a)	(a) A business subject to sections 7070 and/or 7071	Guardian Opt-In Process	i. Privacy Policy	i. sections 7070 and/or 7071;	
	(a)	(a) The purpose of the Notice of Right to Opt-out of	Right to Opt-out Notice	of Opt-out; ii. ACK or screenshot of	i. immediate effectuation	Definitions. (s) "Notice of Right to Opt-
	(f) (2)	shall include the following in its Notice of	Right to Limit Notice Instructions		section 7027, subsection (b)(1)	
	(a)	(a) The purpose of the Alternative	Alternative Opt-out Method		Definitions. (b) "Alternative Opt-Out Link"	
	(e) (3) (A)	(e) The privacy policy shall include the	Explanation of CCPA Request Methods			
		process the request as a request to	Erroneous Treatment of Request			
		process the request as a request to	Erroneous Treatment of Request			
		process the request as a request to	Erroneous Treatment of Request			
		process the request as a request to	Erroneous Treatment of Request			
	(d)	(d) A business's compliance	Unauthorized Deletion or Correction Risk			examples follow: (1) Example 1:
	(a)	(a) In accordance with Civil Code	Proportionate Collection or Purpose	disclosed purpose; ii. PI collection	i. section 1798.100, subsection (c)	necessary and proportionate to achieve the
	(a)	(a) The unauthorized use or	Necessary to Perform or Provide		Definitions. (aa) "Request to limit"	

	(m) (1)	(m) The purposes for which a	Perform Services Or Provide Goods			
	(a) (3)	(a) A service provider or contractor	Quality of Service			examples follow. (A) An email
	(c)	provider or contractor receives a	Direct Requests From Consumers			
	(b) (1)	purpose(s) for which the personal	Between Consumer and Business	i. Describe relationship	i. Consumer's Reasonable Expectations	the consumer is intentionally interacting
	(b) (2)	purpose(s) for which the personal	Type, Nature, and Amount of PI	nature, and amount of PI collected or	i. Consumer's Reasonable Expectations	a business's mobile communicatio
	(j)	(j) Upon request, a business shall	Request specific PI			
	(e)	as required by subsection (b), a business is	Requirement to Retain PI			
	(k) (3)	(k) In responding to a verified	Response Purpose For Collection Or			
	(e)	shall obtain the consumer's	Consent For Other Purposes	Disclosed Purposes; ii. List of	i. section 7004	business cannot comply simply by a
	(a)	business that must comply with the CCPA	No Privacy Policy	locations where privacy policies are	i. section 7011	i. Never enforced by OAG
	(a)	(a) The purpose of the privacy policy	Privacy Policy Purpose		Definitions. (o) "Information Practices"	

Information Security Breaches	(a) (1) (2)	(a) (1) Any consumer whose	Implement and Maintain Reasonable			
-------------------------------	-------------------	----------------------------	-----------------------------------	--	--	--

	(c) (3)	(c) In determining the method by	Verification Process Requirements		shall implement reasonable	Verification for Password-Protected
	(a) (1)	(a) A business that knows or reasonably	Data Broker Registry			



Information Security Breaches	(a) (1) (2)	(a) (1) Any consumer whose	Implement and Maintain Reasonable			
	(a) (1)	provider or contractor shall not	Business Purpose(s) and Service(s)			examples follow. (A) An email
	(a) (2)	provider or contractor shall not	Subcontracting			examples follow. (A) An email



Information Security Breaches	(a) (1) (2)	(a) (1) Any consumer whose	Implement and Maintain Reasonable			
-------------------------------	-------------------	----------------------------	-----------------------------------	--	--	--

Information Security Breaches	(a) (1) (2)	(a) (1) Any consumer whose	Implement and Maintain Reasonable			
	(m) (7)	(m) The purposes for which a	Quality of Service			

	(b)	(b) If a business suspects	Malicious Activity			
Information Security Breaches	(a) (1) (2)	(a) (1) Any consumer whose	Implement and Maintain Reasonable			
	(e) (4)	of time the business intends to	PI Category Retention Time	i. Collection Notice and/or Privacy Policy	there is no standard for allowable	

	(b) (2)	(2) Notifying the business's service	Third Party Delete		provider or contractor shall, with	
	(e)	as required by subsection (b), a business is	Requirement to Retain PI			
	(b)	(b) In determining the accuracy	Consumer Data Quality Baseline		Definitions. (x) "Request to correct"	
	(b)	(b) In determining the accuracy	Business Data Quality Baseline		Definitions. (x) "Request to correct"	
	(b) (1)	(b) A business shall comply with a	Delete Fulfillment		Definitions. (y) "Request to delete" means	
	(a)	shall establish, document, and comply with a	Method For Verifying		i. reasonable	Definitions. (mm) "Verify" means to
	(b) (2)	(2) Notifying the business's service	Third Party Delete		provider or contractor shall, with	

	(c) (1)	determining the method by which the	Matching Method		shall implement reasonable	Verification for Password-Protected
	(b) (3)	purpose(s) for which the personal	Source of PI	Request Response includes Third	i. Consumer's Reasonable Expectations	the consumer is providing their personal
	(k) (2)	responding to a verified request to	Response Source Categories			

Exceptions	Exemptions	Remediation	Remediation Example	Remediation Tools	Complaint	Defense
Verification for Password-Protected		Update Verification Procedures			Match Identifying Information	
Verification for Password-Protected		Update Verification Procedures			PI Not Necessary for Verification	
Verification for Password-Protected		Update Verification Procedures			Process Not Stringent For High Risk PI	
		Security Controls For Processing All			Implement and Maintain Reasonable	
Verification for Password-Protected		Update Verification Procedures			Match Identifying Information	
Verification for Password-Protected		Update Verification Procedures			PI Not Necessary for Verification	
Verification for Password-Protected		Update Verification Procedures			Process Not Stringent For High Risk PI	
		Security Controls For Processing All			Implement and Maintain Reasonable	
		Disclosure and/or Contracts With			Inconsistent With Consumer's	Expectations Cannot Be Defined By
		Purpose of Collection or Processing			Purpose Incompatible With Context	Expectations Cannot Be Defined By
No Direct Control Exception	Registered DataBroker Exemption	Update Notices To Consumers			standard(s) ii. Dark patterns	cookie consents"; ii. Limited
		Update Required Notice			Compliant Notice of Collection	
		Update Required Notice			Compliant Notice of Collection	

		Update Privacy Policy			Compliant Disclosure of Categories of	
section 7027, subsection (m)		Update Privacy Policy			Compliant Disclosure of Specific	
		Update Privacy Policy			Compliant Disclosure of Use or	
		Update Privacy Policy			of How an Opt-out Preference Signal Will Be	
		Reform Requests Processes			Execute Request Methods	
		Update Request Methods			Erroneous Treatment of Requests	
		Update Privacy Policy			Undisclosed Collection	
		Security Controls For Processing All			Treatment of Requests to Know	
					Information Overridden By Inaccurate	
purposes for which a business may		Opt-in / Consent Obtained			No Meaningful Control	
		Opt-in / Consent Obtained			Unauthorized Use	
		Process For Notification Or Confirmation			Notification Failure	
		Security Controls For Processing All			Treatment of Requests to Delete	
		Opt-in / Consent Obtained			Prohibited Use of Consumer's PI	

		Opt-in / Consent Obtained			Non- Compliant Use of PI	
		Security Controls For Processing All			Request Records Improperly	
		Security Controls For Processing All			Implement and Maintain Reasonable	
		Update Purpose of Data Asset			Exception For Posting Notice To Limit	
		Process For Denial of Requests			Malicious Activity Suspected	
		Update Verification Procedures			Re- authentication Not Required	
		Opt-in / Consent Obtained			Non- Compliant Use of PI	
Verification for Password- Protected		Update Verification Procedures			Match Identifying Information	



		Update Link to Notice at Collection			Compliant Link to Notice of Collection	
		Update Webform			Compliant Link to Notice of Collection	
		Update Link to Notice at Collection			Compliant Link to Notice of Collection	
		Implement In- Person Notice at Collection			Notices to Consumers	
		Implement In- Person Notice at Collection			Notices to Consumers	

		Update Notices To Consumers			Notices to Consumers	
		Implement Oral Notice at Collection			Notices to Consumers	
		Update Notices To Consumers			Notices to Consumers	
		Update Staff Training			Staff not informed of all requirements	
		Update Staff Training			Staff unaware of sale / share	
		Update Staff Training			Staff not informed of all requirements	
		Update Privacy Policy			or Concerns Contact Method	"Not required to respond"

		Reform Requests Processes			No Records of Consumer Requests	
		Response Mechanisms to CCPA			Consumer Requests Not Maintained	
		Security Controls For Processing All			Security Not Maintained For Consumer	
		Reform Requests Processes			Records of Consumer Requests	
		Which Data Assets Are Disclosed To			Categories of PI Disclosed for Business	





		Update Privacy Policy			of Verification Methods for CCPA Requests	
--	--	-----------------------	--	--	---	--

		Guardian Verification Method			Compliant Guardian Verification	
		Update Verification Procedures			Compliant Verification Procedures	
		Update Verification Procedures			Non-Verifiable Requests	
		Update Verification Procedures			Compliant Verification Procedures	
		Reform Requests Processes			Non-Verifiable Requests	
		Update Verification Procedures			Compliant Verification Procedures	
		Reform Requests Processes			Non-Verifiable Requests	
(a) does not apply when a consumer has		Update Verification Procedures			No Agent Signed Permission	
		Opt-in / Consent Obtained			Prohibited Use of Consumer's PI	

business maintains consumer		Update Verification Procedures			Compliant Verification Procedures	
Verification for Password-Protected		Update Verification Procedures			Match Identifying Information	
Verification for Password-Protected		Update Verification Procedures			PI Not Necessary for Verification	
		Update Verification Procedures			Inaccurate Data Used For Verification	
		Update Verification Procedures			Re-authentication Not Required	
		Update Verification Procedures			Unreliable Degree of Certainty	
shall deny a request to know specific		Update Verification Procedures			Unreliable High Degree of Certainty	

		Update Purpose of Data Asset			Exception For Posting Notice To Limit	
--	--	------------------------------	--	--	---------------------------------------	--

		Security Controls For Processing All			Implement and Maintain Reasonable	

--	--	--	--	--	--	--

		Update Purpose of Data Asset			Exception For Posting Notice To Limit	
--	--	------------------------------	--	--	---------------------------------------	--

		Security Controls For Processing All			Implement and Maintain Reasonable	



		Update Privacy Policy			Compliant Description of Information	
		Security Controls For Processing All			Implement and Maintain Reasonable	

		Purpose of Collection or Processing			Purpose Incompatible With Context	Expectations Cannot Be Defined By
		at Collection With Undisclosed PI			Undisclosed Collection and Use	
		Update Privacy Policy			Undisclosed Collection	
		Maintain Data Asset Inventory			Incomplete Categories of PI Collected	

		Update Staff Training			Staff not informed of all requirements	
		Update Staff Training			Staff not informed of all requirements	
		Update Privacy Policy			or Concerns Contact Method	"Not required to respond"

i. Neither collects nor controls PI	Revenue Threshold; ii. Sale or	Provide Notices To Consumers			No Notice at Collection	i. Neither collects nor controls PI
		Which Data Assets Are Disclosed To			Categories of PI Disclosed for Business	
		Process For Denial of Requests			Denied Due To Totality of Circumstances	"more likely than not accurate"
		Process For Denial of Requests			Denied Due To Totality of Circumstances	correct what we cannot find"
Verification for Password-Protected		Update Verification Procedures			Match Identifying Information	
		Update Privacy Policy			or Concerns Contact Method	"Not required to respond"
					Metrics Not Disclosed By July 1	
		Update Privacy Policy			No Required Data Reporting	



		Add Required Links for Minors			No Required Links for Minors	
		Add Required Links for Minors			No Required Links for Minors	
that exclusively targets offers		Add Required Links for Minors			Required Links for Minors	
		Provide Opt-out Notice			Missing Opt-out Notice	
that uses or discloses sensitive		Update Privacy Policy			No Limit Request Instructions	
		Update Privacy Policy			Missing Opt-out Notice	
		Update Privacy Policy			of CCPA Request Methods	
		Security Controls For Processing All			Treatment of Requests to Know	
		Security Controls For Processing All			Treatment of Requests to Opt-out	
		Security Controls For Processing All			Treatment of Requests to Limit	
		Security Controls For Processing All			Treatment of Requests to Delete	
		Process For Denial of Requests			Requires Reasonably High Degree of	
		Purpose of Collection or Processing			Unnecessary Collection or Purpose	"reasonably necessary and proportionate"
purposes for which a business may		Opt-in / Consent Obtained			No Meaningful Control	

		Update Purpose of Data Asset			Exception For Posting Notice To Limit	
		Opt-in / Consent Obtained			Non-Compliant Use of PI	
		Process For Denial of Requests			No Notification of Denial	
		Purpose of Collection or Processing			Inconsistent With Consumer's	Expectations Cannot Be Defined By
		Consumer's Expectations Based on Type,			Inconsistent With Consumer's	Expectations Cannot Be Defined By
		Process For Notification Or Confirmation			Confirmation Inaccurate Information	
		Process For Denial of Requests			Requests to Delete Denied	
		Purposes In Data Asset Inventory			Purpose of Collection or Sale	
providers who participate in HIEs provide a		Consumer Consent for each Disclosed			Consent Not Obtained For Each Purpose	General Consent Obtained
i. Internal Privacy Policies	Revenue Threshold; ii. Sale or	Post Privacy Policy			No Privacy Policy	policies are used for disclosing
		Update Privacy Policy			Non-Compliant Privacy Policy	



		Security Controls For Processing All			Implement and Maintain Reasonable	
--	--	--------------------------------------	--	--	-----------------------------------	--

		Security Controls For Processing All			Implement and Maintain Reasonable	
--	--	--------------------------------------	--	--	-----------------------------------	--

		Security Controls For Processing All			Implement and Maintain Reasonable	
		Update Purpose of Data Asset			Exception For Posting Notice To Limit	

		Process For Denial of Requests			Malicious Activity Suspected	
		Security Controls For Processing All			Implement and Maintain Reasonable	
possible, the criteria used to determine the		Update Retention Disclosures			Noncompliant Retention Disclosures	

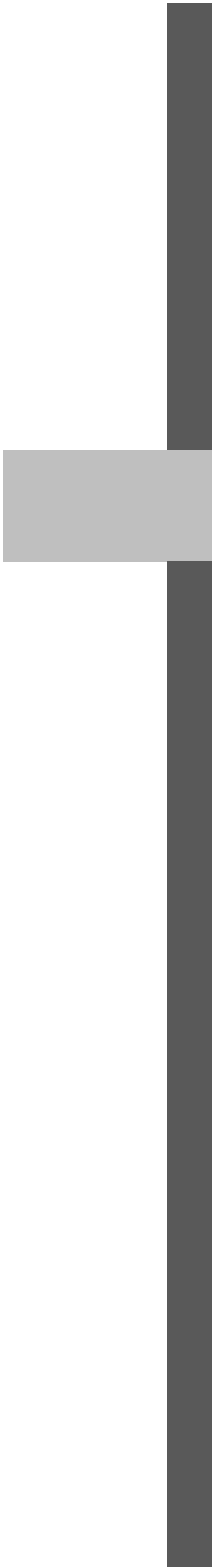
business, service provider, or		Opt-in / Consent Obtained			Unauthorized Use	
		Process For Denial of Requests			Requests to Delete Denied	
		Process For Denial of Requests			Denied Due To Totality of Circumstances	"more likely than not accurate"
		Process For Denial of Requests			Denied Due To Totality of Circumstances	correct what we cannot find"
		Process For Notification Or Confirmation			No Confirmation of Delete	
business maintains consumer		Update Verification Procedures			Compliant Verification Procedures	
business, service provider, or		Opt-in / Consent Obtained			Unauthorized Use	

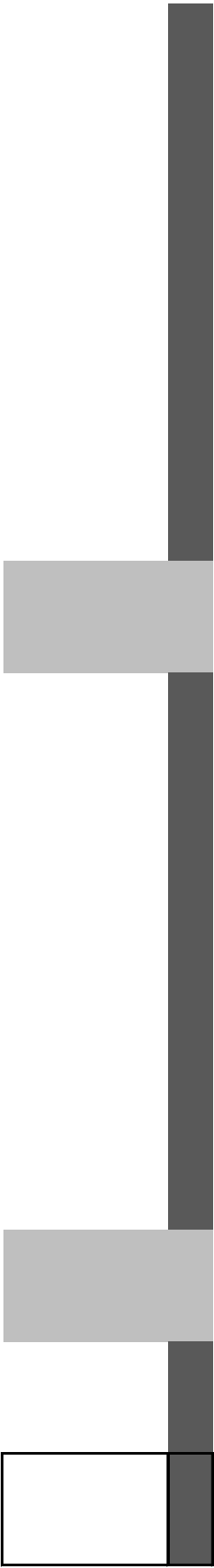
Verification for Password- Protected		Update Verification Procedures			Match Identifying Information	
		Reason PI Collected or Processed			Inconsistent With Consumer's	Expectations Cannot Be Defined By
		Sources In Data Asset Inventory			Incomplete Categories of Sources	

Counter Tests	
Information From Third Parties	
1) iapp to pearson for scheduling	
Visitor logs at offices, facilities	

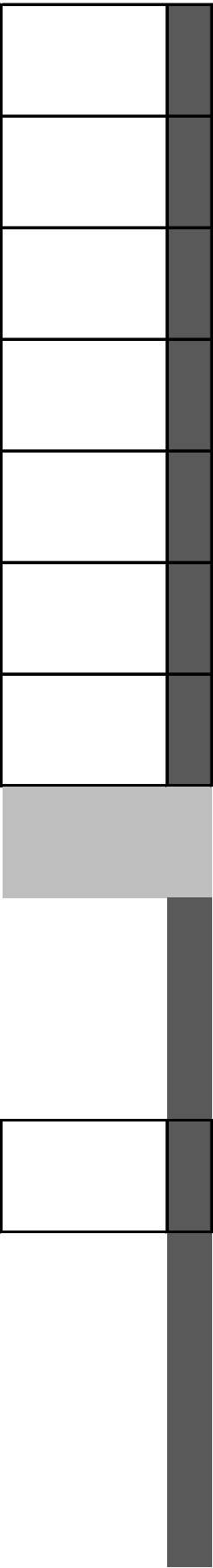
[illegible]

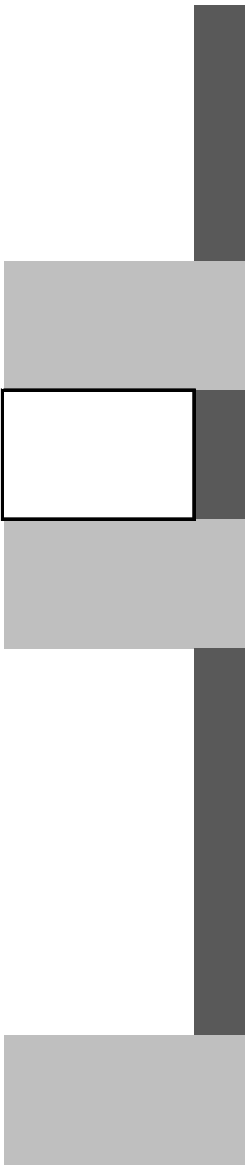
[illegible]

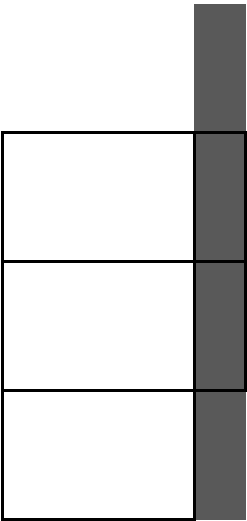
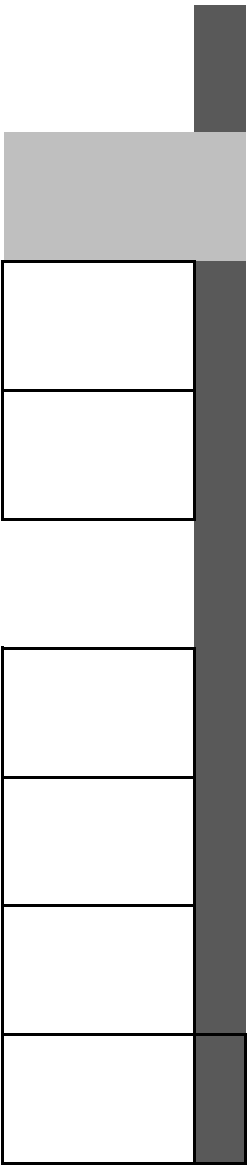




[illegible]



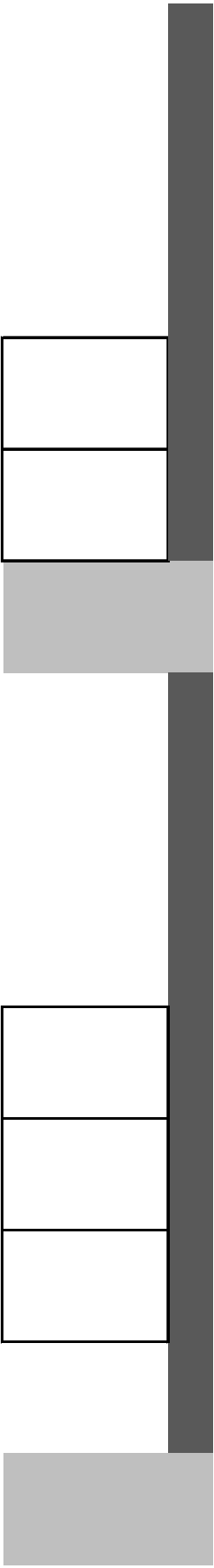


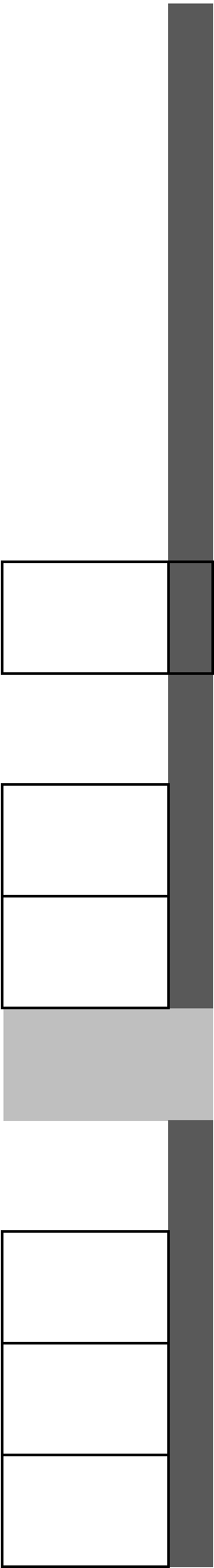


i. Unless it isn't searchable or accessible	
i. Unless it is searchable and accessible	

[illegible]

[illegible]





i. Unless it isn't searchable or accessible
i. Unless it is searchable and accessible
i. Request Information From PI Source

Commenter: Craig Erickson, a California Consumer residing in Alameda, CA

Contact: [REDACTED]

Date Submitted: 03/27/2023

**Craig Erickson's COMMENTS ON PROPOSED RULEMAKING
CYBERSECURITY AUDITS, RISK ASSESSMENTS, AND AUTOMATED DECISIONMAKING**

Background

As a California Consumer, I maintain a personal vendor risk program for testing businesses' compliance with the CCPA and governing use of my personal information. In November of 2020, I voted for Proposition 24, the California Privacy Rights Act of 2020 ("CPRA") because I share

"the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public".

Comment 1, Pursuant to Civil Code section 1798.185(a)(15)-(16):

I ask the Agency to consider all stakeholders when issuing regulations **1798.185(a)(15)-(16)**, instead of **only** requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to perform (B) and (A), because consumers and government agencies can also introduce significant risk by their actions or inaction even though they cannot be legally responsible for following the guidance issued by these regulations.

(B) Consumers should be allowed to submit to the California Privacy Protection Agency on an as-needed basis, their own risk assessment findings, compliance test results, or incident reports with respect to their processing of personal information, and that the Agency should help identify and weigh the benefits against potential risks, with the goal of educating the public about which processing activities and organizational entities are deemed "high-risk".

(A) Based on risk assessments (B) from businesses and consumers which are validated by the Agency, perform a cybersecurity audit on an annual basis, using the State of California's current process as a model, to ensure that audits are thorough and independent. This proposal is documented in Appendix A.

(a) The *non-exclusive* factors to be considered in determining when processing may result in significant risk to the security of personal information shall include *any one of the following factors*:

a) the size of the business; b) complexity of supply-chain dependencies; c) the nature of processing activities; d) scope in terms of company size; e) sensitivity of personal information; f) vulnerability of targeted populations; g) history of non-compliance, breaches, or unlawful practices; h) absence of, or lack of access to other suppliers providing critical services to consumers.

(16) Consider issuing regulations governing access and opt-out rights with respect to any, and all use of automated decisionmaking technology, because businesses aren't the only entities using it; government agencies use it in law enforcement; and consumers use it when transmitting opt-out preference signals or using authorized agents to send delete requests to businesses identified in email messages.

Comment 2, I. Cybersecurity Audits; Question 1 (a) (b) (c) (d) (e):

1.a. California State Laws and the California State Constitution require California State Agencies to have mandatory cybersecurity audits, and in some cases, Privacy Impact Assessments. These state agencies serve businesses and consumers. California already has an established Cybersecurity Program including Independent Security Audits for its agencies, which appears to meet the goals and requirements of Civil Code section 1798.185(a)(15)(A), with minimal modifications.

1.b. California's ISA process, documented in Appendix A, helps agencies comply with other state laws that currently have, or could benefit from, cybersecurity audit requirements. These laws, which are related to security and privacy risks of processing personal information, could be more effective by sharing information and costs from CCPA-mandated risk assessments and cybersecurity audits. These current and pending legislative bills are documented in Appendix B.

1.c. and 1.d. The gaps or weaknesses of any audit or certification is the level of acceptance or validation of the assessment. Obviously, Californians would not vote for mandatory risk assessments and cybersecurity audits if existing ones met the goals and requirements of laws like Civil Code section 1798.185(a)(15)(A). The lack of transparency about what standards and controls are tested, the process, the outcomes, and who this information applies to, greatly impacts consumers' trust in businesses and enforcement agencies. Laws are ineffective when perceived by businesses or consumers, as being unfairly enforced.

1.e. I recommend using a similar model to the existing ISA process within the State because the CPPA is a state agency, and the State uses NIST SP800-53r4 as its primary standard control framework, according to the Office of Information Security (OIS) in the State's Information Security Policy.

Comment 3, I. Cybersecurity Audits; Question 2 (a) (b) (c) (d) (e):

2.a. The Agency should consider in its regulations for CCPA's cybersecurity audits pursuant to Civ. Code § 1798.185(a)(15)(A) alignment with cybersecurity audits, assessments, evaluations, and best practices identified in intra-state, inter-state, and federal requirements and standards, and standards from the EU including the GDPR, the EDPB, and NIS 2.

2.b., 2.c. and 2.d. Current cybersecurity audits, assessments, evaluations, or best practices in the US include responding to self-assessment questionnaires from other businesses, and third-party certifications such as SOC2, PCI-DSS, HITRUST, FedRAMP, and ISO. Consumers do not have access to this information, which is both a gap and a weakness which impacts consumers and businesses by eroding public trust that laws are being fairly and effectively enforced.

Comment 4, I. Cybersecurity Audits; Question 2 (e), and Question 3:

2. e. The Agency should consider these cybersecurity audit models, assessments, evaluations, or best practices when drafting its regulations because, when aligned with common controls in other standard control frameworks, the compliance and audit process can facilitate greater acceptance and leverage information from existing best practices. However, due to the wide variety of interpretations and inconsistent audit execution, existing assessments should not be accepted in place of a state agency-initiated audit that sets the control standards and the audit methodology.

Comment 5, I. Cybersecurity Audits; Question 4, and Question 5:

4. and 5. Similar processes from other government agencies help to ensure that these audits, assessments, or evaluations are thorough and independent, by comparing existing cases which are also relevant to the CCPA. The Agency should also consider publishing a “Communicating our Regulatory and Enforcement Activity Policy”, as the ICO does in the UK because:

Transparency is often mentioned as a key factor in building and maintaining trust among businesses and consumers. It’s also a preventative control mechanism – when businesses and consumers know what enforcement actions are taken, why, and on whom can invoke a sense of fairness, which research has shown tends to encourage compliance.

This topic about transparency relates directly to the Agency’s question regarding the scope of cybersecurity audits:

The scope should be dependent upon the classification of business practices and business entities whose management history has been deemed “high-risk” *and should not be concealed from the public.*

For example, the Agency should also consider “trust services” (NIS 2) that are essential to identity verification, or data brokers that operate CDNs or other services that must be resilient for serving the public interest.

Article 2 of The Network and Information Security (NIS 2) Directive, the EU-wide legislation on cybersecurity states: “2. *Regardless of their size, this Directive also applies to entities ... where:*

(a) services are provided by:

(i) providers of public electronic communications networks or of publicly available electronic communications services;

(ii) trust service providers;

(iii) top-level domain name registries and domain name system service providers;

(b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;

(c) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;

(d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;

(e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State;”

Comment 6, II. Risk Assessments; Question 1 (a), and Question 5:

The CCPA directs the Agency to issue regulations requiring businesses “whose processing of consumers’ personal information presents significant risk to consumers’ privacy or security” to regularly submit to the Agency a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits and risks of such processing.

a. The risk assessment itself should determine the necessary scope and submission process for selecting which businesses should be subject to mandated cybersecurity audits. Existing state, federal, and

international laws, third-party compliance audits employ a similar approach by using self-assessment questionnaires and other tools to evaluate an entity's legal requirements and determine if the inherent risk justifies additional scrutiny or controls, even for businesses that make less than \$25 million in annual gross revenue or enjoy other exemptions.

Comment 7, Pursuant to II. Risk Assessments; Question 1 (b) (c) (d) and (e):

Businesses evaluate other businesses through vendor risk management practices, including the use of "ratings" companies and databases such as MITRE's CVE and US-CERT, to identify product vulnerabilities and data breach histories which can also assist with the CCPA's risk-assessments requirements. The gaps or weaknesses of these risk assessments include lack of data quality standards in reporting and the lack of participation in sharing information about security and privacy incidents among businesses, consumers, and enforcement agencies. These weaknesses impact consumers by depriving them of critical information they need to make risk-based decisions about their vendors.

Not-for-profit Organizations, with few exceptions, are currently exempt from complying with the CCPA. According to page 2 of *"Findings from ICO information risk reviews at eight charities", April 2018*, charitable organizations can be large or small, and engage in very high-risk processing. Under the section entitled, *"Typical processing of personal data by charities"*, the ICO writes, *"The charities involved process a limited amount of sensitive personal data as defined by the DPA, including staff sickness records and sometimes donor or service user information relating to health and receipt of benefits. Some charities also process information relating to children and vulnerable people."*

This is why I propose the Agency send a risk assessment to every organization registered with the California Secretary of State, not only for the purpose of determining inherent risk but also for increasing the public's awareness of these new regulations and the standards used in these assessments.

Comment 8, Pursuant to II. Risk Assessments; Question 2:

I cannot predict what harms, if any, particular individuals or communities are likely to experience from a business's processing of personal information.

Identifying what processing of personal information is likely to be harmful to these individuals or communities, could be discovered through robust reporting process, which would accept input from individual consumers and/or consumer advocacy organizations such as the Identity Theft Resource Center. I recommend not codifying in law or regulations assumptions or current trends which may not hold true in the future, in favor of capturing incident-reporting metrics instead.

Comment 6, Pursuant to II. Risk Assessments; Question 3 (a):

a. To determine what processing of personal information presents significant risk to consumers' privacy or security under Civil Code § 1798.185(a)(15), the Agency should (a) follow an approach similar to those outlined in the European Data Protection Board's Guidelines on Data Protection Impact Assessment.

Comment 9, Pursuant to II. Risk Assessments; Question 3 (b) and (e):

b. e. The agency should consider the PIA Methodology from CNIL for Privacy Impact Assessments because of its widespread adoption and online tools for conducting them. The Agency should also

consider the ISO/IEC JTC 1/SC 27/WG 5 N1320, WG 5 Standing Document 4 (SD4) – Standards Privacy Assessment (SPA). This document determines whether to apply the SPA process by asking three questions concerning the Standard or Specification Under Review (SUR):

- 1. Will the SUR involve technology that will process PII, or will it involve technology that could link information to an identifiable individual?*
- 2. If the SUR will not process PII or involve technology that could link information to an identifiable individual, will it generate PII?*
- 3. If the SUR will not generate PII, will it involve technology that will be used in a network device by an individual?*

If the answer to any of these questions is affirmative, then the SPA process should be applied to the SUR.

The beauty of this approach lies in its granularity, as applied to an entire product offering or introducing a new feature.

In addition, the ISO/IEC JTC 1/SC 27/WG 5 N1320, WG 5 Standing Document 4 (SD4) – Standards Privacy Assessment (SPA) uses this criteria for defining (e) What processing, if any, does not present significant risk to consumers' privacy or security:

"This standard [or specification] does not define technology that will process Personally Identifiable Information (PII), nor will it create any link to PII. Furthermore, the standard [or specification] does not define technology that will be deployed in a network device and used by an individual."

Comment 10, Pursuant to II. Risk Assessments; Question 3 (c):

The risk assessment should be used initially to determine what personal information is processed by an entity, and what their legal obligations are in complying with the CCPA, so that all stakeholders including businesses, consumers, and the Agency can judge for themselves if a cybersecurity audit should be required based on the design of appropriate controls. To protect trade secrets and security measures, only the resulting status should be reported for each entity when or if the entity's status is queried by users through an online tool provided by the CPPA.

Comment 11, Pursuant to II. Risk Assessments; Question 4 (a) (b), Question 6 (a) (b):

The minimum content required in risk assessments should be based on a subset of the most fundamental controls in NIST SP 800-53 r5 which are directly applicable to the CCPA Regulations, and can be mapped to controls in other frameworks such as NIST Cybersecurity Framework, NIST Privacy Framework, and the NIST Framework for Improving Critical Infrastructure, Center for Internet Security Controls, OWASP, and ISO.

As a theoretical construct, I have proposed in Appendix C, a subset of selected NIST controls which provide acceptable standards for cybersecurity and information risk practices that are necessary for complying with the CCPA Regulations.

(a) The GDPR and the Colorado Privacy Act are laws which are subject to change, making these a poor choice for the CCPA's risk assessments. A better choice would be to base risk assessments on standard, mature control frameworks like NIST, which is a commonly used by state and federal government agencies and all companies that do business with these agencies.

(b) Additional content is not required in risk assessments for processing that involves automated decisionmaking, including profiling because several controls included in my proposed NIST subset covers underlying dependencies like data quality and provenance, which are marked with an asterisk in Appendix C. Additional content may be required for mandated cybersecurity audits according to relevant risk factors.

Comment 12, Pursuant to II. Risk Assessments; Question 6 (a):

Businesses should only submit summary risk assessments formatted as a self-assessment questionnaire issued by the Agency, for the purpose of identifying risk factors ascribed to their company.

The Agency should not accept any other risk assessment conducted by the business because most other assessments will likely be outdated and not aligned with CCPA standards which are not yet defined.

These summaries should include a relevant subset of controls based on the NIST standard, similar to my Comment 11, which is documented in Appendix C. They should be submitted at least once annually, or within 90 days of a change in ownership.

Comment 13, Pursuant to II. Risk Assessments; Question 6 (b):

Businesses should designate a company officer that attests to the completeness, accuracy, *and currency* of risk assessment summaries, signed by the designated officer under penalty of perjury, like NIS 2 attestations in the EU, or Sarbanes Oxley in the US.

Combined with other proposals I've made in these comments, these summaries can be verified or refuted by incident reporting and complaints from consumers and other enforcement agencies.

Comment 14, Pursuant to II. Risk Assessments; Question 7:

All organizational entities registered with the California Secretary of State should be required to submit an initial risk assessment, which consists of no more than 100 self-assessment questions designed to identify high-risk processing and high-risk entities. These self-assessment questions are provided alongside the NIST controls I mapped to CCPA Regulations in Appendix C.

Comment 15, Pursuant to III. Automated Decisionmaking; Question 3 and Question 4:

Automated Decisionmaking, and any privacy risks associated with its use is not limited to CCPA-covered entities. Businesses which are exempt from the CCPA due to revenue thresholds have been reluctant to acknowledge their status, which effectively defrauds consumers regarding their CCPA rights according to controlled privacy experiments I have conducted over a two year period. I anticipate that business start-ups, who are eager to accelerate their market positions but less eager to implement privacy controls,

will claim to use AI, ML, Deep Neural Networks, etc. This is problematic because it could be nearly impossible for the Agency to determine who is using this technology, especially if companies make false representations or fall under the revenue threshold to avoid public embarrassment AND regulatory scrutiny.

Comment 16, Pursuant to III. Automated Decisionmaking; Question 3 (a) (d) (e) (f) and Question 5:

The Agency should consider all regulatory frameworks regarding the use of Artificial Intelligence (AI) because AI is the baseline technology underlying Automated Decisionmaking technologies. In particular, the Agency should consider:

- [Regulatory framework proposal on artificial intelligence | Shaping Europe's digital future.\(europa.eu\)](#)
- [explaining-decisions-made-with-artificial-intelligence-1-0.pdf](#) from the ICO
- [guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf](#) from the ICO

The Agency should also consider which AI systems the EU has identified as high-risk in its [Regulatory framework proposal on artificial intelligence](#), for inclusion in its criteria for defining high-risk factors:

- critical infrastructures (e.g. transport), that could put the life and health of citizens at risk;
- educational or vocational training, that may determine the access to education and professional course of someone's life (e.g. scoring of exams);
- safety components of products (e.g. AI application in robot-assisted surgery);
- employment, management of workers and access to self-employment (e.g. CV-sorting software for recruitment procedures);
- essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan);
- law enforcement that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence);
- migration, asylum and border control management (e.g. verification of authenticity of travel documents);
- administration of justice and democratic processes (e.g. applying the law to a concrete set of facts).

3. a. The Agency should use the ICO definition because it's the most concise:

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/>

For related terms, I also recommend

<https://publications.jrc.ec.europa.eu/repository/handle/JRC126426> which provides an "operational definition" consisting of an iterative method providing a concise taxonomy and list of keywords that characterise the core domains of the AI research field.

3. d. e. f. I recommend the Agency analyze how its own regulations on ADM would or would not apply to use cases in the EU, in light of the other conflicting US laws which could circumvent these protections. Existing GDPR case law, and associated privacy risks can be found in the following report, <https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf>.

For example, one consumer complaint I filed with the California Office of Attorney General applies directly to case law, *3.3 Credit Scoring*, which is justified on "contractual necessity" only if it relies on *relevant information*. I was denied access to my business banking account due to their use of an identity

provider which is a credit rating agency exempt from the CCPA, is a registered data broker, and also has a history of data breaches involving my compromised answers to security questions pertaining to another individual which I have no right to correct. In my case there was no automated decisionmaking using machine-learning or artificial intelligence algorithms: just me and my US passport standing in front of the bank branch manager who opened my account but could not authenticate me for online-banking because of a simple “automated process” consisting of a flawed lookup table maintained by an untrustworthy identity provider exempt from the CCPA.

Closing Comment

I want to thank the CPPA for providing this opportunity to participate in its rulemaking process through these public comments. For brevity’s sake, my Appendices are attached (if possible) to this submission, and published in my PrivacyPortfolio for peer review and collaboration with my professional colleagues.

Like laws and audits, my own assumptions and proposals need to be tested. Therefore, as a follow-up to this public comment I will be conducting these tests on my personal vendors and sending my findings to my vendors and the appropriate enforcement agencies and publishing the results of my experiment in my public data catalog.

As a California Consumer who exercises my own rights, I hope that the CPPA succeeds in providing independent assurance to all stakeholders that critical assets and citizen data are protected, which is the stated goal of Mandatory Independent Security Assessments of California Agencies.

Sincerely,

Craig Erickson, a California Consumer

From: Paul Lekas [REDACTED]
Sent: Monday, March 27, 2023 2:52 PM
To: Regulations
Subject: PR 02-2023
Attachments: SIIA CPRA Comment Letter - March 27.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Please find attached comments from the Software & Information Industry Association.

Many thanks for your assistance.

Paul Lekas



Paul Lekas

Senior Vice President, Head of Global Public Policy and Government Affairs
Software & Information Industry Association



[SIIA.net/policy](https://www.siiainc.org/policy)



March 27, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd
Sacramento, CA 95834
Via email: regulations@coppa.ca.gov

Re: PR 02-2023

Dear California Privacy Protection Agency:

The Software & Information Industry Association (SIIA) appreciates the opportunity to submit comments on proposed rulemaking around cybersecurity audits, risk assessments, and automated decisionmaking (ADM).

Background on SIIA

SIIA is the principal trade association for the software and digital information industries worldwide. Our members include over 450 companies, many based in California or primarily serving California residents. Our members include a range of broad and diverse digital content providers and users in specialized content industries, academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide, and companies specializing in data analytics and information services. On behalf of our members' wide interests and services, SIIA has long advocated for privacy protections.

I. Cybersecurity Audits

Question I.3. What would the benefits and drawbacks be for businesses and consumers if the Agency accepted cybersecurity audits that the business completed to comply with the laws identified in question 1, or if the Agency accepted any of the other cybersecurity audits, assessments, or evaluations identified in question 2? How would businesses demonstrate to the Agency that such cybersecurity audits, assessments, or evaluations comply with CCPA's cybersecurity audit requirements?

Response to Question I.3.

We recommend that the Agency allow businesses to comply with cybersecurity audit requirements by submitting self-certifications required by other laws and/or certifications that indicate compliance with industry standards. Cybersecurity audits are necessarily dependent on the nature of the business being audited, and it is important that the requirements are tailored to the types of information systems used by businesses in different sectors. There is a risk that audit requirements that are not sufficiently tailored



will create enormous compliance costs for businesses that are not tailored to achieve the desired objectives.

Question I.4. With respect to the laws, cybersecurity audits, assessments, or evaluations identified in response to questions 1 and/or 2, what processes help to ensure that these audits, assessments, or evaluations are thorough and independent? What else should the Agency consider to ensure that cybersecurity audits will be thorough and independent?

Response to Question I.4.

We recommend that the Agency allow businesses to rely on industry standards for cybersecurity audits, assessments, and evaluations. The Agency could promote best practices to ensure that audits are undertaken in an independent manner.

II. Risk Assessments

Question II.1. What laws or other requirements that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require risk assessments?

Response to Question II.1.

Privacy risk assessments have become increasingly common in jurisdictions with privacy laws and we encourage the Agency to align California's rules to those already in place that cover substantially similar data processing activities. We would recommend the Agency look to existing obligations under Virginia and Connecticut law as models for risk assessment requirements.¹ These jurisdictions have taken care to implement risk assessment requirements that meet the needs of consumers. We would urge caution in expanding the scope of risk assessments that businesses are already conducting unless there is a clear indication that those existing legal frameworks are inadequate to the purpose (and we are aware of none).

In addition, we recommend that risk assessments should be limited to processing of personal data that may have a legal or similarly significant effect on the individual consumer, such as processing that affects access to employment, educational opportunities, housing, and access to financial services. Expanding the scope of risk assessments to cover all processing of personal data will have significant downstream effects that would likely undermine consumer welfare and present compliance challenges to businesses that will especially hurt small- and medium-sized enterprises.

¹ <https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/>;
<https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF>.

While we recognize that the GDPR requires risk assessments, we would caution the Agency against adopting the GDPR approach as it currently stands. The GDPR requirements remain subject to development, compliance hurdles, and legal challenges, and are not adaptable to the U.S. landscape without careful finetuning. We recommend looking to other U.S. jurisdictions as guideposts on what may be appropriate for risk assessment requirements.

III. Automated Decisionmaking

Question III.1. What laws requiring access and/or opt-out rights in the context of automated decisionmaking currently apply to businesses or organizations (individually or as members of specific sectors)?

Response to Question III.1.

On November 8, 2021, SIIA provided the Agency with recommendations to guide rulemaking around ADM technology. We recommended that the Agency look to develop a risk-based framework for assessing such technology and focus on decisions that have a direct effect on the legal rights of the natural person subject to ADM (rather than the technology itself).² We continue to recommend this approach as the Agency develops regulations and supplement our prior recommendations as follows.

First, the Agency should develop a robust record regarding the benefits and myriad uses of ADM technologies for consumers. With respect to the internet ecosystem, ADM technologies are used in many ways to provide services that consumers rely on and expect. This includes using ADM technologies to personalize services, filter content (such as movie and music recommendations), improve the user experience, and assist organizations (including non-profits and government agencies) in finding the leads and information they need to execute their operations more effectively. The vast majority of these uses do not have legal or similarly significant effects on consumers and should be considered “low risk” and not subject to further regulation.

Second, the Agency should focus ADM rulemaking on high-risk decisions. We recommend that the Agency focus rulemaking on those decisions that have “legal or similarly significant effects” on individual consumers that are rendered through fully automated processes, and represent final decisions. As we noted, this approach would align with that of the GDPR, which in Article 22 protects consumers from decisions “based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”³

This approach would also align with laws enacted in other states. Among the laws that require access and/or opt-out rights in the context of automated decision-making are privacy laws enacted in other states. For example, state privacy laws in Colorado, Connecticut, and Virginia permit opt out for high-risk

² <https://www.sii.net/wp-content/uploads/2021/11/CPRA-Comments.pdf>

³ <https://gdpr-info.eu/art-22-gdpr/>

decisions – those that, in the case of Colorado and Virginia, have “legal or similarly significant effects” and, in Connecticut, are “solely” automated decisions.⁴ The approach taken in Virginia’s Consumer Data Protection Act (VCDPA) provides a good model for the Agency’s rulemaking. Under the VCDPA, “[d]ecisions that produce legal or similarly significant effects concerning a consumer” is defined to mean “a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.”⁵

We strongly recommend that California adopt the same approach, focusing on high-risk decisions rendered by ADM technologies – rather than the technologies themselves – and limit any rulemaking to those decisions reached through fully automated processes. Regulatory interoperability should be a guiding principle for the Agency. Consumers should have uniform expectations regarding access to important technologies and personalization, and a patchwork approach at the state level will invariably lead to increased compliance costs for businesses that will be passed on to consumers and create barriers for small- and medium-sized enterprises to provide services to California residents.

Question III.2. What other requirements, frameworks, and/or best practices that address access and/or opt-out rights in the context of automated decisionmaking are being implemented or used by businesses or organizations (individually or as members of specific sectors)?

Response to Question III.2.

Many of SIIA’s member companies have implemented robust frameworks to advance responsible AI in ways that mitigate potential unintended bias from algorithms and datasets, to advance transparency and explainability, and to mitigate safety, security, and reliability concerns. The need to augment these frameworks to provide for access and/or opt-out rights is minimal with respect to common, everyday uses of ADM – such as those ADM engines that generate recommendations for entertainment, provide automated spellcheck or word suggestions, and so on. These “low-risk ADM” technologies do not generate legal or similarly significant effects on consumers and do not require regulation. Regulating low-risk ADM technologies would have a negative impact on consumer welfare and also impede business innovation in ways that benefit consumers.

As noted above, we strongly recommend that the Agency focus any rulemaking on “high-risk ADM.” In advancing rules to ensure the safety, security, and unintended bias of high-risk ADM, we recommend that the Agency align any rulemaking to expert-driven efforts that are currently underway in the United States and internationally. The National Institute of Standards and Technology (NIST) in January 2023

⁴ https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_enr.pdf;
<https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF>;

<https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/>
⁵ <https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/>

released detailed guidance for assessing and mitigating risks associated with AI.⁶ The NIST AI Risk Management Framework is a good touchpoint for companies of all sizes to assess the risks associated with their use of ADM technologies. We recommend the Agency refer to the Framework as a key element of best practices for companies.

Question III.3. With respect to the laws and other requirements, frameworks, and/or best practices identified in response to questions 1 and 2: a. How is “automated decisionmaking technology” defined? Should the Agency adopt any of these definitions? Why, or why not? b. To what degree are these laws, other requirements, frameworks, or best practices aligned with the processes and goals articulated in Civ. Code § 1798.185(a)(16)? c. What processes have businesses or organizations implemented to comply with these laws, other requirements, frameworks, and/or best practices that could also assist with compliance with CCPA’s automated decisionmaking technology requirements? d. What gaps or weaknesses exist in these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? What is the impact of these gaps or weaknesses on consumers? e. What gaps or weaknesses exist in businesses or organizations’ compliance processes with these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? 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?

Response to Question III.3.

The Agency should endeavor to align its definition of key terms such as ADM and ADM technology with how those terms are understood and used in existing legal regimes. We recommend that California align its rules with those of the VDCPA and, further, define ADM as “final decisions made through fully automated processes that employ artificial intelligence technology and result in a legal or similarly significant effect concerning an individual.” We further recommend that California provide a clear definition of AI that aligns with the definition in the NIST AI Risk Management Framework.

Question III.4. How have businesses or organizations 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.

Response to Question III.4.

ADM technologies, including algorithms, have been used for decades by businesses in virtually every sector. These technologies provide ways to streamline operations, provide customized consumer experiences, improve products and services, and address consumer needs. Most uses of AI do not rise to

⁶ <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>



the level of high-risk as we describe in this submission and do not generate decisions that have legal or similarly significant effects on consumers.

Question III.7. How can access and opt-out rights with respect to businesses’ use of automated decisionmaking technology, including profiling, address algorithmic discrimination?

Response to Question III.7.

Algorithmic discrimination, which refers, under one definition, to “unjustified different treatment or impacts disfavoring people based on” their identification in various protected classes, as a result of automated systems,⁷ is a significant issue that must be addressed in the design, development, and deployment of ADM technologies. While we encourage the development of guardrails to protect against algorithmic discrimination, we would caution against using access and opt-out rights as appropriate tools to mitigate unintended bias in ADM systems. Instead, we would recommend that the Agency consider rules (such as safe harbors) that recognize the need to collect – rather than restrict collection of – data that relates to identification with protected classes, at least in the context of high-risk ADM, with the consumers’ consent. Having additional information about individuals may be critical to ensuring that datasets that inform ADM systems are sufficiently robust to anticipate and prevent unintended bias with respect to critical, high-risk decisions.

Question III.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?

Response to Question III.8.

Access and opt-out rights, if appropriate, should be tailored by sector and usage. Even with respect to high-risk ADM, the requirements will differ depending on context. We recommend deference to sector-specific approaches and frameworks, such as in the employment context, where there are already robust efforts underway to craft regulatory approaches.

In addition, there are situations in which access and/or opt-out rights would be harmful to the consumers who may benefit from ADM technology, even in high-risk scenarios. The Agency should take care to identify scenarios in which consumers could be harmed by having access or opt-out rights. In situations where ADM technologies are used to detect fraud, to facilitate medical care and emergency treatment, and others, permitting access or opt-out could undermine the efficacy and effectiveness of

⁷ <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf>



those ADM-driven services and cause harm to consumers who rely, directly or indirectly, on those services.

Question III.9. What pieces and/or types of information should be included in responses to access requests that provide meaningful information about the logic involved in automated decisionmaking processes and the description of the likely outcome of the process with respect to the consumer?

Response to Question III.9.

Regulations that require detailed information on specific decisions and the processes that lead to those decisions and processes run the risk of revealing trade secrets, which will have downstream effects on consumers and serve as a barrier to innovation. We believe the meaningful information can be provided to consumers and the broader public through general descriptions of how the high-risk ADM systems work and how those systems are used. We would caution the Agency against requiring detailed disclosures of algorithms or datasets and encourage the Agency to exempt disclosure of information that would reveal trade secrets or proprietary information.

Question III.10. To the extent not addressed in your responses to the questions above, what processes should be required for access and opt-out rights? Why?

Response to Question III.10.

We recommend that the Agency avoid creating new access or opt-out requirements without a fulsome understanding of the unintended consequences and, to the extent the Agency moves ahead with access or opt-out requirements, they should apply only to high-risk decisions. A broad approach to regulating in the ADM space will have a negative impact on consumer expectations and experiences, and could raise safety and security risks - including by limiting the ability of businesses to protect individuals from harmful content and cybersecurity risks.

In addition, we recommend that the Agency include critical exceptions to any access or opt-out rights to avoid consequences that may result from individuals (including bad actors) who seek to undermine processes that are in place to protect consumers. For example, access and opt-out rights could be abused by individuals to circumvent detection of fraudulent and malicious activity, undermine processes designed to buttress the safety and security of online platforms, assist government agencies in criminal, regulatory, and other matters, and more.

From: Hilary Cain [REDACTED]
Sent: Monday, March 27, 2023 2:51 PM
To: Regulations
Subject: PR 02-2023 (Preliminary Comments on Proposed Rulemaking - Alliance for Automotive Innovation)
Attachments: Auto Innovators Comments CPPA Invitation for Preliminary Comments FINAL 3.27.23.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good Afternoon –

Please find attached comments from the Alliance for Automotive Innovation in response to the Invitation for Preliminary Comments on Proposed Rulemaking (Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking).

Cheers,
Hilary

Hilary M. Cain
Vice President - Technology, Innovation, & Mobility Policy
O: [REDACTED]
Alliance for Automotive Innovation
1050 K Street, NW - Suite 650 Washington, DC 20001
autosinnovate.org - [twitter](https://twitter.com) - [linkedin](https://www.linkedin.com/company/allianceforautomotiveinnovation)



March 27, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

RE: Invitation for Preliminary Comments on Proposed Rulemaking

Dear Mr. Sabo:

The Alliance for Automotive Innovation (“Auto Innovators”) appreciates the opportunity to provide feedback to the California Privacy Protection Agency (“Agency”) in response to its invitation for preliminary comments on proposed rulemaking relating to automated decisionmaking, cybersecurity audits, and risk assessments.

Auto Innovators represents the manufacturers that produce most of the cars and light trucks sold in the U.S., original equipment suppliers, technology companies, and other value chain partners within the automotive ecosystem. Representing approximately 5 percent of the country’s GDP, responsible for supporting 10 million jobs, and driving \$1 trillion in annual economic activity, the automotive industry is the nation’s largest manufacturing sector.

As this rulemaking addresses novel topics, we respectfully request that the Agency provide sufficient lead time between the finalization of the regulations and the effective date of the regulations. Our member companies take their compliance obligations seriously and need adequate time to align their processes and mechanisms with any new regulatory requirements. To that end, we request that the regulations be finalized at least 12 months before any new obligations or responsibilities take effect. In addition, to ensure sufficient input from stakeholders, we also request that any draft regulations be released for a public comment period of at least 90 days.

Automated Decisionmaking

The term “automated decisionmaking” captures a range of use cases that do not have significant consumer privacy impacts. For example, automated driving systems and other advance vehicle safety systems incorporate artificial intelligence that makes automated decisions about what actions a vehicle will take to safely navigate the driving environment. Proving opt-out rights to disable or reduce the effectiveness of such systems could unintentionally and significantly implicate motor vehicle safety. For example, if a consumer opts out of automated decisionmaking that supports a crash avoidance system, the system may no longer help avoid or mitigate a crash’s impact on the driver, passengers, or other road users. The complexity of these vehicle systems also means that it is rarely possible to provide meaningful information to consumers about the logic involved in the decisionmaking process.

For this reason, we recommend that the Agency limit the scope of automated decisionmaking technology covered by the forthcoming regulations to “profiling.” If the Agency chooses to cover automated decisionmaking beyond profiling, the Agency should only include decisionmaking technology with significant economic or legal impact for a consumer, such as decisions about educational opportunities, employment, housing, or lending. This would be consistent with other legislation and the White House’s Blueprint for an AI Bill of Rights, which applies to automated systems that “have the potential to meaningfully impact individuals’ or communities’ exercise” of “civil rights, civil liberties, and privacy,” “equal opportunities,” or “access to critical resources or services.” At a minimum, such regulations should not apply to decisionmaking technology onboard vehicles that aids or automates driving functions.

To the maximum extent possible, the Agency should avoid requiring separate and distinct disclosures for various aspects of the CPRA. Any requirements to disclose that automated decisionmaking technologies are in use should be incorporated into the existing disclosure requirements in §1798.110.

Finally, we recommend that any right to request access to specific pieces of information related to automated decisionmaking technologies be limited to personal information. In other words, if the information is not stored by the business in a way 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, it should not be subject to an access request. This limitation would be aligned and entirely consistent with the right to access information in §1798.110 of the CPRA, as well as the general exceptions at 1798.145(j)(1) and (j)(3).

Cybersecurity Audits

We appreciate that the CPRA recognizes that not all processing of personal information presents a significant risk to consumers’ privacy or security and only requires an annual cybersecurity audit for the subset of processing activities that pose such a risk. The Agency should focus on processing that involves “sensitive personal information,” as defined in §1798.140(ae) when determining what processing presents a significant risk to consumers’ privacy and security.

The Agency should take a flexible approach with regards to the content of, and the process for conducting, such audits. Instead, businesses should be able to appropriately tailor their implementation of these audits to the size and complexity of their operations, including the nature and scope of processing activities and expectations of their customers. In addition, the Agency should expressly provide organizations the ability to leverage existing standards and best practices, such as the National Institute of Standards and Technology’s Cybersecurity Framework.

Finally, since an audit may reveal sensitive information about an organization’s cybersecurity posture which could result in increased risk of a cybersecurity attack if disclosed, the Agency should not require agencies to submit their audits to the Agency. If audits are submitted to the Agency, they should be treated as confidential information with sensitive technical information redacted, subject to applicable privileges and exempt from public disclosure under the Public Records Act.

Risk Assessments

Once again, we appreciate that the CPRA recognizes that not all processing of personal information presents a significant risk to consumers’ privacy or security and only requires regular risk assessment for the subset of processing activities that pose such a risk. In determining what processing

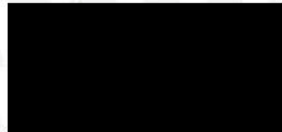
presents a significant risk to consumers' privacy and security, we reiterate our support for a focus on processing that involves "sensitive personal information" as defined in §1798.140(ae).

The Agency should refrain from setting out or establishing overly prescriptive requirements as to the content of or process for conducting such risk assessments. Instead, businesses should be provided flexibility in implementing these assessment requirements so that they can be appropriately tailored to their size and complexity, including the nature and scope of processing activities and expectations of customers.

We also discourage the Agency from specifying a regular cadence for risk assessments. If the Agency seeks to establish a trigger for risk assessments, the Agency should consider requiring businesses to update their risk assessment when there is a material change in their processing activities that is likely to have an impact on consumer privacy. Moreover, in determining when such risk assessments should be submitted to the Agency, we encourage the Agency to carefully balance the value of such submissions against the burden that such submissions may impose on businesses and the Agency. Rather than requiring every relevant business in California to periodically submit risk assessments to the Agency, the Agency should consider limiting risk assessment submissions to those requested by the Agency in conjunction with a relevant investigation or inquiry.

We appreciate the opportunity to provide input on this rulemaking and look forward to further engagement with the Agency on these important topics.

Sincerely,



Hilary M. Cain
Vice President
Technology, Innovation, & Mobility Policy

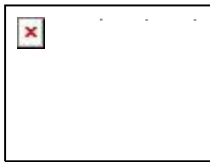
From: Keir Lamont [REDACTED]
Sent: Monday, March 27, 2023 2:53 PM
To: Regulations
Cc: Chloe Suzman
Subject: PR 02-2023 Future of Privacy Forum Comments
Attachments: [FPF] PR 02-2023 Comments (3.27.23).pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Please find attached the response of the Future of Privacy Forum regarding the California Privacy Protection Agency's Invitation for Preliminary Comments on Proposed Rulemaking on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking (PR 02-2023).

Cheers,
Keir

--



Keir Lamont
Director for U.S. Legislation
Future of Privacy Forum
[REDACTED] | www.fpf.org | 1350 Eye Street NW,
Suite 350, Washington, DC 20005



March 27, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

RE: Future of Privacy Forum Comments, PR 02-2023

Mr. Sabo and Members of the California Privacy Protection Agency,

Thank you for your ongoing work regarding the implementation of requirements for cybersecurity audits, risk assessments, and automated decisionmaking systems under the California Privacy Rights Act amendments to the California Consumer Privacy Act (CCPA).¹ In response to the Agency's request for comment on pre-rulemaking considerations, the Future of Privacy Forum (FPF) recommends that forthcoming regulations prioritize:

1. ensuring the protection of individual privacy interests and the effective exercise of new consumer rights under the CCPA;
2. maximizing clarity and ease of understanding for individuals who may be subject to automated decisions and organizations' compliance efforts, and;
3. promoting interoperability with emerging U.S. and global privacy frameworks where consistent with the above goals.

FPF is a non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies in the United States and globally. FPF seeks to support balanced, informed public policy and equip regulators with the resources and tools needed to craft effective regulation.² FPF welcomes this opportunity to respond to the California Privacy Protection Agency's invitation for preliminary comment.

1. Automated Decisionmaking Systems

Individuals and communities can benefit from automated decisionmaking (ADM) tools used in the provision of important services concerning education, employment, housing, credit, insurance, and government benefits. When the digital economy functions properly, all individuals, regardless of race, gender, or other protected class, are able to equally access the benefits of technology,

¹ California Privacy Protection Agency, "Invitation for Preliminary Comment on Proposed Rulemaking" (Feb. 10, 2023), https://cppa.ca.gov/regulations/pdf/invitation_for_comments_pr_02-2023.pdf.

² The opinions expressed herein do not necessarily reflect the views of FPF's supporters or Advisory Board.

including better access to opportunities such as education and employment, while trusting that their personal data is protected from misuse.

Unfortunately, existing regulatory regimes, including civil rights laws, have struggled to keep pace with the speed and use of new technologies and business practices that utilize ADM systems. Too often, marginalized communities are vulnerable to discrimination when it comes to economic and other important life opportunities based on historical data or unrepresentative data sets.³ When the digital economy reinforces human bias, individuals suffer concrete harms, including artificially limited educational opportunities, reduced access to jobs and financial services, and lack of access to government services. In response to these harms, data protection regimes are increasingly adopting rules to ensure that automated tools used for consequential decisions are used in a transparent and fair manner.

For example, the European Union’s General Data Protection Regulation (GDPR) directly limits discriminatory processing by prohibiting most “solely” automated decision-making that leads to legal or similarly significant effects absent explicit consent.⁴ The proposed American Data Privacy and Protection Act would also prohibit the processing of personal data (including by automated means) in a “manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability.”⁵

The CCPA adopts a different focus in responding to the risk of algorithmic harms by providing for individual opt-out rights with respect to automated decisionmaking and profiling. Given this approach, forthcoming regulations must clarify the scope and application of CCPA § 1798.185(a)(16) and determine whether it creates a standalone consumer right to opt-out of ADM or directs the creation of guidance for the application of the law’s opt-out rights in the context of ADM and profiling. Under either approach, FPF recommends that forthcoming rules for ADM draw upon emerging national and global standards and associated guidance in order to protect individual autonomy and support interoperability.

A. Regulations should govern automated decisionmaking systems that produce “legal or similarly significant effects”

Strictly interpreted, the term “automated decisionmaking” could encompass many forms of modern technology including routine, minimal-risk practices, such as loading a website, filtering email for spam or malware, spell-checking documents, making content recommendations, and

³ See Nicol Turner Lee, Paul Resnick & Genie Barton, “Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms,” Brookings (May 22, 2019), <https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/>.

⁴ General Data Protection Regulation Art. 22.

⁵ H.R. 8152, The American Data Privacy and Protection Act (July 18, 2022), *available at* <https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-117-8152-P000034-Amdt-1.pdf>.

providing GPS navigation. Creating an individual right to obtain an alternative process for such operations would be impractical in many cases and would not advance goals of increasing the privacy of personal information. However, other areas where ADM is utilized pose inherently greater risks, including areas such as hiring, tenant screening, insurance, and other consumer scoring.⁶ Therefore, the Agency should specify standards and conditions under which individuals may exercise the right to opt-out of ADM, including profiling. Promulgating a single set of rules that apply across decisions in various domains would allow the Agency to rapidly bring a new set of important consumer rights into practice.

The Agency should consider aligning forthcoming regulations to define and scope the term “ADM” with the GDPR. Article 22 establishes heightened protections for automated decisions that lead to ‘legal or similarly significant effects’ for which a growing amount of legal guidance is becoming available.⁷ In establishing individual rights over ADM with “legal or similarly significant effects,” comprehensive state laws in Virginia, Colorado, and Connecticut further clarify this standard as applying to decisions that result in the provision or denial of “financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to [essential goods or services].”⁸

Given the CCPA’s unique (for a U.S. context) application to employee information, forthcoming regulations should also clarify when automated employment related decisions may be subject to consumer opt-out rights. Such decisions could include screening job applicants and decisions regarding employee promotion and termination. A potential resource for delineating the scope of opt-out rights with respect to ADM in an employment context is New York Local Law 2021/144 and associated regulations governing automated employment decision tools.⁹ FPF further recommends that the Agency use the forthcoming rulemaking process to craft rules regarding application of the full range of CCPA rights and obligations in the employment data context, which has emerged as a major point of uncertainty for regulated entities.¹⁰

⁶ We note that many of the most serious use cases fall outside the scope of CPRA (e.g., decisionmaking systems used in criminal sentencing, or by HIPAA-covered entities to make diagnosis decisions).

⁷ See European Commission, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)” (Aug. 8, 2018), <https://ec.europa.eu/newsroom/article29/items/612053>.

⁸ See Virginia Consumer Data Protection Act § 59.1-571, Colorado Privacy Act § 6-1-1303(10), Connecticut Data Privacy Act § 1(13).

⁹ New York City Local Law 2021/144 on automated employment decision tools, *available at* <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9>.

¹⁰ See Maeve Allsup & Jake Holland, “Bosses Brace for Worker Chaos If California Privacy Law Expands,” Bloomberg Law (June 8, 2022), <https://news.bloomberglaw.com/privacy-and-data-security/bosses-brace-for-worker-chaos-if-california-privacy-law-expands>.

B. Regulations should clarify how the California Consumer Privacy Act will apply to automated decisions and profiling subject to varying degrees of human oversight

Some decisionmaking systems are purely automated and others are purely human-driven, but many decisions with legal effects involve some combination of automated assessment and human decisionmaking. In developing regulations on profiling and automated decisions, FPF recommends clarifying under what conditions human involvement and oversight will mean that a decision has *not* been carried out on an “automated” basis (and would thus not be subject to opt-out rights). Where human review of a legal or similarly significant decision amounts to little more than a “rubber stamp,” the regulations should clearly preserve consumer opt-out rights. Specifically, regulations should clarify that a human nominally making a final determination or sending an otherwise automated decision along for implementation is likely insufficient to determine that a decision is not “automated.” Instead, meaningful human involvement should require consideration of available data as well as the authority and competency to change outcomes.

The European Data Protection Board has clarified that the GDPR’s definition of “profiling,” which is closely aligned with the CCPA, “has to involve some form of automated processing – although human involvement does not necessarily take the activity out of the definition.”¹¹ This underlines the need for clarifying the meaning of “automated” in the context of both “automated decision-making” and “profiling”¹² through regulations, as well as the degree of human involvement that would exclude certain evaluations, analyses, or predictions about data subjects from the scope of the definitions and, therefore, of the right to opt-out.

As a practical example in the GDPR context, in 2021 the Portuguese Data Protection Authority reviewed a university’s use of proctoring software to analyze students’ behavior during exams in pursuit of building a fraud likelihood score which informed final human-made decisions (by professors) on whether to invalidate students’ exams or not. The Court found such decisions to be fully automated despite professors making the final decision as to whether to conduct an investigation and ultimately on whether to invalidate the exam. Central to the Court’s determination was a finding that the lack of “guiding criteria” for evaluating the automated scores could “generate situations of discrimination and lead teachers to validate the systems’ decisions

¹¹ See European Data Protection Board, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, p. 7 (Feb. 6, 2018), <https://ec.europa.eu/newsroom/article29/items/612053/en>.

¹² The CCPA § 1798.140 defines “profiling” as: “any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185, to evaluate certain personal aspects relating to a natural person and 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.” (emphasis added)

as a rule.”¹³ For further examples of European courts’ interpretation and application of the GDPR’s approach to ADM, please see FPF’s comprehensive report analyzing over 70 related judgments.¹⁴

We further encourage the Agency to consider recently finalized regulations addressing “automated” processing under the Colorado Privacy Act which delineates three forms of automated processing::

- **“Human Involved Automated Processing”** means the automated processing of Personal Data where a human (1) engages in a meaningful consideration of available data used in the Processing or any output of the Processing and (2) has the authority to change or influence the outcome of the Processing.
- **“Human Reviewed Automated Processing”** means the automated processing of Personal Data where a human reviews the automated processing, but the level of human engagement does not rise to the level required for Human Involved Automated Processing. Reviewing the output of the automated processing with no meaningful consideration does not rise to the level of Human Involved Automated Processing.
- **“Solely Automated Processing”** means the automated processing of Personal Data with no human review, oversight, involvement, or intervention.

Under the Colorado regulations, each defined category of automated processing is subject to risk assessments, but a controller may decline an opt-out request directed towards a “human involved automated processing” system if certain disclosures are made to the consumer.¹⁵

Finally, in promulgating rules or future guidance on ADM systems, the Agency should ensure the application of consumer rights to the cumulative or compounding automated decisions that substantially contribute to the provision or denial of significant opportunities (so-called ‘pipeline’ decisions), rather than only the final decisions.¹⁶ For example, in considering employment opportunities, consumer rights could extend to automated profiling that elevates or scores resumes, evaluates “personality” or “fit,” or makes predictions about future success, rather than narrowly applying to a final decision of whether to offer or terminate a job or contract.

¹³ CNPD, Deliberação n.º 2021/622 (May 11, 2021) *available at*

[https://gdprhub.eu/index.php?title=CNPD_\(Portugal\)_-_Delibera%C3%A7%C3%A3o/2021/622](https://gdprhub.eu/index.php?title=CNPD_(Portugal)_-_Delibera%C3%A7%C3%A3o/2021/622).

¹⁴ Sebastião Barros Vale and Gabriela Zanfir-Fortuna, “Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities,” *Future of Privacy Forum* (May 23, 2022) <https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf>.

¹⁵ Colorado Department of Law “Colorado Privacy Act Rules” (Mar. 15, 2023) *available at* <https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf>.

¹⁶ Miranda Bogen & Aaron Rieke, “Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias,” *Upturn* (Dec. 2018), <https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf>.

C. Regulations should establish rules that will support meaningful access rights with respect to automated decisionmaking systems

When companies rely on biased algorithms to make important decisions, they can unintentionally exacerbate existing inequalities and continue historical patterns of discrimination based on race, gender, sexual orientation, disability, and other protected characteristics. Therefore, it's important to focus this Agency's rulemaking on how consumers can meaningfully inform themselves regarding the use of personal data in ADM systems that present higher risks to individuals.

In practice, it can be a challenge to provide truly meaningful, explainable, or interpretable AI for average consumers, particularly with more complex automated systems such as neural networks and unsupervised machine learning. Individuals will typically be best informed if provided with information about categories of data used, the factors that led to a high-impact decision, and the main reasons for it, rather than divulging specific algorithms or source code, which can be difficult to interpret and will frequently implicate trade secrets.

In developing regulations on this topic, we recommend that the Agency consider best practices and guidance from both the U.S. National Institute for Science and Technology (NIST) and European Data Protection Board (EDPB). NIST's "Four Principles of Explainable Artificial Intelligence" articulates principles for explainable AI systems: "that the system produce an explanation, that the explanation be meaningful to humans, that the explanation reflects the system's processes accurately, and that the system expresses its knowledge limits."¹⁷ The guidelines establish principles for explainable systems covering how they should (1) provide an explanation; (2) be understandable to its intended end-users; (3) be accurate; and (4) operate within its knowledge limits, or the conditions for which it was designed. As noted in the NIST guidance, the Agency should also consider that "meaningful" is highly contextual, and should be tailored to the audience's need, level of expertise, and relevancy to what they are interested in.

The EDPB has endorsed guidelines that state that information provided to data subjects about automated decision-making under GDPR Articles 13(2)(f) and 14(2)(g) should include:

- The categories of data that have been or will be used in the profiling or decision-making process;
- Why these categories are considered pertinent;
- How any profile used in the automated decision-making process is built, including any statistics used in the analysis;
- Why this profile is relevant to the automated decision-making process; and

¹⁷ P. Jonathon Phillips et. al, "Four Principles of Explainable Artificial Intelligence," U.S. Department of Commerce, National Institute of Standards and Technology, p.21 (Sept. 2021), <https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8312.pdf>.

- How it is used for a decision concerning the data subject.¹⁸

Finally, ensuring equitable access of information to all individuals may include: requiring entities to offer consumer access rights in non-English languages, requiring web accessibility mechanisms, and providing alternative processes for those without access to broadband to submit consumer access requests, and receive responses, including through paper forms or other means.

2. Risk Assessments

The California Privacy Protection Act as amended by the California Privacy Rights Act, is one of four U.S. state privacy laws taking effect in 2023 that will require organizations to conduct and document assessments of the risk of data processing activities. Data protection assessments are an important tool for ensuring that organizations consider privacy implications and safeguards in the development of products and services while also providing for a record that allows organizations to demonstrate compliance efforts.¹⁹ Although data protection assessments have long been a feature of administrative governance in the United States,²⁰ U.S. consumer privacy laws have not historically mandated that private organizations conduct data risk assessments. As a result, both formal and informal regulatory guidance will be helpful to ensure that these assessments fulfill their intended purposes without creating unnecessary costs and procedural hurdles for covered entities.

A. Regulations should provide guidance that supports context-appropriate flexibility in developing and conducting data protection assessments

With the exception of the CCPA's general grant of rulemaking authority, the risk assessment requirements under forthcoming U.S. state privacy laws in Virginia, Colorado, and Connecticut contain substantially similar provisions in regard to the scope of assessments, assessment content, and reporting requirements. These laws stand in stark contrast with the CCPA where the grant of rulemaking authority raises various threshold questions such as: (1) if a single risk assessment is expected to cover the entirety of data processing activities of an organization; (2)

¹⁸ European Data Protection Board, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679," p.31 (Feb. 6, 2018), <https://ec.europa.eu/newsroom/article29/items/612053/en>.

¹⁹ See Information Commissioner's Office, "Guide to Data Protection Impact Assessments, 'What is a DPIA?'," <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/#dpia2> (last accessed Mar. 20, 2022).

²⁰ See Revision of OMB Circular A-130, "Managing Information as a Strategic Resource," FR Doc. 2016-17872 (July 28, 2016), <https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circularno-a-130-managing-information-as-a-strategic-resource>.

whether risks assessments are supposed to cover every data processing activity carried out by a covered organization in equal depth, even activities that facially pose minimal risk to consumers; and (3) how the Agency will protect risk assessments in transmission and storage should the Agency require the affirmative submission of millions or more risk assessments?

While clarity of content and scope of assessments is crucial, FPF recommends that forthcoming regulations avoid prescriptive requirements on the form that risk assessments should take, which could result in organizations preparing duplicative, state-specific assessments, which contain no additional information or add any benefit in terms of consumer privacy, but greatly increase compliance costs. Regulations should also ensure that organizations have appropriate leeway to seriously examine their data flows, associated risks, and mitigating safeguards and are not incentivized to treat assessments as a purely defensive or box-checking measure. A flexible approach may also support the development of sector-specific, context appropriate assessments best suited for particular types of data processing (e.g., targeted advertising or consumer scoring), and sensitive categories of data (e.g., health data or mobility information).²¹

Global data protection standards recognize that risk assessments provide the most value to covered businesses, enforcers, and data subjects, if the focus of their analysis is directed toward inherently sensitive categories of data and potentially harmful processing activities.²² For example, the three state comprehensive privacy laws that directly establish standards for risk assessments require them to be conducted where sensitive personal data is being processed, or for inherently risky processing purposes, such as targeted advertising, sale of data, or other activities that present a heightened risk of harm to consumers (defined broadly to include unfair or deceptive treatment, financial, physical, or reputational injury, or intrusion upon solitude or seclusion that would be offensive to a reasonable person).²³ FPF recommends that regulations should explicitly provide that risk assessments originally conducted pursuant to comparable data protection regimes should be acceptable as CCPA risk assessments if they are reasonably similar in scope and effect to forthcoming regulations.

B. The Agency should develop regulations and informal guidance informed by existing best practices for data protection assessments

Given that many organizations, especially small companies, will likely conduct risk assessments for the first time as part of their CCPA compliance operations following the forthcoming rulemaking, it may be appropriate for the Agency to assemble a catalog of resources containing

²¹ See e.g., Chelsey Colbert & Kelsey Finch, “FPF and Mobility Data Collaborative release resources to help organizations assess the privacy risks of sharing mobility data,” Future of Privacy Forum (Aug. 30, 2021), <https://fpf.org/blog/fpf-and-mobility-data-collaborative-release-resources-to-help-organizations-assess-the-privacy-risks-of-sharing-of-mobility-data/>.

²² The CPRA amendments to the CCPA create a new category of “sensitive” personal information at § 1798.140(ae).

²³ See Virginia Consumer Data Protection Act § 59.1-576, Colorado Privacy Act § 6-1-1309, Connecticut Data Privacy Act § 8.

sample assessment guides, templates, and other informal guidance outside the formal regulatory process.

Requirements to conduct and document assessments of inherently risky data processing practices, risks, and mitigating safeguards are a common feature of modern global privacy laws.²⁴ To support compliance efforts, regulators in the United Kingdom, France, Spain, Singapore, and New Zealand have all developed extensive guidance documents and tools (typically available in multiple languages) to help organizations determine when to conduct assessments, key concepts that assessments must consider, and procedures for reviewing and updating assessments over time (see resources below). The Commission nationale de l'informatique et des libertés (CNIL), the French Data Protection Authority (DPA), has even developed software to assist organizations conducting DPAs.²⁵

FPF recommends that the Attorney General's Office draft regulations and develop guidance for conducting CCPA-compliant assessments that are informed by existing requirements and best practices for data protection assessments. This approach will allow Californian businesses and consumers to benefit from high existing standards for data protection and promote harmonization with global privacy frameworks, a stated statutory priority.

Global Resources on Data Protection Risk Assessments:

- Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679" WP 248 rev.01 (Oct. 4, 2017), <https://ec.europa.eu/newsroom/article29/items/611236>.
- Information Commissioner's Office [United Kingdom], "Sample DPIA Template" (Feb. 2018), <https://ico.org.uk/media/2258461/dpia-template-v04-post-comms-review-20180308.pdf>.
- Commission nationale de l'informatique et des libertés (CNIL) [France] "GDPR Toolkit > Privacy Impact Assessments," <https://www.cnil.fr/en/privacy-impact-assessment-pia>.
- Agencia Española de Protección de Datos (AEDP) [Spain], "Risk Management and Impact Assessment Regarding Data Protection" (June 27, 2022), <https://www.aepd.es/en/areas/innovation-and-technology>.
- Personal Data Protection Commission (PDPC) [Singapore], "Guide to Data Protection Impact Assessments" (Sept. 14, 2021), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPIA/Guide-to-Data-Protection-Impact-Assessments-14-Sep-2021.ashx?la=en>.
- New Zealand Privacy Commissioner, "Privacy Impact Assessment Handbook" (July, 2015), <https://privacy.org.nz/publications/guidance-resources/privacy-impact-assessment/>.

²⁴ See e.g., GDPR Art. 35; General Personal Data Protection Law (Brazil) Art. 38; Personal Information Protection Law (China) Art. 56; Personal Data Protection Act (Singapore) Art. 14.

²⁵ CNIL, "The open source PIA software helps to carry out data protection impact assessment" (June 30, 2021), <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment>.

Thank you for this opportunity to provide input on initial rulemaking under the California Privacy Rights Act amendments to the California Privacy Rights Act. We welcome any further opportunities to provide resources or information to assist in this important effort.

Sincerely,

Keir Lamont
Director for U.S. Legislation

From: Abdelaziz, Laila [REDACTED]
Sent: Monday, March 27, 2023 2:53 PM
To: Regulations
Cc: Haylamaz, Burak; Reisman, Matthew; Heyder, Markus
Subject: PR 02-2023
Attachments: CIPL Response to CPPA Invitation for Preliminary Comments on Proposed Rulemaking on Cybersecurity Audits, Risk Assessment and ADM - March 27, 2023.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hi there,

Attached is the Centre for Information Policy Leadership (CIPL)'s response to the CPPA's February 2023 Invitation for Preliminary Comments on Proposed Rulemaking.

Thank you for the opportunity to comment on these important topics. Please do not hesitate to reach out to us if more information is needed.

Thank you in advance for your consideration,
Laila



Laila Abdelaziz
Privacy & Data Policy Manager

Tel: [REDACTED]
Mob: [REDACTED]

Hunton Andrews Kurth LLP
2200 Pennsylvania Avenue, NW
Washington, DC 20037
HuntonAK.com
informationpolicycentre.com

This communication is confidential. If you are not an intended recipient, please advise by return email immediately and then delete this message, including all copies and backups.

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 CCPA 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 unsustainable 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 GDPR¹² (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, health 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 produce 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	<ul style="list-style-type: none"> • 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 <i>Some of these examples may also fall within the category of legal effects depending on the applicable</i>	<ul style="list-style-type: none"> • 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](#).

<i>legal regime and the specific decision in question</i>	<ul style="list-style-type: none"> • Decision to promote or pay a bonus to an individual; • Decisions affecting an individual's access to energy services and determination of tariffs.
<p>Decisions <u>Not</u> Producing Legal or Similarly Significant Effects</p> <p><i>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.</i></p>	<ul style="list-style-type: none"> • 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 patterns 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	<ul style="list-style-type: none"> • 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”.

	<ul style="list-style-type: none"> • Preventing cybercrimes.
Health	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Cyber-incident prevention and diagnostics; • Network and information protection; • Personalization of Internet browsing sessions.
Insurance	<ul style="list-style-type: none"> • Underwriting risks and allocating premiums.
Human Resources	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Predicting energy consumption; • Forecasting demand and supply levels; • Understanding usage peaks; • More efficiently detecting and responding to utility outages.
Education	<ul style="list-style-type: none"> • School and university admissions; • Promoting policies of affirmative action; • Using analytics to optimize learning environments.
Marketing	<ul style="list-style-type: none"> • Providing recommendations based on profiles, previous and peer purchases; • Loyalty programs – retail, hotel, travel services, etc.; • Customer segmentation.
Non-profit	<ul style="list-style-type: none"> • Identifying potential supporters and patterns of charitable behaviors.
Public Sector	<ul style="list-style-type: none"> • 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										
Risks	Unjustifiable Collection			Inappropriate Use			Security Breach			Aggregate
				Inaccuracies Not expected by individual Viewed as Unreasonable Viewed as Unjustified			Lost Data Stolen Data Access Violation			
	Likely	Serious	Score	Likely	Serious	Score	Likely	Serious	Score	Risk Rank
<u>Tangible Harm</u>										
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
<u>Intangible Distress</u>										
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 ?	

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?		ANNEX
		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 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 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 serious?		how serious?		how serious?		how serious?		how serious?		how serious?		

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?		

From: Matt Schwartz [REDACTED]
Sent: Monday, March 27, 2023 3:05 PM
To: Regulations
Subject: PR 02-2023 - Consumer Reports Comments
Attachments: Comments of Consumer Reports on CPPA Proposed Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking Rulemaking.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good afternoon,

Attached please find comments from Consumer Reports in response to the Invitation for Preliminary Comments on Proposed Rulemaking for Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking.

Thank you,
-Matt

--

Matt Schwartz
Policy Analyst

o [REDACTED] | m [REDACTED]

Pronouns: he, him, his

[CR.org](https://www.consumerreports.org)



This e-mail message is intended only for the designated recipient(s) named above. The information contained in this e-mail and any attachments may be confidential or legally privileged. If you are not the intended recipient, you may not review, retain, copy, redistribute or use this e-mail or any attachment for any purpose, or disclose all or any part of its contents. If you have received this e-mail in error, please immediately notify the sender by reply e-mail and permanently delete this e-mail and any attachments from your computer system.

Comments of Consumer Reports
In Response to the
California Privacy Protection Agency's
Invitation for Preliminary Comments On
Proposed Rulemaking for Cybersecurity Audits, Risk Assessments, and Automated
Decisionmaking

By

Matt Schwartz, Policy Analyst
Justin Brookman, Director of Technology Policy

March 27, 2023



Consumer Reports¹ appreciates the opportunity to provide feedback on the California Privacy Protection Agency's (CPPA) Invitation for Preliminary Comments on Proposed Rulemaking on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking. We thank the CPPA for initiating this proceeding and for its other efforts to protect consumer privacy.

We describe our views on each of the potential areas for rulemaking in the course of providing answers to the questions posed by the CPPA in its invitation.

I. Cybersecurity Audits

1. What laws that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require cybersecurity audits? For the laws identified:

- a. To what degree are these laws' cybersecurity audit requirements aligned with the processes and goals articulated in Civil Code § 1798.185(a)(15)(A)?*
- b. What processes have businesses or organizations implemented to comply with these laws that could also assist with their compliance with CCPA's cybersecurity audit requirements?*
- c. What gaps or weaknesses exist in these laws for cybersecurity audits? What is the impact of these gaps or weaknesses on consumers?*
- d. What gaps or weaknesses exist in businesses' compliance processes with these laws for cybersecurity audits? What is the impact of these gaps or weaknesses on consumers?*
- e. Would you recommend that the Agency consider the cybersecurity audit models created by these laws when drafting its regulations? Why, or why not?*

Though cybersecurity audits are admittedly far from Consumer Reports' top priority in privacy law, we do believe they have a role to play and that fulsome outside evaluation of businesses' cybersecurity risk is likely to benefit consumers. In order to pass audits, businesses will be motivated to invest more resources into safeguards to protect personal data from unauthorized access that could result in a host of secondary harms that extend beyond the original collection, including, physical, reputational, psychological, discriminatory, and economic harms. Basic cybersecurity hygiene calls for consumer friendly behaviors such as encrypting data, reducing employee access, and simply minimizing the amount of consumer data the business collects and retains to begin with.

¹ Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

Extant state law focusing *specifically* on cybersecurity is minimal compared to state data security law, where at least 25 states have passed measures that address the data security practices of private entities.² The handful of state laws that specifically address cybersecurity, such as those in Massachusetts, New York, and Oregon, typically require businesses to “assess” the safeguards they have implemented to mitigate cyber risks, rather than accede to a formal audit.³ Similarly, state data security laws typically require that businesses adopt “reasonable” safeguards, but do not require businesses to submit to formal third-party audits. Since many existing state data security and cybersecurity laws only require businesses to *internally* assess their relevant safeguards, whereas CPRA clearly contemplates independent audits (which, in our view, means those conducted by a dispassionate third-party), CPRA seems to raise the bar above existing law.

Other strong state cybersecurity provisions include those instituted by the New York Department of Financial Services (NYDFS), which recently adopted new requirements for financial institutions, including annual penetration testing and bi-annual vulnerability assessments, limits on access privileges, and a requirement to designate a chief information security officer who is responsible for the company’s security program.⁴

On the federal level, the FTC recently updated its Safeguards Rule with more specific security requirements, consistent with the NYDFS regulation, including placing limits on internal access to data, new encryption requirements, and a requirement to establish a chief security officer. The new rules also require covered businesses to conduct an assessment (internal *and* external) to determine foreseeable risks and threats to the security, confidentiality, and integrity of customer information.⁵ Separately, the FTC has interpreted its Section 5 authority to mandate that companies take reasonable security measures to protect consumer information – though it is unclear when that may require auditing.⁶ The Health Information Technology for Economic and Clinical Health Act also requires that the U.S. Department of Health and Human Services, through its Office of Civil Rights (OCR), periodically audit covered entities and business associates for their compliance with the Health Insurance Portability and Accountability Act privacy, security, and breach notification rules.⁷

² Data Security Laws | Private Sector, National Council of State Legislatures, (May 29, 2019), <https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx>.

³ See, e.g., Code of Massachusetts Regulations 201 Section 17.03 2(b), <https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the/download>

⁴ 23 CRR-NY § 500.0 et seq., https://www.governor.ny.gov/sites/default/files/atoms/files/Cybersecurity_Requirements_Financial_Service_s_23NYCRR500.pdf

⁵ Federal Trade Commission, FTC Safeguards Rule: What Your Business Needs to Know, (May 2022) <https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know>

⁶ Federal Trade Commission, FTC Brings Action Against Ed Tech Provider Chegg for Careless Security that Exposed Personal Data of Millions of Customers, (October 31, 2022) <https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-brings-action-against-ed-tech-provider-chegg-careless-security-exposed-personal-data-millions>

⁷ Office of Civil Rights, HIPAA Privacy, Security, and Breach Notification Audit Program, (December 17, 2020), <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html>

Unfortunately, the lack of regulatory bandwidth to intervene when businesses fail to remedy shortcomings identified by self-assessments and audits often hampers their effectiveness as accountability mechanisms. According to its last available fiscal year report, OCR audited around 150 businesses.⁸ OCR employs around 200 full time employees. Scaling down to an agency of CPPA's size, even assuming massive efficiency gains from the CPPA outsourcing audit responsibilities to third parties, it is clear that CPPA will not be able to review cybersecurity audits on a mass scale.

Absent the expectation of robust oversight, businesses are less likely to invest the resources necessary to protect consumer information above levels that the market may bear, which, for a variety of reasons – including many industries operating in non-competitive markets, can be an exceedingly low bar. The consistent drumbeat of news articles describing the increase in successful cyberattacks on companies of all sizes seems to bear this out.⁹

Consistent underfunding of key regulators has left them under-equipped to keep pace and police the market. Consumer Reports has consistently called for legislators to raise funding levels for key regulators; until more appropriate funding levels are reached, underenforcement of all business requirements, but especially laborious ones like cyber audits, will continue to be endemic.¹⁰

II. Risk-Assessments

1. What laws or other requirements that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require risk assessments? For the laws or other requirements identified:

a. To what degree are these risk-assessment requirements aligned with the processes and goals articulated in Civil Code § 1798.185(a)(15)(B)?

Following the passage of the General Data Protection Regulation (GDPR) in the European Union, data protection risk-assessments have emerged as a consistent presence in comprehensive state privacy laws and proposals in the United States. Of the four other comprehensive state privacy laws, three, Virginia (VCDPA), Connecticut (CTDPA), and Colorado (CPA), include a requirement for covered entities to conduct data protection assessments regarding processing activities that pose a “heightened risk of harm” or other specific risks to consumers. Drawing from the text of GDPR, each of the risk-assessments requires that businesses weigh the benefits of processing to all relevant stakeholders against

⁸ Office of Civil Rights, Health Information Privacy Division, 2016-2017 HIPAA Audits Industry Report (December 2020), <https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf>

⁹ E.g., Joy LePree Anderson, Global Cyberattacks Increased 38 percent in 2022, Security Magazine, (January 20, 2023), <https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022>

¹⁰ Consumer Reports, Group Letter in Support of FTC Privacy Funding, (September 2021), <https://advocacy.consumerreports.org/wp-content/uploads/2021/09/Group-letter-in-support-of-FTC-privacy-funding.pdf>

the potential risks to the rights of the consumer associated with such processing. Through its rulemaking process, Colorado has gone furthest to outline the discrete elements and process required to complete a risk assessment.

Though the aforementioned requirements largely align with those articulated in CPRA, it is not a one-to-one match. Firstly, the risk assessment requirement under CPRA applies to businesses whose processing presents “significant risk to consumers’ privacy or security,” rather than a “heightened risk” as in the other laws.¹¹ The term “significant risk” is undefined in CPRA. CPRA also requires that businesses identify when their processing involves sensitive personal information, whereas that requirement lives elsewhere in the other state laws (though Colorado did include this in their regulations).¹² Finally CPRA attaches a normative goal to its risk-assessment requirement, which is to “[restrict] or [prohibit] the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.”

b. What processes have businesses or organizations implemented to comply with these laws, other requirements, or best practices that could also assist with compliance with CCPA’s risk-assessments requirements (e.g., product reviews)?

Businesses with operations in Europe should be familiar with the broad framework and goals of a data protection risk-assessment through their compliance with GDPR. Risk assessments may be a newer undertaking for smaller U.S. based businesses, especially those that do not operate in other states with comprehensive privacy laws.

c. What gaps or weaknesses exist in these laws, other requirements, or best practices for risk assessments? What is the impact of these gaps or weaknesses on consumers?

One major weakness in the existing risk-assessment framework as set out in Virginia, Connecticut, and Colorado is that the assessment must only be produced if the controller is being investigated by a supervisory authority.¹³ In fact, each of the laws completely exempts risk assessments from public inspection. Unless a company’s behavior is suspicious enough to warrant an Attorney General investigation, nobody outside of the business will ever see the risk assessment.

Another weakness stems from the assumption that by forcing controllers to confront the risks inherent to their data processing activities, they will automatically change their behavior. The reality is that even when tech companies fully recognize the harms their services cause, they often do not act to countervail them; Frances Haugen’s revelations regarding Facebook’s lack of action in the face of multiple known harms created by the platform provide the most high-profile

¹¹ Civil Code § 1798.185(a)(15)(B)

¹² Colorado Department of Law, Consumer Protection Section, Colorado Privacy Act Rules 4 CCR 904-3, Section 8.04 A(2), (March 2023), <https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf>

¹³ Code of Virginia, Consumer Data Protection Act, Section 59.1-580(C), <https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/>

example.¹⁴ The more intertwined a business' revenue model is with the harms they produce, as in the case of the surveillance advertising model, the less likely risk assessments are to change behavior voluntarily. If the goal of improving consumer outcomes through risk assessments is even achievable, stronger accountability mechanisms are required.

CPRA's risk assessment does differ somewhat from other states, since it explicitly states that the goal is "restricting or prohibiting" processing if the risks outweigh the benefits. However, without strict enforcement, businesses are likely to simply downplay the risks in order to avoid any affirmative requirement to change. At the very least, CPPA should require that businesses provide risk assessments to the agency on an ongoing basis – rather than only when the business is being investigated – so that they may review for systemic underreporting or other obvious noncompliance. In any case, proving a business outright lied on its risk assessment will likely be a difficult endeavor.

At the same time, we recognize that state Attorneys General or even dedicated supervisory authorities like the CPPA do not possess the resources to closely and continually monitor risk assessments. For this reason, we believe it is crucial that the public also be able to review risk assessments (with tightly scoped exemptions around revealing business trade secrets), so that interested consumers can use this information to weigh their engagement with businesses. Public inspection of risk assessments will also deputize the public by allowing it to relay important information back to the agency that it may not have uncovered on its own. While few people will likely read risk assessments and the business will still be incentivized to emphasize the public benefits of its processing and minimize the risks, more documentation is probably better than nothing at all. CPPA's forthcoming regulations should also require that businesses share any internal documentation they possess on the concrete harms caused by the service to avoid large-scale coverups like at Facebook.

Similar to cybersecurity audits, it all comes down to enforcement. If businesses fear the consequences of not being forthcoming, risk assessments could produce additional information that improves regulators' and the public's understanding of the processing harms caused by businesses. If left to their own devices, businesses will likely produce anodyne documents that serve few and the process will simply become a "check the box" exercise.

d. What gaps or weaknesses exist in businesses' or organizations' compliance processes with these laws, other requirements, or best practices for risk assessments? What is the impact of these gaps or weaknesses on consumers?

As previously mentioned, comprehensive state privacy laws that require risk assessments do not *allow* them to be publicly available, let alone require it. GDPR also does not mandate public disclosure. As such, our understanding of business' compliance processes with existing risk assessment frameworks is minimal.

¹⁴ Wall Street Journal, The Facebook Files, (October 1, 2021), <https://www.wsj.com/articles/the-facebook-files-11631713039>

In the rare instances that businesses do make risk assessments publicly available, evidence of their efficacy is sketchy, if inconclusive. For example, Google recently reduced the results of its voluntary civil rights audit, which was roundly criticized by civil rights advocates for being performative and light on details.¹⁵

e. Would you recommend the Agency consider the risk assessment models created through these laws, requirements, or best practices when drafting its regulations? Why, or why not? If so, how?

See above (*supra* Section 2, Question 1(c)) for our view on how existing models can be improved.

2. What harms, if any, are particular individuals or communities likely to experience from a business's processing of personal information? What processing of personal information is likely to be harmful to these individuals or communities, and why?

It is first important to note that unwanted observation, through excessive data collection and use, is harmful in and of itself. Intrusion upon seclusion has long been recognized as a privacy tort, and consumers will always have a legitimate interest in constraining unnecessary processing of their data. That applies both on the individual level, as well as collectively.

Consumers have no shortage of reasons to object to the collection and retention of their personal information per se even if a company has no immediate plans to do anything with that data. Some of those reasons include:¹⁶

- **Data breach:** The data could be breached and accessed by outside attackers, or inadvertently exposed to the world.
- **Internal misuse:** Bad actors within the company could access and misuse the data for their own purposes.¹⁷
- **Loss of economic power and future unwanted secondary use:** Even if the company today has no present plans to use the data, the company could change its mind in the future (privacy policies often reserve broad rights to use personal information for any number of reasons). Such usage could range from the merely annoying (say, retargeted advertising) to price discrimination to selling the information to data brokers who could then use the information to deny consumers credit or employment. Differential pricing is

¹⁵ Cristiano Lima, Google's civil rights audit lacked teeth, advocates say, Washington Post (March 10, 2023), <https://www.washingtonpost.com/politics/2023/03/10/googles-civil-rights-audit-lacked-teeth-advocates-say/>

¹⁶ These categories are derived from a paper for the Future of Privacy Forum and the Stanford Center for Internet & Society's "Big Data and Privacy: Making Ends Meet" workshop. For further elaboration on these categories, see Justin Brookman and G.S. Hans, Why Collection Matters: Surveillance as a De Facto Privacy Harm, (Sep. 30, 2013), <https://cdt.org/wp-content/uploads/2018/08/September-2013-Brookman-Hans-Why-Collection-Matters.pdf>

¹⁷ Adrian Chen, GCreep: Google Engineer Stalked Teens, Spied on Chats, Gawker (Sep. 14, 2010) <http://gawker.com/5637234/gcreep-googleengineer-stalked-teens-spied-on-chats>

a special concern, as companies with more data about an individual will have a better sense of how much that person is willing to pay for a particular product. This in turn will empower the company to set personal prices closest to that equilibrium point, allowing the company to take relatively more of the consumer surplus from any transaction. This type of first-degree price discrimination is all the more of a concern to consumers as increasing corporate concentration means that consumers have fewer market alternatives.

- **Government access:** Consumers may be legitimately concerned about illegitimate government access to their personal information. TikTok, for example, has been dogged by fears of Chinese government access¹⁸ — fears that appear to be justified.¹⁹ Moreover, in the wake of the Dobbs Supreme Court decision, many Americans worry that fertility and health information generated and stored by tech companies may be accessed by states that criminalize abortion access.²⁰
- **Chilling effect:** Finally, all these concerns together —along with others, and even with an irrational or inchoately realized dislike of being observed — has a chilling effect on public participation and free expression. People will feel constrained from experimenting with new ideas or adopting controversial positions. In fact, this constant threat of surveillance was the fundamental conceit behind the development of the Panopticon prison: if inmates had to worry all the time that they were being observed, they would be less likely to engage in problematic behaviors.²¹ The United States was founded on a tradition of anonymous speech. In order to remain a vibrant and innovative society, citizens need room for the expression of controversial — and occasionally wrong — ideas without worry that the ideas will be attributable to them in perpetuity. In a world where increasingly every action is monitored, stored, and analyzed, people have a substantial interest in finding some way to preserve a zone of personal privacy that cannot be observed by others.

With that said, there are also many, many examples of *discrete* commercial surveillance and processing practices negatively impacting individuals and disproportionately harming vulnerable populations and communities historically subjected to discrimination. For example, the Department of Housing and Urban Development has charged Facebook for targeting housing advertisements based on protected categories like race and religion.²² These targeting systems have also been used to interfere with elections and fuel voter suppression efforts and to carry

¹⁸ Jack Sommers, Nearly half of Americans fear TikTok would give their data to the Chinese government, Business Insider, (Jul. 15, 2021), <https://www.businessinsider.com/nearly-half-of-americans-fear-tiktok-would-give-china-data-2021-7>

¹⁹ Christianna Silva and Elizabeth de Luna, It looks like China does have access to U.S. TikTok user data, Mashable, (Nov. 3, 2022), <https://mashable.com/article/tiktok-china-access-data-in-us>.

²⁰ Naomi Nix and Elizabeth Dwoskin, Search warrants for abortion data leave tech companies few options, Washington Post, (Aug. 12, 2022), <https://www.washingtonpost.com/technology/2022/08/12/nebraska-abortion-case-facebook/>.

²¹ Michel Foucault, Discipline and Punish: The Birth of the Prison (1977).

²² Sec'y of Hous. & Urban Dev. v. Facebook, Inc., No 01-18-0323-8, 1, Charge of Discrimination, FHEO No. 01- 18-0323-8 (Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.

out disinformation campaigns that undermine public trust.²³ Further, some data brokers provide this information to employers, landlords, and others, while evading the Fair Credit Reporting Act, giving consumers next to no control over these uses.²⁴ The increasing use of automated decision-making can further exacerbate these problems, as opaque algorithms, often trained on historical data, can perpetuate existing inequalities.²⁵

In one recent example, Consumer Reports uncovered evidence that auto insurers were engaging in algorithmically-driven discriminatory pricing schemes based on educational attainment and employment data they had collected from consumers.²⁶ These factors disproportionately penalize drivers of color and working-class people, often costing them hundreds of dollars per year.

Consumer Reports has also written about the use of race as a variable in medical algorithms, which can determine eligibility for critical services, such as risky treatments or organ transplants.²⁷ One paper found that Black patients were assigned lower-risk scores than white patients, even when they were equally sick; the algorithm used data about patients' historical healthcare costs to make decisions, and Black patients were routinely spent less on, which the scientists speculated is due to systemic barriers to healthcare access.²⁸ While many hospitals have dropped race as a consideration in medical algorithms, citing a lack of evidence, many still use them, often without the patient knowing their race was a consideration in the clinical decisionmaking process.²⁹

²³ FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, Fed. Trade Comm'n (July 24, 2019), <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billionpenalty-sweeping-new-privacy-restrictions>.

²⁴ Spokeo to Pay \$800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA, Fed. Trade Comm'n (June 12, 2012), <https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-chargescompany-allegedly-marketed>; Big Data, A Big Disappointment for Scoring Consumer Credit Risk, Nat'l Consumer Law Ctr. at 26 (Mar. 2014), <https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf>

²⁵ See Erin Simpson & Adam Conner, How to Regulate Tech: A Technology Policy Framework for Online Services, Ctr. for Am. Progress (Nov. 16, 2021) (discussing the extensive literature on civil rights harms caused by automated decision-making systems, biometric surveillance, amplification of civil-rights suppressing content, and reification of prejudice), <https://www.americanprogress.org/article/how-to-regulate-tech-a-technology-policy-framework-for-online-services/>.

²⁶ Chuck Bell, CR investigates how auto insurers are using drivers' education and occupation to set premiums, (January 28, 2021) <https://advocacy.consumerreports.org/research/report-effects-of-varying-education-level-and-job-status-on-online-auto-insurance-price-quotes/>

²⁷ Kaveh Waddell, Medical Algorithms Have a Race Problem, Consumer Reports, (September 18, 2020), <https://www.consumerreports.org/medical-tests/medical-algorithms-have-a-race-problem/>

²⁸ Heidi Ledford, "Millions Affected by Racial Bias in Health-Care Algorithm," *Nature* 574 (October 31, 2019): 608-609, <https://media.nature.com/original/magazine-assets/d41586-019-03228-6/d41586-019-03228-6.pdf>.

²⁹ Kaveh Waddell, Medical Algorithms Have a Race Problem, Consumer Reports, (September 18, 2020), <https://www.consumerreports.org/medical-tests/medical-algorithms-have-a-race-problem/>

In the employment context, some AI companies are developing algorithms that are intended to help human resources departments narrow down job applicants or monitor/encourage productivity in the workplace. Companies like HireVue have been criticized for incorporating facial and other analysis into their video interviewing software which monitors the applicant's expressions, their tone of voice, perceived traits like "enthusiasm," eye contact, and their word choice. After much pushback from civil rights groups including an official complaint to the FTC from the Electronic Privacy Information Center, the company discontinued their facial analysis component of their software. HireVue is not the only company using biometrics to assess job applicants; other companies like Interviewer.AI and MyInterview assess candidates' faces, body language, and/or voices and rank candidates perceived characteristics like "sociability," "humility," and "positive attitude." Consumers typically have little ability to revoke consent for such uses.

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?

It is unclear whether there is a truly meaningful distinction between risky and non-risky processing activities. While some activities might be risky no matter the context (facial recognition or automated decisionmaking with legal or similarly significant effects), almost any processing activity poses some degree of inherent risk. Even the most basic activity, such as collecting and processing a consumer's information to consummate a purchase, can entail high-risk depending on the category of item or contextual personal factors of the purchaser.

Plenty of so-called "non-sensitive" personal information, when combined in certain ways, can become sensitive, and companies can often use their vast stores of non-sensitive data to infer sensitive attributes about a person. The Federal Trade Commission has, for example, identified categories such as geolocation³⁰ and TV viewing³¹ as "sensitive" and worthy of greater protection; however, other common categories of data collection — such as web browsing and shopping — can in many cases be at least as if not more revealing about personal behavior.

The boundaries of "risky" behavior are also highly dependent on the person and context, which brings to the fore important equity and civil rights considerations. Individuals with certain lived experiences may not want information about their lives revealed, whereas that same information may be entirely unobjectionable to another person. As such, there are immense challenges in scoping the definitions of risk and sensitive information. A common outcome, at least in the case

³⁰ FTC v Kochava, Inc., Complaint for Permanent Injunction and Other Relief, (August 2022) https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf

³¹ FTC v Vizio and Vizio Inscape, Complaint for Permanent Injunction and Other Equitable and Monetary Relief, (February 2017) https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf

of state privacy laws and proposals, is that the sensitive data category (if such a category exists) is under-inclusive.³²

For that reason, we support a broad definition of risky behavior, which is largely reflected in the European Data Protection Board's (EDPB) approach. The EDPB lists nine categories of processing activity that would meet its definition:

- Evaluation or scoring
- Automated-decision making with legal or similar significant effect
- Systematic monitoring
- Sensitive data or data of a highly personal nature
- Data processed on a large scale
- Matching or combining datasets
- Data concerning vulnerable data subjects
- Innovative use or applying new technological or organizational solutions
- Prevents data subjects from exercising a right or using a service or a contract

In addition to the factors included in the EDPB's analysis, we would add several criteria present in the Colorado Privacy Act rules, including information processed for the purposes of targeting advertising (insofar as that is not already covered by other factors), selling of personal information, and physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person.³³

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

c. Should the models or factors be different, or assessed differently, for determining when processing requires a risk assessment versus a cybersecurity audit? Why, or why not? If so, how?

We do not believe there is a strong reason to differentiate the factors for determining when processing requires a risk assessment versus a cybersecurity audit.

d. What processing, if any, does not present significant risk to consumers' privacy or security? Why?

See above (*supra*, Section 2, Question 3(a)).

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

³² For example, in relation to health information, Virginia's Consumer Data Protection Act only includes "mental or physical health diagnosis" in its definition of sensitive personal information, leaving reproductive health information uncovered. Code of Virginia, Chapter 53, § 59.1-575, <https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/>

³³ Colorado Department of Law, Consumer Protection Section, Colorado Privacy Act Rules 4 CCR 904-3, Section 8.04 (6), (March 2023), <https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf>

a. What would the benefits and drawbacks be if the Agency considered the data protection impact assessment content requirements under GDPR and the Colorado Privacy Act?

See above (*supra* Section 2, Questions 1(c) and 3(a))

b. What, if any, additional content should be included in risk assessments for processing that involves automated decisionmaking, including profiling? Why?

Consumer Reports believes that in the case of automated decisionmaking, especially when those decisions involve legal or similarly significant effect, businesses should provide additional transparency, including an evaluation of how the algorithm works under various conditions and in what circumstances the model is intended to be used.

However, we do not believe that internal risk assessments should be the primary mechanisms to hold businesses accountable for their use of automated decisionmaking systems. Instead we recommend that algorithms that may have significant legal effects undergo third party audits before deployment, and regularly after deployment; we also recommend that these auditors are required to undergo an accreditation process to evaluate algorithms that can have significant legal effects. In order for these audits to be effective, companies should be required to disclose specific data to the auditors, such as training data used to develop the model, a standardized API to easily test the system, or even the code itself, depending on the case. We also recommend that specific issues be investigated by auditors such as discrimination against protected classes, etc. Finally, the results of the audit should be made public if the algorithm has already been deployed to the public. If not, the company must address the results of the audit in a timely manner, and before deployment.

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?

See above (*supra* Section 2, Question 1(c)) for our view on the weaknesses of existing risk assessment models.

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?*

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)?

7. Should the compliance requirements for risk assessments or cybersecurity audits be different for businesses that have less than \$25 million in annual gross revenues? If so, why, and how?

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

It is worth keeping in mind that the primary motivation behind privacy law is to combat the excesses of big internet companies and a small number of niche companies whose primary business is trafficking in personal data. We do not necessarily want to subject smaller companies with far less sophisticated processing capabilities to the same requirements as the largest tech companies. That said, businesses that engage in certain types of behaviors, such as applying novel technologies, processing data of vulnerable individuals, engaging in systematic monitoring of individuals or deploying automated decisionmaking tools that produce legal or significantly similar effects should have to complete risk assessments no matter their size.

III. Automated Decisionmaking

The CCPA directs the Agency to issue regulations “governing access and opt-out rights with respect to businesses’ use of automated decision making technology, including profiling and requiring businesses’ response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer.” In determining the necessary scope of such regulations, the Agency is interested in learning more about existing state, federal, and international laws, other requirements, frameworks, and/or best practices applicable to some or all CCPA-covered businesses or organizations that presently utilize any form of automated decisionmaking technology in relation to consumers, as well as businesses’ compliance processes with these laws, requirements, frameworks, and/or best practices. In addition, the Agency is interested in learning more about businesses’ uses of and consumers’ experiences with these technologies, including the prevalence of algorithmic discrimination. Lastly, the Agency is interested in the public’s recommendations regarding whether access and opt-out rights should differ based on various factors, and how to ensure that access requests provide meaningful information about the logic involved in automated decisionmaking processes as well as a description of the likely outcome of the process with respect to the consumer. Accordingly, the Agency asks:

1. What laws requiring access and/or opt-out rights in the context of automated decisionmaking currently apply to businesses or organizations (individually or as members of specific sectors)?

A right to opt-out of automated decisionmaking is expressed in Article 22 of GDPR, which states that data subjects “shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or

similarly significantly affects him or her.”³⁴ Recent state privacy laws in Virginia, Connecticut, and Colorado have followed suit by allowing consumers to opt out of “profiling” in furtherance of automated decisions that produce legal or similarly significant effects concerning the consumer.

In the financial sector, both the Equal Credit Opportunity Act (ECOA) and Fair Credit Reporting Act (FCRA) provide something resembling access and explainability rights.³⁵ When a consumer is denied credit, under ECOA creditors must provide consumers with the main reasons for that denial. The CFPB recently clarified that creditors that use complex algorithms or artificial intelligence to help generate credit decisions must still “provide a notice that discloses the specific, principal reasons for taking adverse actions.”³⁶ Meanwhile, FCRA requires that when an adverse action, such as the denial of credit, is based on a credit score, the creditor must disclose the key factors that affected the score, among other information.

2. What other requirements, frameworks, and/or best practices that address access and/or opt out rights in the context of automated decisionmaking are being implemented or used by businesses or organizations (individually or as members of specific sectors)?

Some businesses that operate in Europe may also apply opt-out rights to consumers in the United States, but this practice is not widespread, to our knowledge. We are unaware of any self-regulatory frameworks to provide rights to access or explainability when it comes to automated decisionmaking.

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

a. How is “automated decisionmaking technology” defined? Should the Agency adopt any of these definitions? Why, or why not?

The term “automated decisionmaking” is not defined in GDPR, VCDPA, CPA, or CTDPA. Instead, each of those laws defines a related concept, “profiling”, which is automated processing to evaluate certain aspects of a person’s life. Each of those laws allows consumers to opt out of profiling. Of course, while some automated decisionmaking may involve profiling, profiling does not always constitute automated decisionmaking.

In the CPA rules, the Attorney General defines the terms “Human Involved Automated Processing”, “Human Reviewed Automated Processing”, and “solely automated processing” to

³⁴ General Data Protection Regulation, Article 22 (1), <https://gdpr-info.eu/art-22-gdpr/>

³⁵ Patrice Alexander Ficklin, Tom Pahl, and Paul Watkins, Innovation spotlight: Providing adverse action notices when using AI/ML models, Consumer Financial Protection Bureau, (July 7, 2020), <https://www.consumerfinance.gov/about-us/blog/innovation-spotlight-providing-adverse-action-notices-when-using-ai-ml-models/>

³⁶ Consumer Financial Protection Bureau, CFPB Acts to Protect the Public from Black-Box Credit Models Using Complex Algorithms (May 26, 2022), <https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/>

differentiate between different circumstances in which the right to opt out of profiling should apply.³⁷ This conception appears to have been drawn from the GDPR, which only grants opt-out rights when legal or similarly significant decisions are “solely” automated.

Though the CPA and GDPR relieve controllers of their opt out responsibilities when a human is involved with an automated process, we question at what level humans can be meaningfully involved in the outcome of more complicated algorithmic processes. In other words, the weight we should apply to human involvement is highly dependent on context. A growing corpus of scholarship has found that humans, even those technically empowered to intervene in automated processes, often cannot do so effectively.³⁸ This can occur for a multitude of reasons, but perhaps most vexingly of all is the “black box” problem, where a human may indeed consider the data used in the processing and have the authority to change a result once the processing occurs, but simply possesses no understanding of how the automated process arrived at the conclusion that it did. This problem plagues even the most technically-attuned humans in the loop, including engineers of the systems themselves, and will only worsen as automated processes become more sophisticated.³⁹

In deference to the growing complexity of algorithmic systems, we urge CPPA to define automated decisionmaking broadly and apply opt out rights even when a human is technically “in the loop.”

b. To what degree are these laws, other requirements, frameworks, or best practices aligned with the requirements, processes, and goals articulated in Civil Code § 1798.185(a)(16)?

CPRA's conception of automated decisionmaking shares much with GDPR and diverges somewhat from other state privacy laws. Like GDPR, CPRA clearly paves the path for both a right to opt out of automated decisionmaking, as well as access rights that “include meaningful information about the logic involved in those decision making processes, as well as a description of the likely outcome of the process with respect to the consumer.” VCDPA and CTDPA do not include similar requirements that businesses share information about the logic of the algorithm or its likely outcomes.

Though the text of CPA unfolds in much the same way as the other two state laws, the recently finalized CPA rules do require businesses that profile consumers to provide in their privacy

³⁷ Colorado Department of Law, Consumer Protection Section, Colorado Privacy Act Rules 4 CCR 904-3, Section 2.02, (March 2023), <https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf>

³⁸ See, e.g., Brennan-Marquez, Kiel and Susser, Daniel and Levy, Karen, Strange Loops: Apparent versus Actual Human Involvement in Automated Decision-Making (October 2, 2019). 34 Berkeley Technology Law Journal 745–771 (2019), <https://ssrn.com/abstract=3462901>

³⁹ Will Knight, The Dark Secret at the Heart of AI, MIT Technology Review, (April 11, 2017), <https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/>

policy “[a] non-technical, plain language explanation of the logic used in the Profiling process.”⁴⁰ The CPA rules also clarify that a business must disclose, “[t]he benefits and potential consequences of the decision based on the Profiling,” which bears a resemblance to CPRA’s “likely outcomes” provision.⁴¹

Moreover, under the CPA rules, businesses that profile consumers must include in their data protection assessments “[a]n explanation of the training data and logic used to create the Profiling system, including any statistics used in the analysis, either created by the Controller or provided by a Third Party which created the applicable Profiling system or software.”⁴²

c. What processes have businesses or organizations implemented to comply with these laws, other requirements, frameworks, and/or best practices that could also assist with compliance with CCPA’s automated decisionmaking technology requirements?
d. What gaps or weaknesses exist in these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? What is the impact of these gaps or weaknesses on consumers?

As a bare minimum, Consumer Reports believes automated decisions with legal or similarly significant effects should be explainable, and thus the Virginia and Connecticut laws appear to be weaker (barring future re-interpretation) than GDPR and CPA.

One weakness of all the state automated decisionmaking provisions compared to the GDPR is that those laws lack the right of contestation outlined in Article 22 of the GDPR. The right to contest substantially strengthens the right to an explanation; under such a regime, consumers can (theoretically, at least) use the information they have gleaned from a business’ explanation to provide countervailing documentation to contest and, perhaps, overturn an unjust decision.

At the same time, GDPR’s right to contest is only cursorily described in the text, which has given rise to questions about the feasibility of producing explanations detailed enough to render such a right to contest meaningful, especially in the case of complex machine learning algorithms.⁴³ Moreover, several years on from the implementation of GDPR, we still do not have a clear procedural understanding of what the right to contest looks like in practice.⁴⁴ Additionally, as with the right to explanation, the right to contest only exists when legal or similarly significant decisions are solely automated. In light of these limitations, some scholars have rejected the right to contest, and instead advocated for a “right to a well-calibrated machine” – in other

⁴⁰ Colorado Department of Law, Consumer Protection Section, Colorado Privacy Act Rules 4 CCR 904-3, Section 9.03, (March 2023), <https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf>

⁴¹ Ibid., Section 9.03 (A)(6)

⁴² Ibid., Section 9.06(F)(5)

⁴³ Margot Kaminski and Jennifer Urban, The Right to Contest AI, Columbia Law Review, Vol. 121, No. 7, 2021, (November 16, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3965041

⁴⁴ Ibid.

words, the right to unbiased and accurate automated decisionmaking systems.⁴⁵ In any case, we urge the CPPA to think broadly about what access rights may entail, including whether a right to contest may be appropriate and statutorily defensible.

e. What gaps or weaknesses exist in businesses or organizations' compliance processes with these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? What is the impact of these gaps or weaknesses on Consumers?

See above (*supra* Section 3, Question 3(d)) – relative to the right to contest in GDPR, it is arguable that the law does not provide a clear road map to compliance. Relative to the right to explainability, it is unclear whether existing law and enforcement has incentivized businesses to create the framework for meaningful explainability relative to more complex automated decisionmaking processes.

On top of access and opt out rights, Consumer Reports has previously advocated for algorithms to be auditable.⁴⁶ While explainability mandates may get us part of the way there, independent, and standardized third-party audits for companies whose algorithms pose significant legal effects are likely a more direct way of improving our understanding of algorithmic processes.

In addition to laws that require companies using AI to undergo independent, rigorous third-party audits, public interest researchers can play a vital role in uncovering the harms caused by algorithmic decision-making. We've advocated for several policy solutions to make public interest auditing easier.⁴⁷

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?

See above (*supra* Section 3, Question 3(d)).

4. How have businesses or organizations 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.

⁴⁵ Aziz Huq, A Right to a Human Decision, Virginia Law Review, Vol. 106, No. 3, (May 1, 2020), <https://virginialawreview.org/articles/right-human-decision/>

⁴⁶ Nandita Sampath, "Opening Black Boxes: Addressing Legal Barriers to Public Interest Algorithmic Auditing," Consumer Reports, (October 2022), https://digital-lab-wp.consumerreports.org/wp-content/uploads/2022/10/CR_Algorithmic_Auditing_Final_10_2022VF2.pdf

⁴⁷ Ibid.

Algorithms are increasingly used to supplement or replace human decisionmaking, and in some cases they are touted as being more objective and thorough than a human decisionmaker.⁴⁸ However, an algorithm is only as good as the engineer who designs it and the data it is trained on—human error, including biased data collection methods and the type of algorithm that is chosen by the engineer, can also cause bias. No algorithm will ever be perfect, because a model is a simplified version of real-world events. Most algorithms make mistakes — or are more accurate on certain groups than others⁴⁹ — due to these errors during the design process. This can cause real harm when the algorithm is used by a government, school, workplace, or even a landlord.⁵⁰

As mentioned in Section 2, Question 2, employers are using facial recognition algorithms to analyze the emotional states of interviewees and spy on employees. Hospitals use algorithms to assign to patients risk scores that can determine their ability to receive certain treatments. Landlords have used automated tenant screening reports (which include an algorithmically generated score) to make determinations about potential tenants.⁵¹ In the criminal justice system, risk assessments have been used to, among other things, quantify a defendant's future risk of misconduct to determine whether they should be incarcerated before their trial.⁵²

Companies like these are typically not required to disclose how their algorithms work, how they trained them, what issues they identified with their technology, and what steps they took to mitigate harm.⁵³ Furthermore, people usually do not know how the algorithm works on others, so it could be difficult for them to even identify whether they were discriminated against (for example, a woman who is rejected for a job by a resume-screening algorithm may not know that it allowed a man of similar experience to pass through).

In many cases, automated decisionmaking systems, which rely on large stores of data to run, exist on top of a foundation of improperly sourced data. Consumers who did not have the right to object to their personal data being used to train an algorithm are now being evaluated by that

⁴⁸ Rebecca Heilweil, "Artificial intelligence will help determine if you get your next job," Vox, (December 12, 2019), <https://www.vox.com/recode/2019/12/12/20993665/artificial-intelligence-ai-job-screen>; Sendhil Mullainathan, "Biased Algorithms Are Easier to Fix Than Biased People," The New York Times, (December 6, 2019), <https://www.nytimes.com/2019/12/06/business/algorithm-bias-fix.html>.

⁴⁹ The National Institute of Standards and Technology found that certain facial recognition algorithms were more likely to misidentify Asian and African American faces relative to Caucasians. "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects," National Institute of Standards and Technology: News, (December 2019), <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>

⁵⁰ There are entire books written about these issues, such as Weapons of Math Destruction by Cathy O'Neil (Crown Publishing Group, 2016) and Race After Technology by Ruha Benjamin (Polity, 2019).

⁵¹ Kaveh Waddell, "How Tenant Screening Reports Make It Hard for People to Bounce Back From Tough Times," Consumer Reports, (March 11, 2021), <https://www.consumerreports.org/algorithmic-bias/tenant-screening-reports-make-it-hard-to-bounce-back-from-toughtimes-a2331058426>.

⁵² Alex Chohlas-Wood, "Understanding risk assessment instruments in criminal justice," Brookings Institution, (June 19, 2020), <https://www.brookings.edu/research/understanding-risk-assessment-instruments-in-criminal-justice>.

⁵³ Hannah Bloch-Wehba, "Transparency's AI Problem," Knight First Amendment Institute at Columbia University, (June 17, 2021), <https://knightcolumbia.org/content/transparencys-ai-problem>.

same algorithm. Recent settlements at the FTC that use the “algorithmic disgorgement” remedy imply that the Commission is coming to a similar understanding. That type of improper collection and subsequent usage should be thought of as a privacy invasion in and of itself.

5. What experiences have consumers had with automated decisionmaking technology, including algorithms? What particular concerns do consumers have about their use of businesses’ automated decisionmaking technology? Please provide specific examples, studies, cases, data, or other evidence of such experiences or uses when responding to this question, if possible.

See above (*supra* Section 3, Question 4 and Section 2, Question 2).

6. How prevalent is algorithmic discrimination based upon classifications/classes protected under California or federal law (e.g., race, sex, and age)? Is such discrimination more pronounced in some sectors than others? If so, which ones? Please provide specific examples, studies, cases, data, or other evidence of such discrimination when responding to this question, if possible.

See above (*supra* Section 2, Question 2) for examples.

While some types of data are more capable of serving as proxies on their own due to historical injustices (i.e. location data), another risk that increases along with the ability of firms to process enormous data sets is the risk of businesses combining many small data points to create a profile for a person that implicitly reveals or exploits protected traits. Moreover, even when there is no intention to discriminate, black box algorithms can produce discriminatory results by replicating patterns of inequity that are already present in societal data inputs. This segmentation is often done through algorithms that are inherently difficult for external observers to test and hold accountable — especially when companies take affirmative measures to frustrate researchers testing for potential bias.

7. How can access and opt-out rights with respect to businesses’ use of automated decisionmaking technology, including profiling, address algorithmic discrimination?

Opt out rights may reduce instances of algorithmic discrimination if fewer individuals are subject to automated decisions, but on their own those rights will not eliminate the ability of algorithms to discriminate. Access and explainability rights supplemented with a right to contest could also reduce discrimination if consumers are able to leverage knowledge of an algorithm’s logic or inputs to refute its decisions as discriminatory.

Ideally consumers should not be forced to take action to “opt out” of algorithmic discrimination or contest discriminatory decisions on an individual basis - discriminatory technologies should be clearly prohibited through law. Consumer Reports has previously advocated for

anti-discrimination provisions in ADPPA and included similar provisions in our model state privacy act that use a disparate impact analysis.⁵⁴

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?

Consumer Reports believes all consumer rights, including access and opt-out rights relating to automated decisions with legal or similarly significant effects, should apply as broadly as possible. See above (*supra* Section 2, Question 3(a)) for our view on the difficulties of differentiating between “risky” and “non-risky” technologies.

9. What pieces and/or types of information should be included in responses to access requests that provide meaningful information about the logic involved in automated decisionmaking processes and the description of the likely outcome of the process with respect to the consumer? In addition:

a. What mechanisms or frameworks should the Agency use or require to ensure that truly meaningful information is disclosed?

b. How can such disclosure requirements be crafted and implemented so as not to reveal a business or organization's trade secrets?

10. To the extent not addressed in your responses to the questions above, what processes should be required for access and opt-out rights? Why?

See above (*supra*, Section 3, Question 3 (c)) for a discussion on the difficulties of producing meaningful information about the logic of automated decisionmaking processes.

We thank the California Privacy Protection Agency for its consideration of these points, and for its work to secure strong privacy protections for consumers. We are happy to answer any questions you may have, and to discuss these issues in more detail. Please contact Matt Schwartz ([REDACTED]) or Justin Brookman ([REDACTED]) for more information.

⁵⁴ Consumer Reports, Model State Privacy Act, (Feb. 2021), Sections 126 and 127, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf .

From: Nate Haderlie [REDACTED]
Sent: Monday, March 27, 2023 3:06 PM
To: Regulations
Subject: PR 02-2023 - Group letter of concern
Attachments: Alliance letter on CPPA ADM Regs 3-27.pdf

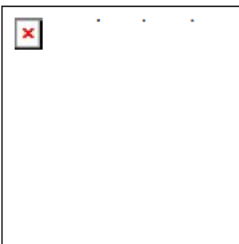
WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello,

Please see the attached letter signed by more than sixty business organizations from across California that expresses their concerns pertaining to rulemaking on automated decision making.

Thank you for allowing public comment, and we look forward to working with you.

Thanks,



Nathan Haderlie

Sr. Account Executive



[Website](#) |





March 27, 2023

California Privacy Protection Agency

Sacramento, CA 95814

Dear California Privacy Protection Agency Board Members and Staff,

Thank you for the opportunity to weigh in on the rulemaking process as it relates to cybersecurity audits, risk assessments, and automated decision making (ADM). On behalf of the organizations listed below and our members, we are writing to express our concerns as it specifically relates to rulemaking focused on ADM.

Our business community understands the importance of the work you are doing to protect consumers' privacy and personal information but as we have stated several times in the past, we are concerned that the harmful disruptions it may cause for all internet users in California. We highly encourage the Agency to do a thorough analysis of the potential consequences, before developing new regulations to ensure they do not do more harm than good. And, as a larger request, we ask that you support the business community in its effort to comply by providing guidance on how to adhere to these highly technical laws and regulations.

The undersigned businesses and our members use technologies that enable automated decision-making processes, such as customer relationship management, marketing automation, inventory management, financial management, human resources, production monitoring, to provide valuable services to create a convenience for our consumers every day. These technologies span across many different business operations areas for both small and large sized businesses and provide the following benefits:

- Ability to analyze large amounts of data quickly and accurately, which can lead to enhanced experiences and outcomes for customers, such as improved customer service, lower costs, increased transactional efficiencies, and better product/service recommendations.
- Greater accessibility for vulnerable populations particularly important for consumers with disabilities or other special needs by increasing accessibility.
- Personalized recommendations and automated processes that make it easier to find and purchase goods and services that meet their specific needs is crucial and must stay intact.
- Assists small businesses with data protection, using software that allows them to detect and respond to cybersecurity risks.

We encourage the Board members and staff to work collaboratively with businesses to develop standards and best practices that can ensure the fair and responsible use of these technologies and provide support businesses in their efforts to comply. This approach can help to protect consumers while also promoting innovation and business growth in California.

In conclusion, we ask that you carefully consider the potential impact of new regulations on automated decision making and to work with businesses to develop reasonable, effective solutions that protect consumers' privacy while preserving the value of ADM for consumers and the business community.

Thank you for your attention to this important issue.

Sincerely,

Asian Industry Business to Business
Associated Builder and Contractors Northern California
Automotive Service Councils of California
Bay Area Council
Beverly Hills Chamber of Commerce
BuildOUT California
Burbank Chamber of Commerce
California African American Chamber of Commerce
California Asian Chamber of Commerce

California Association of Parks & Attractions
California Association of REALTORS
California Autobody Association
California Automotive Business Coalition
California Beer & Beverage Distributors
California Black Chamber of Commerce
California Builders Alliance
California Business Roundtable
California Chamber of Commerce
California Craft Brewers Association
California Delivery Association
California Farm Bureau Association
California Food Producers
California Fuels and Convenience Association
California Golf Course Owners Association
California Hispanic Chambers of Commerce
California Hotel and Lodging Association
California Lodging Industry Association
California Manufacturers & Technology Association
California new Car Dealers Association
California Restaurant Association
California Small Business Association
California Tire Dealers Association
California Urban Partnership
Coalition of Small & Disabled Veteran Businesses
Culver City Chamber of Commerce
Danville Area Chamber of Commerce
Downtown San Diego Partnership
Family Business Association of California
Flasher Barricade Association
Folsom Chamber of Commerce
Glendale Chamber of Commerce
Golden Gate Business Association
Golden Gate Restaurant Association
Greater Arden Area Chamber of Commerce
Independent Automotive Professionals Association
Inland Empire Economic Partnership
Latin Business Association
Long Beach Chamber of Commerce
Los Angeles County Business Federation
National Association of Women Business Owners

National Federation of Independent Business
Orange County Business Council
Orange County Hispanic Chamber of Commerce
Sacramento Region Builders Exchange
San Juan Capistrano Chamber of Commerce
Santa Monica Chamber of Commerce
SCALE Health
Slavic American Chamber of Commerce
Small Business California
United Chamber Advocacy Network
United Chambers of Commerce of the San Fernando Valley
Valley Industry Commerce Association
Western Steel Council

From: Lucy Chinkezan [REDACTED]
Sent: Monday, March 27, 2023 3:12 PM
To: Regulations
Subject: PR 02-2023
Attachments: CJAC Comments on Cybersecurity Audits, Assessments, ADS - 3-27-23.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

California Privacy Protection Agency
Attn. Kevin Sabo
2101 Arena Blvd., Sacramento, CA 95834
regulations@coppa.ca.gov

Dear CPPA:

The Civil Justice Association of California hereby submits its comments on the CPPA's proposed rulemaking on relating to cybersecurity audits, risk assessments, and automated decisionmaking for your consideration.

Lucy Chinkezan
Counsel
Mobile [REDACTED] | www.cjac.org





March 27, 2023

Sent via email

California Privacy Protection Agency
Attn. Kevin Sabo
2101 Arena Blvd., Sacramento, CA 95834
regulations@coppa.ca.gov

Re: *Comments by the Civil Justice Association of California on Proposed Rulemaking – Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking*

Dear California Privacy Protection Agency Board:

The Civil Justice Association of California¹ appreciates the opportunity to provide comments to the California Privacy Protection Agency ("Agency") on proposed regulations under the California Privacy Rights Act of 2020 (CPRA).

Below we respectfully provide comments on behalf of our membership in response to the Agency's Invitation for Preliminary Comments on Proposed Rulemaking – Cybersecurity Audits, Risk Assessments, And Automated Decisionmaking. While we appreciate the agency's commitment to consumer protection in these areas, we urge the Agency to refrain from being overly prescriptive in its regulations as many businesses already apply rigorous auditing and data protection practices and adhere to numerous existing laws and industry standards. In this vein, the recommendations below will help to avoid overly broad regulations that drive up costs and burdens for both the state and businesses.

I. Cybersecurity Audits

- 1. What laws that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require cybersecurity audits? For the laws identified:**

- a. To what degree are these laws' cybersecurity audit requirements aligned with the processes and goals articulated in Civil Code § 1798.185(a)(15)(A)?**

¹ CJAC is a more than 40-year-old nonprofit organization representing a broad and diverse array of businesses and professional associations. A trusted source of expertise in legal reform and advocacy, we confront legislation, laws, and regulations that create unfair litigation burdens on California businesses, employees, and communities.

- b. What processes have businesses or organizations implemented to comply with these laws that could also assist with their compliance with CCPA's cybersecurity audit requirements?
- c. What gaps or weaknesses exist in these laws for cybersecurity audits? What is the impact of these gaps or weaknesses on consumers?
- d. What gaps or weaknesses exist in businesses' compliance processes with these laws for cybersecurity audits? What is the impact of these gaps or weaknesses on consumers?
- e. Would you recommend that the Agency consider the cybersecurity audit models created by these laws when drafting its regulations? Why, or why not?

Answer:

There are various existing laws and regulations that require cybersecurity audits of businesses processing consumers' personal information. These include the following. We defer to other industry groups and organizations who have industry-specific or state-specific expertise in these laws to address particulars:

- **General Data Protection Regulation (GDPR):** Enforces requirements through audits, the frequency of which depends on the size of the organization and the sector it operates in.²
- **Gramm-Leach-Bliley Act (GLBA):** Enforces requirements through annual compliance audits.
- **Federal Trade Commission Safeguards Rule³:** Ensures covered entities safeguard customer information including conducting risk assessments.
- **The National Association of Insurance Commissioners Insurance Data Security Model Law:** Establishes data security standards for insurers and other entities licensed by a state department of insurance.
- **New York Department of Financial Services (NYDFS) Cybersecurity Regulation:** Code Section 500.06: Provides, in part – Audit Trail. (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.⁴

² REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 Article 58.

³ 16 CFR Part 314

⁴ NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES 23 NYCRR 500 CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES.

- **Virginia Consumer Data Protection Act (VADPA):** Code Section 59.1-580C: Provides, in part, that the Attorney General may request, pursuant to a civil investigative demand, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General.⁵

As a general matter, we urge the Agency to provide clear and objective bases for any audits under CCPA and CPRA ("CCPA") and to establish limits as to when and how they will be conducted. Without these, audits could be unproductive and unnecessarily drain resources, and could also lead to unwarranted fishing expeditions.

Furthermore, as discussed below, we urge conformity with existing laws, recognition of current industry standards, and utilization of business self-audits as foundational elements of CCPA audit rules to avoid duplication and unnecessary costs and burdens on businesses already exercising robust cybersecurity audit practices.

2. In addition to any legally required cybersecurity audits identified in response to question 1, what other cybersecurity audits, assessments, or evaluations that are currently performed, or best practices, should the Agency consider in its regulations for CCPA's cybersecurity audits pursuant to Civil Code § 1798.185(a)(15)(A)? For the cybersecurity audits, assessments, evaluations, or best practices identified:
 - a. To what degree are these cybersecurity audits, assessments, evaluations, or best practices aligned with the processes and goals articulated in Civil Code § 1798.185(a)(15)(A)?
 - b. What processes have businesses or organizations implemented to complete or comply with these cybersecurity audits, assessments, evaluations, or best practices that could also assist with compliance with CCPA's cybersecurity audit requirements?
 - c. What gaps or weaknesses exist in these cybersecurity audits, assessments, evaluations, or best practices? What is the impact of these gaps or weaknesses on consumers?
 - d. What gaps or weaknesses exist in businesses or organizations' completion of or compliance processes with these cybersecurity audits, assessments, evaluations, or best practices? What is the impact of these gaps or weaknesses on consumers?
 - e. Would you recommend that the Agency consider these cybersecurity audit models, assessments, evaluations, or best practices when drafting its regulations? Why, or why not? If so, how?
3. What would the benefits and drawbacks be for businesses and consumers if the Agency accepted cybersecurity audits that the business completed to comply with the laws identified in question 1, or if the Agency accepted any of the other cybersecurity audits, assessments, or evaluations identified in question 2? How would businesses demonstrate to the Agency that such cybersecurity audits,

⁵ Code of Virginia § 59.1-580 C.

assessments, or evaluations comply with CCPA's cybersecurity audit requirements?

Answer:

- The Agency should allow annual self-certification to the Agency in line with other existing laws, such as NYDFS.
- For data processing that is already the subject of another audit such as Payment Card Industry (PCI) or Sarbanes-Oxley Act (SOX), then the existing audit should satisfy CCPA requirements.
- The Agency should provide businesses with options from which they can select to prove compliance with audit requirements, such as certifications by PCI, National Institute of Standards and Technology (NIST), or International Organization for Standardization (ISO). For example, storage of payment cards on file is regulated by the PCI Data Security Standard and is subject to annual certifications.
- Businesses should also be permitted to use available certifications and audits related to cybersecurity from service providers to help meet their requirements to conduct cybersecurity audits and provide risk assessments.
- Any audits required by the Agency should not be annual. Every 2-3 years should suffice.

4. With respect to the laws, cybersecurity audits, assessments, or evaluations identified in response to questions 1 and/or 2, what processes help to ensure that these audits, assessments, or evaluations are thorough and independent? What else should the Agency consider to ensure that cybersecurity audits will be thorough and independent?

Answer:

- The Agency should allow companies to rely on reasonable industry standards to satisfy CCPA requirements.
- Businesses should not be required to use third party auditors as the burden and expense would be excessively disproportionate to any downstream consumer benefit, and the likely result will be increased consumer costs. Moreover, third party audits can result in increased security risks due to exposure of data and confidential security practices.
- Instead, companies should be permitted to rely on internal entities that meet industry safeguards establishing independence. Many businesses have self-audit mechanisms and other internal standards and protocols based on exacting industry standards. Larger businesses often have internal teams that are separate from other business units and exist solely to conduct audits. These teams are designed to be independent and provide accountability.

5. What else should the Agency consider to define the scope of cybersecurity audits?

Answer:

- The Agency should clearly define what type of processing creates a significant risk, preferably by limiting the types of personal information to which the audit requirement applies in the same manner as other sector-specific laws. For example, NYDFS limits audits to specific types of personal information such as payments data.
- Requiring businesses to conduct audits for lower risk information that is not subject to audits by any other laws would be very costly while providing minimal consumer benefit.
- The Agency should also consider confining audits to situations where there is reasonable suspicion of possible violations and audit businesses only, not individuals.
- The Agency should provide reasonable notice of any audits and incorporate flexibility and a range of enforcement mechanisms into the regulations as other California enforcement bodies have done. For example, the California Public Utilities Commission implements progressive enforcement, beginning with actions such as a notice or warning and only later in the process may impose penalties or file a civil or criminal action. This process may not apply if the violation is egregious or widespread.
- The Agency's rules should provide protections for such risk assessments conducted under attorney-client privilege or self-evaluative privilege. If such assessments must be submitted to the agency, companies should not be required to waive any attorney-client privilege. For example, the Virginia DPA makes specific mention that a company providing data protection assessment does not waive the attorney-client privilege or work product protection.⁶
- Companies should also be able to protect trade secrets or proprietary information from disclosure to other companies or to the public when turning over assessments to the Agency.

II. Risk Assessments

1. What laws or other requirements that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require risk assessments? For the laws or other requirements identified:

⁶ Code of Virginia § 59.1-580 C.

- a. To what degree are these risk-assessment requirements aligned with the processes and goals articulated in Civil Code § 1798.185(a)(15)(B)?
- b. What processes have businesses or organizations implemented to comply with these laws, other requirements, or best practices that could also assist with compliance with CCPA's risk-assessments requirements (e.g., product reviews)?
- c. What gaps or weaknesses exist in these laws, other requirements, or best practices for risk assessments? What is the impact of these gaps or weaknesses on consumers?
- d. What gaps or weaknesses exist in businesses' or organizations' compliance processes with these laws, other requirements, or best practices for risk assessments? What is the impact of these gaps or weaknesses on consumers?
- e. Would you recommend the Agency consider the risk assessment models created through these laws, requirements, or best practices when drafting its regulations? Why, or why not? If so, how?

Answer:

As noted under I above, there are a variety of global, federal, and state laws governing cybersecurity audits to which businesses may already be subject. To the extent possible, there should be consistency with other applicable requirements to prevent unnecessary burdens and costs.

2. What harms, if any, are particular individuals or communities likely to experience from a business's processing of personal information? What processing of personal information is likely to be harmful to these individuals or communities, and why?
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?
 - b. What other models or factors should the Agency consider? Why? How?
 - c. Should the models or factors be different, or assessed differently, for determining when processing requires a risk assessment versus a cybersecurity audit? Why, or why not? If so, how?
 - d. What processing, if any, does not present significant risk to consumers' privacy or security? Why?

Answer:

- From a privacy risk perspective, risk assessments should be limited to processing that has a legal or similarly significant effect on an individual, i.e., where it materially affects a decision that will impact housing, education, employment and other areas protected from discrimination under the law, or where there has been a material breach of information regulated by the statute, or confirmed

collection, use, sharing of data inconsistent with what is disclosed in privacy notices.

- From a security risk perspective, risk assessments should be limited to processing of data that, if compromised, is likely to result in real, concrete harms to individuals. Examples may include identity theft/fraud, extortion, or physical injury from disclosure of intimate or other objectively sensitive personal details (e.g., sexual orientation).
- Processing of personal information in any context for fraud prevention or to otherwise prevent unlawful activity or comply with legal obligations should be exempted from the scope of risk assessments. These activities protect consumers' privacy and security and often apply data protection measures like pseudonymizing or encrypting that significantly reduce processing risks. Requiring any disclosure of these activities can allow bad actors to gain access to companies' internal systems.
- In the employment context, regular risk assessments relating to the processing of personal information should not be required because the processing of most personal information does not present a "significant risk to [employees'] privacy or security." If the Agency does require regular risk assessments, they should be limited to the following:
 - (1) specific categories of sensitive personal information or instances where sensitive personal information is collected and processed for the purpose of inferring characteristics about a consumer; and
 - (2) specific types of processing that present a significant risk.
- Any rules for risk assessments in the employment context should also take into account the relationship between employees or independent contractors and businesses—including: (a) existing state and federal laws that require businesses to collect and retain employment related records for compliance, reporting and benefits purposes; (b) whether the personal information is collected and processed solely within the HR context; and (c) the burden associated with regular risk assessments relating to the processing of personal information collected and used solely within the HR context.

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

a. What would the benefits and drawbacks be if the Agency considered the data protection impact assessment content requirements under GDPR and the Colorado Privacy Act?

Answer:

- Any data protection impact assessment (DPIA) requirements should be detailed enough for the business and the regulator to understand the risks being addressed. However, it should not be so prescriptive

or specific so that businesses do retain sufficient flexibility and can scale existing processes.

- The Agency should consider adopting an approach that aligns with the EU's Article 29 Data Protection Working Group Report (2017): "The GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit with existing working practices. There are a number of different established processes within the EU and worldwide which take account of the components described in recital 90. However, whatever its form, a DPIA must be a genuine assessment of risks, allowing controllers to take measures to address them."
- The DPIA should be viewed as a documentation requirement rather than a substantive requirement to mitigate or fix any identified risk. The DPIA should also be limited to the actual processing of data — it should not be used as a proxy to require a risk assessment of the feature itself as distinct from any processing of data that occurs as part of that feature.
- The Agency should permit a single risk assessment to cover multiple related types of data processing activities.
- Assessments should not be required for Personal Identifiable Information (PII) or any other information not regulated by the CCPA.
- Finally, regulators should be encouraged, if not required, to use independent experts to review any submitted Assessment.

b. What, if any, additional content should be included in risk assessments for processing that involves automated decisionmaking, including profiling? Why?

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?

Answer:

- The regulations should recognize that risk assessments are an increasingly common requirement under U.S. and international privacy and data protection laws. To promote interoperability and minimize burdens to covered businesses, the regulations should specify that the Agency will accept risk assessments that were originally conducted pursuant to a comparable legal requirement.
- Privacy obligations and risk balancing should also be consistent across jurisdictions relating to the same requirements. As such, we suggest aligning with any data impact or risk assessments required under other similar laws, such as the CPA and VCDPA.

- For example, under the VCDPA framework for risk assessments, the statute specifies triggers for risk assessments, requires the regulatory agency to weigh the benefits to all stakeholders (including consumers) versus risks to consumer rights, and factors in the use of deidentified data.
- However, the Agency should be wary of adopting in full any future regulatory guidance under other laws, including the GDPR. European Union case law is evolving in unpredictable ways, and California should develop guardrails that would ensure that the any future obligations on California businesses are appropriately balanced against any potential burden.
- The Agency should strive for consistency across jurisdictions as this will allow businesses to continue to innovate and build robust systems to protect consumers' information.

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?**

Answer:

- The Agency should first clarify that its function under the statute to provide "a public report summarizing the risk assessments filed with the agency" refers to the risk assessments identified in 1798.185(15)(b). The statute appears to refer in error to 1798.185(15)(a), which concerns cybersecurity audits.
- As to (a)(i), risk assessments should highlight the most significant privacy risks associated with the processing activity in question and the steps being taken to address and mitigate that risk. They should not require the company to divulge commercially sensitive information or sensitive security information, such as details about technical safeguards that would allow a bad actor to compromise the company's security practices.
- With respect to (a)(ii), the Agency should not overly prescribe the format in which the business must submit the risk assessment. Businesses may prepare and record assessments in different ways and for different jurisdictions, and so they need flexibility to submit the assessment without having to alter the format or content to match California-specific requirements.

- As for (a)(iii), the Agency should only require businesses to “regularly submit” assessments for new or materially changed processing practices that present a significant risk. If the Agency requires periodic updates absent any change, then such updates should not occur more frequently than once every three years. Anything more frequent will be overly burdensome and costly, particularly for small and medium sized businesses, and could incentivize businesses to treat risk assessments as a mere ‘check-the-box’ compliance exercise.

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)?

7. Should the compliance requirements for risk assessments or cybersecurity audits be different for businesses that have less than \$25 million in annual gross revenues? If so, why, and how?

Answer:

Yes. As noted above, small and medium businesses have fewer resources than larger businesses, so the Agency should be sensitive to disproportionate impacts on these businesses if requirements and assessments are too prescriptive, rigid, broad, or frequent.

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

Answer:

- The regulations should provide factors that balance benefits of processing with potential risks, including:
 - Technical and organizational measures and safeguards implemented by the business to mitigate privacy and security risks;
 - The reasonable expectations of consumers; and
 - The context of the processing with respect to the relationship between the business and consumers.
- In the context of human resources, balancing factors considered by the regulations should include:
 - The differences in the relationship between employees or independent contractors and businesses in comparison to consumers and businesses;
 - Existing state and federal requirements which require businesses to collect, retain, and secure HR records for compliance, reporting and benefits purposes; and
 - The burden of regular risk assessments for the processing of personal information that is collected and used solely within the HR context or required by state and federal law.

- Agency rules should also include protections to ensure that businesses have the necessary confidence to use risk assessments to fully document and assess processing practices rather than being incentivized to treat assessments as a defensive measure against potential future litigation.
- The regulations should also clarify that risk assessments conducted pursuant to the CCPA protect trade secrets and proprietary information from public disclosure and are confidential and exempt from public inspection and copying under the California Public Records Act. Furthermore, submitting an assessment to the agency should not constitute a waiver of any attorney-client privilege or work-product protection.
- The Agency should not be permitted to use the submitted assessment as evidence of wrongdoing or used to penalize the business for weighing the risks in a way with which the Agency disagrees.

III. Automated Decisionmaking

1. What laws requiring access and/or opt-out rights in the context of automated decisionmaking currently apply to businesses or organizations (individually or as members of specific sectors)?

Answer:

- Since automation is a subset of decisionmaking, the Agency should take into account that existing laws (such as anti-discrimination frameworks) that govern how a company makes decisions generally would also apply to ADM.
- As noted earlier, companies in the US are subject to several existing privacy laws that already impose substantial obligations with respect to the consumer's right to opt out of automated decisionmaking. This includes the CO, CT, and VA state privacy laws. Importantly, each of these laws limits the opt-out right to high risk decisions, described as those which have "legal or similarly significant effects," and in the case of CT, target "solely" automated decisions.
- To ensure interoperability with those laws and to balance protection of consumers with access to important technology, the Agency should similarly establish in rulemaking that the profiling opt out is limited to all three of the following criteria:

1) Only to decisions with "legal or similarly significant effect"

The Agency should focus on high risk use cases, such as using technology to make final decisions regarding access to housing, medical benefits, or other critical services without appropriate human involvement. For example, under the VA privacy law, decisions with legal or similarly significant effect is defined as "a decision made by the controller that results in the provision or

denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.”

Conversely, the Agency should not regulate low-risk automated decisionmaking technology such as spell check, GPS systems, and transcription services. Doing so could interfere with their function while providing little meaningful benefit to consumers.

2) Only to decisions that are solely or fully automated

This limitation avoids creating an unreasonable obligation on businesses, without impacting the right of a consumer to have their decisions assessed by a human.

3) Only after the final automated decision is made

This limitation is important for several reasons. First, any opt-out right that is pre-final decisions could result in significant costs and delays for businesses and consumers. If a manual human step is required, companies might not be able to support the same number of requests without incurring unreasonable expenses. For example, individuals receive faster access to services if businesses can quickly identify low fraud risks.

Second, a pre-decision opt out right provides consumers with little added benefit beyond what a post-decision opt out provides. For example, if consumers apply for a loan and have a positive outcome on the first automated decision, they likely will not want or need to opt-out but would have the right to do so. If the outcome is negative, they can still contest that decision or request a new decision. Under a pre-decision opt out scenario, these decisions could take several days to process rather than several seconds which will likely pose a greater burden to the consumer.

- Finally, in the event that any required opt-out right that is required by the Agency interferes with the ability of a company to deliver products or services, the company should be allowed to apply a price increase based on the actual cost differential.

2. What other requirements, frameworks, and/or best practices that address access and/or optout rights in the context of automated decisionmaking are being implemented or used by businesses or organizations (individually or as members of specific sectors)?

Answer:

- Companies typically do not have requirements, frameworks, or best practices that address access or opt-outs related to low-risk, every day technology, such as spellcheck of documents.

- Access or opt out rights for these types of automated decisions would slow down business substantially with no benefit to consumers. For example, businesses do not typically give consumers the right to opt out of using optical character recognition on PDF documents containing that consumer's personal information. Regulations should not dictate how businesses operate routine, low-risk technology.
- To the extent that artificial intelligence (AI) and machine learning (ML) is used in high-risk automated decisionmaking, this is an area where robust requirements, frameworks, and best practices are continually being developed and deployed. For example, in recent years there has been a proliferation of AI/ML International Standards, such as those created by the International Organization for Standardization (ISO) and the U.S. National Institute of Standards and Technology (NIST).

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

a. How is "automated decisionmaking technology" defined? Should the Agency adopt any of these definitions? Why, or why not?

Answer:

- Industry needs a clear and specific definition of automated decisionmaking technology. The Agency should avoid a sweeping definition that captures all technology or software. It should instead focus the definition on systems that solely use machine learning to automate decisions that produce legal or similarly significant effects.
- Accordingly, we propose the following definitions:
 - Automated decisionmaking should be defined as: "Final decisions that are made solely/fully with AI/ML technology with legal or similarly significant effects."
 - AI/ML technology should be defined as: "The use of machine learning and related technologies that use data to train algorithms and predictive models for the purpose of enabling computer systems to perform tasks normally associated with human intelligence or perception, such as computer vision, natural language processing, and speech recognition."
- Industry also needs the Agency to provide concrete, real-world examples of what falls within the scope of these definitions.

b. To what degree are these laws, other requirements, frameworks, or best practices aligned with the requirements, processes, and goals articulated in Civil Code § 1798.185(a)(16)?

c. What processes have businesses or organizations implemented to comply with these laws, other requirements, frameworks, and/or best practices that could also assist with compliance with CCPA's automated decisionmaking technology requirements?

Answer:

To comply with GDPR, companies already allow EU customers to request review of certain fully automated decisions. Companies can extend that process to US customers as appropriate.

- d. What gaps or weaknesses exist in these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? What is the impact of these gaps or weaknesses on consumers?**
- e. What gaps or weaknesses exist in businesses or organizations' compliance processes with these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? 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?**

4. How have businesses or organizations 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.

Answer:

- Businesses in every industry sector use ADM to improve their competitiveness and enhance their product and service offerings.
- Uses of ADM can include routine and low-risk applications like spellcheck, book or song recommendations, or marketing by small businesses of its affordable products to the right consumers.
- With respect to artificial intelligence (AI) and machine learning (ML), adoption of AI is so widespread that a 2021 McKinsey and Company study found that 56% of business leaders across the globe use it in at least one business function. Most of these are low risk use cases such as service-or operations optimization, enhancement of products, and contact-center automation.
- The expansive use of AI for low risk use cases underscores the importance of limiting Agency rules to high-risk applications, consistent with other states.

5. What experiences have consumers had with automated decisionmaking technology, including algorithms? What particular concerns do consumers have about their use of businesses' automated decisionmaking technology? Please provide specific examples, studies, cases, data, or other evidence of such experiences or uses when responding to this question, if possible.

Answer:

- The Agency should take a very measured approach with giving opt-out rights in the case of automated activities. Automated technology

has major benefits for consumers and businesses, including improved accuracy, safety, and cost efficiencies. For certain high-risk service offerings automation may be a core component, making opt-outs infeasible. Examples are emergency response systems for injured consumers or fraud detection for bank and insurance transactions by consumers. Opt-out rights for these technologies could undo these benefits, increase the risk of harm to consumers, and hamper innovation that is highly advantageous to consumers.

- If high risk business offerings are essential or critical, and it is not reasonable for consumers to consider other options, the Agency should allow businesses to establish guardrails that protect the consumer rather than an opt-out right. Depending on the use case, guardrails could include establish criteria like rigorous testing, system monitoring, and consumer complaint processes.
- Automation may also be essential to products that involve less significant effects, but which nonetheless provide high value with minimal risk to consumers. Examples include routing of phone calls, travel alerts based upon traffic patterns in the consumer's location, or voice command services to select entertainment.
- Opt-out rights for these kinds of services could result in reduced accuracy and functionality and unnecessary interruptions. The Agency should take the same approach as other state privacy laws and limit profiling opt out to automation that has legal or similarly significant effects. Rules should also tailor the scope of legal or similarly significant effects to the specific harms the Agency is addressing, e.g., discrimination.

6. How prevalent is algorithmic discrimination based upon classifications/classes protected under California or federal law (e.g., race, sex, and age)? Is such discrimination more pronounced in some sectors than others? If so, which ones? Please provide specific examples, studies, cases, data, or other evidence of such discrimination when responding to this question, if possible.

7. How can access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling, address algorithmic discrimination?

Answer:

The rules should provide a safe harbor for businesses who use race, ethnicity, or other demographic data with user consent for the narrow purpose of evaluating and preventing bias. It is not possible to prevent bias without measuring the algorithm's impact on different user groups, including minority groups.

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?

Answer:

- Yes. Given the extensive and complex nature of automated decisionmaking (ADM) technology and profiling use cases, the Agency should defer to sector-specific regulations to address any concerns and specifically examine each sector in question.
- Any Agency rules for ADM technology should consider the parameters set out in response to Question III.1 above.
- The Agency should consider that requiring an opt-out right for some ADM use cases involving high-risk service offerings raises additional concerns. For example, it could interfere with emergency response systems or devices.
- The regulations should also recognize that some uses of ADM that produce legal or similarly significant effects may be highly beneficial to consumers and if turned off could create risk of harm. An example is fraud detection used for financial or insurance decisions.
- Any ADM rules should also recognize benefits of reducing human review that can lead to processing errors, improper disclosure or review of consumer personal data, or bias.
- To protect consumers' interests without hindering beneficial uses, the regulations should tailor the scope of "legal or similarly significant effects" to the specific harms in question.
- In the employment context, the profiling opt out should exclude automation involving individual data, because state and local laws are already being developed to specifically target the use of these technologies in the workplace. Additionally, nearly any decision relating to employment could have a "legal or similarly significant effect," including innocuous ADM like task allocation to enable efficiency.

9. What pieces and/or types of information should be included in responses to access requests that provide meaningful information about the logic involved in automated decisionmaking processes and the description of the likely outcome of the process with respect to the consumer? In addition:

- a. What mechanisms or frameworks should the Agency use or require to ensure that truly meaningful information is disclosed?
 - b. How can such disclosure requirements be crafted and implemented so as not to reveal a business or organization's trade secrets?
- 10. To the extent not addressed in your responses to the questions above, what processes should be required for access and opt-out rights? Why?**

Answer:

- Businesses should be able to satisfy consumer access requests with a general explanation of technology functionality via their public web page, rather than having to provide specific information about decisions made.
- Providing general criteria or categories of input for decision-making should suffice as “meaningful” information about the logic involved in a decision. Detailed descriptions of complex algorithms used in automated decisionmaking will not be “meaningful” to the average consumer and can result in violations of intellectual property, trade secrets, and other legal rights of businesses.
- Disclosure of fraud or security decision-making poses serious security risks providing a roadmap for fraudsters or bad actors to breach the system.
- As earlier noted, Agency rules should also protect businesses from having to disclose proprietary or trade secret information in response to consumer access requests.

10. To the extent not addressed in your responses to the questions above, what processes should be required for access and opt-out rights? Why?

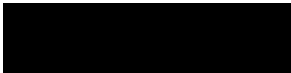
Answer:

- Agency rules should recognize differences between developer versus deployers of automated decision technology. Rules should not impose standalone obligations for consumer access requests or opt-outs on developers; instead they should only be required to provide “reasonable” assistance to deployers, e.g., with generally available documentation.
- Regulations concerning automated decisionmaking should include exceptions for access or opt out to avoid abuses or illegal activity, comply with law enforcement, respond to or protect consumers, or address research or errors. Colorado, Connecticut, and Washington have provided exceptions along these lines.

We appreciate the opportunity provide preliminary comments on this proposed rulemaking. It is in the Agency's and stakeholders' best interests to have a set of regulations which will facilitate compliance and help to avoid unnecessary and unproductive enforcement actions and litigation.

Thank you for your consideration, and we are happy to address any questions you have.

Respectfully submitted,

A solid black rectangular box used to redact the signature of the person submitting the comments.

Counsel

From: Tonsager, Lindsey [REDACTED]
Sent: Monday, March 27, 2023 3:19 PM
To: Regulations
Cc: Scott, Alexandra
Subject: PR 02-2023 Comments of the Entertainment Software Association (ESA)
Attachments: Comments of ESA.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Attached please find the comments of the Entertainment Software Association responding to the CPPA's Invitation for Preliminary Comments on Proposed Rulemaking on the following topics: cybersecurity Audits, Risk Assessments, and Automated Decisionmaking (PR 02-2023).

Best,
Lindsey Tonsager
Alex Scott
Counsel for the Entertainment Software Association

Lindsey Tonsager

Pronouns: She/Her/Hers

Covington & Burling LLP
Salesforce Tower, 415 Mission Street, Suite 5400
San Francisco, CA 94105-2533
T + [REDACTED] | [REDACTED]
www.cov.com

COVINGTON

This message is from a law firm and may contain information that is confidential or legally privileged. If you are not the intended recipient, please immediately advise the sender by reply e-mail that this message has been inadvertently transmitted to you and delete this e-mail from your system. Thank you for your cooperation.



March 27, 2023

Via Email

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

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

Dear Mr. Sabo:

The Entertainment Software Association (“ESA”)¹ submits these comments in response to the California Privacy Protection Agency’s (“CPPA”) Invitation for Preliminary Comments on Proposed Rulemaking on the following topics: cybersecurity audits, risk assessments, and automated decisionmaking.² ESA and its members appreciate the CPPA’s goal to “implement the [California Privacy Rights Act (“CPRA”)] in the most effective manner,” as well as the agency’s recognition of the overlap between the CPRA and existing legal frameworks.³

Consistent with this goal, ESA makes two overarching requests. First, ESA asks the CPPA to adopt regulations that align with the statutory text. That alignment is consistent with the agency’s goal and the agency’s authority under California law.⁴ Second, ESA requests that the CPPA issue regulations that promote interoperability with existing frameworks. That promotion is consistent with the statute’s stated purpose that “to the extent it advances consumer privacy and business compliance, the law should be compatible with privacy laws in other jurisdictions.”⁵ It also ensures that the regulations will not violate the CPRA by restricting a

¹ ESA is the U.S. association for companies that publish computer and video games for video game consoles, handheld devices, personal computers, and the internet. There are over 400 video game companies in the state of California.

² California Privacy Protection Agency, Invitation for Preliminary Comments on Proposed Rulemaking Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking (Feb. 10, 2023), https://cppa.ca.gov/regulations/pdf/invitation_for_comments_pr_02-2023.pdf (hereinafter, “Invitation”).

³ Invitation; 3-4, 6.

⁴ California agencies have the authority to adopt regulations that are “reasonably necessary to effectuate the purpose of the statute.” Cal. Gov’t Code § 11342.2. California Courts have expanded on this requirement, explaining that not only must the regulation adopted by an agency be necessary to effectuate the purpose of the statute, it also must be “consistent with and not in conflict with the enabling statute.” *In re Gadlin*, 31 Cal. App. 5th 784, 788, 243 Cal. Rptr. 3d 331, 334 (2019), *aff’d*, 10 Cal. 5th 915, 477 P.3d 594 (2020).

⁵ California Privacy Rights Act of 2020, § 3(C)(8), 2020 Cal. Stat. A-85.

business's ability to comply with federal, state, or local laws.⁶ Specifically, ESA requests that the CPPA issue regulations:

- Requiring businesses to conduct cybersecurity audits, only if the compromise of the personal information the business processes could trigger data breach notification requirements;
- Protecting sensitive cybersecurity audits and privacy risk assessments from Public Records Act ("PRA") requests;
- Permitting companies to rely on audits and privacy risk assessments conducted under other frameworks;
- Aligning the content requirements of privacy risk assessments and automated decisionmaking rights with existing laws;
- Giving businesses flexibility to assess risks; and
- Allowing businesses to protect consumers using automated decisionmaking.

ESA discusses each of these requests in further detail below. Section I details our requests for the regulations governing cybersecurity audits, section II explains our requests for the regulations governing privacy risk assessments, and section III includes our requests for the regulations governing automated decisionmaking.

I. The CPPA Should Issue Regulations Governing Cybersecurity Audits That Conform With Other California Laws And Industry Standards.

The Invitation asks several questions about how the CPPA should regulate cybersecurity audits. In particular, it solicits feedback regarding the current laws that apply to businesses' cybersecurity audits and industry practices regarding the same. The following sections identify California laws that are relevant to cybersecurity audits, as well as industry standards that can inform them. They also provide language that can align the CPRA regulations with both authorities.

A. The Regulations Should Specify That They Require Cybersecurity Audits, Not Cybersecurity Risk Assessments.

The CPRA should not require businesses to engage in both a cybersecurity audit and a cybersecurity risk assessment. Notably, the statute contemplates a risk assessment only to address "risks to privacy."⁷ In contrast, the statutory text is clear that "processing [that] may result in significant risk to the security of personal information" requires businesses to perform a "cybersecurity audit."⁸ Any interpretation requiring businesses to conduct a separate cybersecurity risk assessment in addition to a cybersecurity audit would be inconsistent with this

⁶ Cal. Civ. Code § 1798.145(a)(1).

⁷ Cal. Civ. Code § 1798.185(a)(15)(B).

⁸ Compare Cal. Civ. Code § 1798.185(a)(15)(A) with Cal. Civ. Code § 1798.185(a)(15)(B).

plain language.⁹ It also would afford consumers no incremental benefit. Consumers will not be more secure if a business identifies a cybersecurity vulnerability in a risk assessment and an audit. Instead, the regulations should require businesses to conduct a single cybersecurity audit, which permits businesses to prioritize protecting consumers from the cybersecurity issues they identify in that audit.

For these reasons, ESA urges the CPPA to issue the following regulation:

A business shall perform a cybersecurity audit and privacy risk assessment only. These regulations shall not be construed to require a business to perform a cybersecurity risk assessment.

B. The Regulations Should Require Businesses To Conduct Cybersecurity Audits Only When Processing Involves Personal Information Subject To Data Breach Notification Requirements.

The CPRA's annual cybersecurity audit requirements apply only to those businesses whose processing of personal information presents a significant risk to consumers' security. In identifying what processing may create such a risk, the CPPA must consider the nature and scope of processing activities.¹⁰ Because different processing activities involve different types of information, the CPPA must consider the types of personal information associated with each processing activity.

ESA requests that the CPPA clarify that a processing activity results in a significant risk to consumers' security only if it involves personal information, the compromise of which would trigger a data breach notification requirement under Cal. Civ. Code § 1798.82.¹¹ California's data breach notification law initially required companies to notify consumers only if they experienced a breach that put consumers at risk of identity theft.¹² However, over the years, the California legislature updated the law multiple times "in response to emerging threats and rapidly changing technology."¹³ Today, California's data breach notification law requires companies to issue notifications if they experience any incident that would present a significant risk to consumer's security — namely, if the compromised data could result in insurance fraud, disclosure of medical information, financial injury, or exposure of online accounts.

⁹ See, e.g., *Hernandez v. Dep't of Motor Vehicles*, 49 Cal. App. 5th 928, 935, 263 Cal. Rptr. 3d 500, 505 (2020) ("[W]e construe the words in question in context, keeping in mind the statute's nature and obvious purposes. We must harmonize the statute's various parts by considering it in the context of the statutory framework as a whole.") (internal citations omitted).

¹⁰ Cal. Civ. Code § 1798.185(a)(15).

¹¹ Cal. Civ. Code § 1798.182.

¹² California Attorney General, Data Breach Report 2012 (2012), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2012data_breach_rpt.pdf?

¹³ California Attorney General, Data Breach Report 2016 (2016), <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf>.

Therefore, ESA asks that the CPPA adopt the following regulation:

A business shall conduct a cybersecurity audit of only those processing activities that involve personal information, as defined in subdivision (h) of Section 1798.82.

- C. The Regulations Should Specify That The Agency Will Withhold Cybersecurity Audits From Public Disclosure Consistent With The Public Records Act.

The CPRA permits the agency to subpoena the production of any items material to a business's compliance with the CPRA, which could include a cybersecurity audit.¹⁴ The CPRA requires members of the CPPA to "maintain the confidentiality of information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers, except to the extent that disclosure is required by the Public Records Act."¹⁵

The PRA permits agencies to withhold records when the public interest in not disclosing the record clearly outweighs any interest in disclosing it.¹⁶ The PRA includes non-exhaustive examples of records that are to be withheld; one of which is records for which disclosure "would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency."¹⁷ A business's cybersecurity audit might contain information about a business's cybersecurity vulnerabilities and what a business is doing to address them. Publishing these audits, therefore, similarly would reveal a business's cybersecurity vulnerabilities and how to exploit them, thereby increasing the potential for an attack on a business. That attack could result in bad actors gaining unauthorized access to both the business's system and the business's customers' personal information. Because disclosing the records of cybersecurity audits presents a significant risk of harm to both the business and its customers, the public interest in not disclosing the audit clearly outweighs the public interest in disclosing it. Accordingly, the regulations should specify that the PRA does not require the CPPA to disclose cybersecurity audits.

ESA asks the CPPA to adopt the following regulation, which tracks the PRA's language:

If a cybersecurity audit would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a business, the CPPA shall not disclose it in response to a request under Cal. Gov't Code § 7922.000, et seq.

¹⁴ Cal. Civ. Code § 1798.165.

¹⁵ Cal. Civ. Code § 1798.199.15(b).

¹⁶ Cal. Gov't Code § 7922.000.

¹⁷ Cal. Gov't Code § 7929.210.

D. The Scope Of The Cybersecurity Audit Regulations Should Conform With Existing Data Security Frameworks.

The CPRA requires the CPPA to define the scope of the audit in regulations.¹⁸ To address that requirement, the regulations should adopt a flexible approach that permits businesses to rely on the audit components of various established data security standards. For example, the Center for Internet Security publishes a list of the top 18 security controls that it recommends companies adopt; one of which requires developing a plan to continuously assess and track vulnerabilities.¹⁹ Another example of an established data security standard that requires assessments is the National Institute of Standards and Technology's Special Publication 800-53a. The California Attorney General's Office recognized both of these standards specifically; additionally, that office noted "there are a number of authoritative information security standards that organizations can and do use to develop their information security programs."²⁰ Other authoritative industry-standard protocols on which businesses rely include the National Institute of Technology's Risk Management Framework, ISO 27001, the annual attestations associated with the Payment Card Industry Standards, the Statement on Standards for Attestation Engagements no. 18, and System and Organization Controls 2.

Therefore, ESA asks the CPPA to adopt a regulation along the following lines:

A business may comply with its obligations to conduct a cybersecurity audit annually by executing the assessment requirement in industry-standard data security protocols, including, but not limited to, the National Institute of Standards and Technology's Special Publication 800-53a assessment, and Control 7 of the Center for Internet Security's Top 18 Controls.

II. The CPPA Should Align The Regulations Governing Privacy Risk Assessments With Existing Legal Frameworks.

The Invitation asks several questions about privacy risk assessments, including what content such assessments should include and whether other laws require them. ESA encourages the CPPA to adopt regulations that align with the statute's and other legal requirements for the content of risk assessments.

A. The Regulations Should Limit The Requirements Regarding The Content of Risk Assessments To Those In The Enabling Statute.

The CPRA specifies what risk assessments must include: whether the processing involves sensitive personal information, the benefits of the processing, and the potential risks to the rights

¹⁸ Cal. Civ. Code § 1798.185(a)(15).

¹⁹ Center for Internet Security; CIS Critical Security Control 7: Continuous Vulnerability Management (May 2021), <https://www.cisecurity.org/controls/continuous-vulnerability-management>.

²⁰ California Attorney General, Data Breach Report 2016 (2016), <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf>, 40.

of the consumer.²¹ The Invitation suggests that the CPPA might permit companies to submit a summary of their risk assessment instead of the actual risk assessment. ESA appreciates and supports this approach, which provides the agency sufficient information while balancing the need to protect trade secrets. The regulations should require the summary to include no more information than otherwise would be required under the enabling statute, but with less detail. To that end, ESA urges the CPPA to adopt a regulation along the lines of:

Any summary of a risk assessment shall be comprised of a statement whether the processing involves sensitive personal information, as well as a synopsis of whether the benefits from the processing to the business, the consumer, other stakeholders, and the public, are greater than the potential risks to the rights of the consumer.

The CPRA further states that nothing in the regulations “shall require a business to divulge trade secrets.”²² Accordingly, any regulations should reaffirm that statutory carve out. The CPPA should adopt the following regulation:

Nothing in these regulations shall require a business to divulge a trade secret.

B. The Regulations Should Give Businesses Flexibility To Assess and Reasonably Mitigate Risk.

The CPRA specifies that risk assessments must weigh the benefits from processing personal information against the potential risks to the rights of the consumer.²³ The goal of such assessments should be to facilitate and encourage a business’s reasonable, good faith efforts to identify and mitigate substantial harm to consumers that is likely to result from the data processing. The goal should not be to second guess or penalize reasonable balancing of risks and benefits. Such a prescriptive, punitive approach would chill innovation with no meaningful benefit to consumers.

The CPPA should follow the approach the California Attorney General took when providing flexibility in the CCPA regulations. For example, recognizing that the regulations would apply to a range of different businesses interacting with a variety of different consumers in various contexts,²⁴ the regulations governing verification of consumers adopted a flexible standard that could evolve with changes in technology and data security tools. The CPPA similarly should give businesses flexibility in conducting their privacy risk assessments to accommodate their particular industry, consumers, changes in technology, and risks in processing over time.

²¹ Cal. Civ. Code § 1798.185(a)(15)(B).

²² Cal. Civ. Code § 1798.185(a)(15)(B) reads “Nothing in this *section* shall require a business to divulge trade secrets” (emphasis added). Accordingly, the CPRA dictates that no regulation (including those governing cybersecurity audits) issued under Section 1798.185 of the California Civil Code shall require a business to divulge trade secrets.

²³ Cal. Civ. Code § 1798.185(a)(15)(B).

²⁴ Initial Statement of Reasons, §§ VII. B, D, F.

To give businesses the flexibility to tailor their assessments to their industry, customers, and technology, ESA asks that the CPPA adopt the following regulation:

A business shall reasonably weigh the benefits and risks associated with any particular processing activity in each privacy risk assessment. A privacy risk assessment shall not constitute conclusive evidence of a violation of the California Privacy Rights Act.

C. The Regulations Should Align With Existing Laws Requiring Assessments.

Virginia, Colorado, and Connecticut recently passed laws that require companies to assess certain data processing activities.²⁵ The General Data Protection Regulation contains a similar requirement.²⁶ ESA requests that the CPPA align its regulations regarding privacy risk assessments with these other laws in four ways.

1. The Regulations Should Clarify That The Requirement To Conduct Privacy Risk Assessments Is Prospective.

Requiring privacy risk assessments prospectively would bring California’s regulations into alignment with existing state privacy frameworks. Virginia, Colorado, and Connecticut each specify that their data protection assessment requirements apply to processing activities created after the law’s effective date.²⁷

Importantly, this approach also would be consistent with California case law. California courts have found that statutes should apply prospectively absent clear legislative intent.²⁸ The CPRA does not give any explicit indication that its privacy risk assessment requirements should apply retroactively. Therefore, the regulations should apply the privacy risk assessment requirements to only those processing activities that are created or generated after the regulations’ effective date.

²⁵ Consumer Data Protection Act, Va. Legis. Serv. 1st Sp. Sess. 36 (2021) (to be codified at Va. Code Ann. § 59.1-576) (hereinafter “VCDPA”); Concerning Additional Protection of Data Relating To Personal Privacy, 2021 Colo. Legis. Serv. Ch. 483 (to be codified at Colo. Rev. Stat. § 6-1-1309) (hereinafter “CPA”); An Act Concerning Personal Data Privacy And Online Monitoring, 2022 Conn. Legis. Serv. 22-15 § 8(f) (Same) (hereinafter “CTDPA”).

²⁶ General Data Protection Regulation, Article 35.

²⁷ VCDPA § 59.1-576(f) (“Data protection assessment requirements shall apply to processing activities created or generated after January 1, 2023, and are not retroactive.”); CPA § 6-1-1309(6)) (“Data protection assessment requirements shall apply to processing activities created or generated after July 1, 2023, and are not retroactive.”); CTDPA § 8(f) (same).

²⁸ See, e.g., *Abernathy Valley, Inc. v. Cnty. of Solano*, 173 Cal. App. 4th 42, 53, 92 Cal. Rptr. 3d 459, 468 (2009) (“A basic canon of statutory interpretation is that statutes do not operate retrospectively unless the Legislature plainly intended them to do so.”); *Dep’t of Fin. v. Comm’n on State Mandates*, 85 Cal. App. 5th 535, 573, 301 Cal. Rptr. 3d 562, 592 (2022), review denied (Mar. 1, 2023).

This clarification also would exclude processing that ESA’s members conduct to provide services for platforms that are no longer being updated or that are no longer on the market. Similarly, it would avoid forcing consumers to purchase new hardware or install updates that they might prefer not to have.

For these reasons, ESA requests that the CPPA adopt the following regulation:

*Privacy risk assessment requirements shall apply to processing activities created or generated after [effective date of the regulations] and are not retroactive.*²⁹

2. The Regulations Should Permit Businesses to Rely On Assessments Conducted In Accordance With Other Privacy Laws.

Virginia, Colorado, and Connecticut explicitly permit companies to comply with their assessment requirements by relying on assessments they conducted pursuant to other laws.³⁰ The CPPA should take a similar approach in its regulations. That approach would further the CPRA’s purpose of promoting compatibility with privacy laws in other jurisdictions, while at the same time advancing consumers’ privacy interests and businesses’ compliance. Specifically, allowing businesses to rely on existing assessments would advance consumers’ privacy by ensuring that the processing of California residents’ data is subject to the same scrutiny as in other states, and would also advance businesses’ compliance via streamlining the assessments they must conduct. Thus, ESA asks the CPPA to adopt the following regulation:

*Privacy risk assessments conducted by a business for the purpose of compliance with other laws or regulations may comply under this section if the assessments have a reasonably comparable format, scope, and effect.*³¹

3. The Regulations Should Clarify That The Risk Assessment Requirement Applies To Processing, Only If It Results In Decisions That Produce Legal Or Similarly Significant Effects.

Importantly, the CPRA does not require businesses to conduct a risk assessment for *any* risks to privacy, just significant ones. As other laws have recognized, there is significant risk to a consumer when a business processes information in a manner that produces decisions that legally affect a consumer, or affect the consumer in a similarly significant way.³² Various U.S. state

²⁹ This language tracks similar provisions in the VCDPA, CPA, and CTDPA.

³⁰ VCDPA § 59.1-576(E); CTDPA § 8(e); Co. Dep’t Law, *Colorado Privacy Act Rules* (Jan. 27, 2023), available at https://coag.gov/app/uploads/2023/01/CPA_Version-3-Proposed-Draft-Regulations-1.27.2023.pdf, § 8.02(B)(1).

³¹ This language generally tracks similar provisions in the VCDPA, CPA, and CTDPA.

³² General Data Protection Regulation, Article 35(1) (requiring data protection impact assessments for processing that “is likely to result in a high risk to the rights and freedoms of natural persons”), Article 35(3) (specifying that a data protection impact assessment is required in the case of “a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which

laws define decisions that produce legal or similarly significant effects to include the provision or denial of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities.³³ Accordingly, these effects cover the significant harms that can arise to consumers from processing their data.

By requiring businesses to conduct a risk assessment when their processing produces decisions that have legal or similarly significant effects, the regulations will require businesses to assess processing that results in a significant risk to consumers' privacy.³⁴ To that end, the CPPA should adopt the following regulation:

A business shall conduct a privacy risk assessment of only those processing activities that result in decisions that produce legal or similarly significant effects.

"Decisions that produce legal or similarly significant effects concerning a consumer" means a decision made by the business that results in the provision or denial by the business of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.³⁵

4. The Regulations Should Specify That The Agency Will Withhold Privacy Risk Assessments From Public Disclosure Consistent With The Public Records Act.

Virginia, Colorado, and Connecticut specify that assessments will not be subject to public records requests. Adopting a similar specification in the CPRA rules would be consistent with these frameworks, as well as the CPRA and the PRA. The CPRA permits the CPPA to subpoena the business's privacy risk assessments.³⁶ As discussed in Section I.C, the CPRA requires the agency to maintain the assessment's confidentiality, unless the PRA requires the CPPA to disclose it.³⁷ The PRA does not require the CPPA to disclose privacy risk assessments, since the public interest in keeping them confidential clearly outweighs any interest in publishing them.³⁸

decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person") (emphasis added); CTDPA § 8(a)(3); CPA § 6-1-1309(2)(a).

³³ VCDPA § 59.1-571; CTDPA § 1(12); CPA § 6-1-1303(10).

³⁴ Importantly, this would not include decisions that involve incidental processing of consumers personal information. In which case, the processing of personal information would not produce the legal or similarly significant effect. Instead, other aspects of the decisionmaking would produce the effect. For example, a credit card company might identify a risk to its branded card and instruct our members to reject transactions from players using that card. If our members reject transactions in that hypothetical, the decision to deny the financial transaction is driven by which card the consumer uses not the consumer's personal information.

³⁵ This language tracks similar provisions in the VCDPA, CTDPA, and CPA.

³⁶ Cal. Civ. Code § 1798.165.

³⁷ Cal. Civ. Code § 1798.199.15(b).

³⁸ Cal. Gov't Code §§ 7922.000, 7929.210.

Publishing these assessments could reveal a business's privacy vulnerabilities and how the business is addressing them. That publication would increase the potential for an attack on a business, because it would provide bad actors with information they could use to gain access to the business's system and the business's customers' personal information. The resulting risk of harm to both consumers and the business is significant, so the public interest in keeping the risk assessment confidential clearly outweighs the one in disclosing it.

Therefore, the CPPA should adopt the following regulation:

If a privacy risk assessment would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a business, the CPPA shall not disclose it in response to a request under Cal. Gov't Code § 7922.000, et seq.

III. The CPPA Should Align The Regulations Governing Access and Opt-out Rights with Respect to Automated Decisionmaking With Existing Legal Frameworks.

The Invitation asks several questions about access and opt-out rights with respect to automated decisionmaking, including how businesses use automated decisionmaking technologies. Automated decisionmaking technologies are a foundational component of all online services, including the computational processes that power video games. ESA and its members have been at the forefront of using these technologies to protect their users and promote a positive gameplay environment, player safety, and online safety; for example, by using these technologies to detect and prevent security incidents, cheating, fraud, harassment, bullying, and other unlawful or malicious activity. ESA encourages the CPPA to adopt regulations that permit its members to continue this work. The regulations also should make the rights associated with this technology consistent with the CPRA and other applicable laws. Importantly, the CPPA should take care not to issue overly broad regulations, which would impede the basic functionality and business operations of online services.

A. Any Access and Opt-in Regulations With Respect To Automated Decisionmaking Should Apply To Only That Processing That Involves Sensitive Personal Information And Produces Legal Or Similarly Significant Effects.

The CPRA did not give consumers a blanket right to opt out of all automated decisionmaking technologies. Instead, the CPRA requires the agency to issue regulations giving consumers the right to opt out of certain automated decision-making technologies that involve sensitive personal information, including "profiling."³⁹

The regulations should clarify that the right to opt out of automated decisionmaking applies only to automated decisionmaking involving sensitive personal information for two reasons. First, the scope of the right to opt out of certain uses of sensitive personal information is most similar to the automated decisionmaking opt-out right. Because the regulations cannot expand the scope of the statute, the regulations must align consumers' rights to opt out of automated decisionmaking technology with the opt-out rights provided explicitly in the statute.

³⁹ Cal. Civ. Code § 1798.185(a)(16).

The CPRA provides consumers with three opt-out rights: the right to opt out of sales, sharing, and certain uses and disclosures of sensitive-personal information. The rights to opt out of sales and sharing govern disclosures of personal information, which is a limited type of processing.⁴⁰ By contrast, the CPRA’s remaining opt-out right applies to uses *and* disclosures of sensitive personal information. Second, the definition of “sensitive personal information” aligns with the definition of “profiling,” a type of automated decisionmaking. The CPRA defines sensitive personal information to include information revealing a consumer’s union membership, financial account information, genetic and health data, religious or philosophical beliefs, sex life, and precise geolocation.⁴¹ This definition largely overlaps with the CPRA’s concept of “profiling,” which includes processing data concerning the consumer’s employment, economic situation, health, personal preferences, interests, reliability, behavior, and location or movements.⁴²

Additionally, the regulations should limit the right to opt out of automated decisionmaking to that which produces legal or similarly significant effects. No other jurisdiction has created a blanket right to opt out of automated decisionmaking. Instead, other jurisdictions limit the right to opt out of automated decisionmaking technologies to those that produce legal or similarly significant effects.⁴³ Accordingly, ESA encourages the CPPA to adopt the following regulations:

*A consumer may request to opt out of a business’s use of automated decisionmaking technology, but only to the extent such technology (1) uses or discloses the consumer’s sensitive personal information, and (2) produces legal or similarly significant effects.*⁴⁴

Not only will this language align the right to opt out of automated decisionmaking with the enabling statute and other jurisdictions, but it also has the added benefit of fulfilling the CPRA’s purpose. The CPRA states that one of its purposes is to enable pro-consumer new products and services while promoting efficiency of implementation for businesses.⁴⁵ Focusing the right to opt out of automated decisionmaking on this subset of technologies will permit businesses to continue to innovate technology that helps consumers. For example, automated decisionmaking technologies used in gaming played an integral role in advancing “deep learning” algorithmic processes. Learnings from the gaming industry’s use of machine learning contributed to the development of technology used to support machine learning in the medical context, specifically to improve breast cancer reduction.⁴⁶ The agency should avoid stifling the

⁴⁰ Cal. Civ. Code §§ 1798.140(ad), (ah).

⁴¹ Cal. Civ. Code § 1798.140(ae). Note that the color coding in this sentence and the next is intended to highlight the significant overlap between the definition of “sensitive personal information” and that of “profiling.”

⁴² Cal. Civ. Code § 1798.140(z).

⁴³ VCDPA § 59.1-573(A)(5)(iii); CTDPA § 4(a)(5)(C); CPA § 6-1-1306(10(a)(I)(C).

⁴⁴ If the CPPA does not adopt the draft regulation in §II.C.3 of these comments, we recommend adding the same definition of “decisions that produce legal or similarly significant effects concerning a consumer” here.

⁴⁵ California Privacy Rights Act of 2020, § 3(C)(5), 2020 Cal. Stat. A-85.

⁴⁶ Catherine Gray, How does the gaming industry help with AI development?, AI Magazine (May 11, 2022), <https://aimagazine.com/technology/how-does-the-gaming-industry-help-with-ai-development>. See also

potential to use automated decisionmaking technology to create new and innovative products and services that haven't even been conceived yet. It also preserves businesses' ability to protect their platforms, since businesses use automated decisionmaking to prevent and detect harmful, inappropriate, and illegal conduct. That use would not rise to the level of legal or similarly significant effect, and consumers should not have a right to opt out of it.

B. The Regulations Should Clarify That Any Rights With Respect To Automated Decisionmaking May Not Impair Businesses' Ability To Protect Themselves And Their Customers.

The CPRA specifies that businesses do not have to disclose information in response to an access request that would jeopardize the security or integrity of the platform.⁴⁷ The regulations should make a similar statement about any request to access information about automated decisionmaking technology. The regulations should not require businesses to disclose information about automated decisionmaking technology that would jeopardize security or integrity. This includes information that would preclude a company from efficiently preventing, detecting, and defending against harmful, illegal, and inappropriate conduct like cheating or toxic behavior. For example, a video game company might need to withhold information to prevent financial fraud. If a video game company detects that a player is trying to use someone else's credit card to purchase content, that company should not be required to respond to that player's access request by providing information to the player that would allow the player to circumvent the company's automated decisionmaking technologies that are used to detect fraud. A video game company also might need to withhold information on such technologies to prevent cheating or toxic behavior to maintain a positive game play environment. For example, a bad actor might request information about the algorithms, tools, and processes a gaming company created to detect and prevent cyberbullying or grooming. If disclosing that information (including about the logic involved in automated decisionmaking processes) would permit the bad actor to continue bullying or grooming their victim, the video game company should not have to do so. Accordingly, ESA requests that the CPPA adopt the following regulation:

Nothing in these regulations shall require businesses to provide consumers with access to information about automated decision-making technology that would compromise security and integrity.

The CPRA also specifies that businesses do not have to disclose trade secret information in response to access requests.⁴⁸ Similarly, the regulations should specify that in response to requests for information about automated decisionmaking, businesses are only required to

Gamechangers: More than just a game, The Economist (Aug. 16, 2021), <https://www.economist.com/podcasts/2021/08/16/shall-we-play-a-game-how-video-games-transformed-ai>; Catherine Gray, DeepMind's pioneering work with artificial intelligence, AI Magazine (July 29, 2021), <https://aimagazine.com/ai-applications/deepminds-pioneering-work-artificial-intelligence>.

⁴⁷ Cal. Civ. Code § 1798.130(a)(3)(B)(iii).

⁴⁸ Cal. Civ. Code § 1798.185(a)(3).

produce that information that is not a trade secret. ESA urges the department to consider adopting the following regulation.

Nothing in these regulations shall require businesses to provide consumers with access to trade secrets.

* * *

ESA appreciates the CPPA's consideration of these comments, and we look forward to continuing to work with the CPPA on these important issues.

Sincerely,



Maya McKenzie
Counsel, Technology Policy
Entertainment Software Association

From: McArthur, Webb [REDACTED]
Sent: Monday, March 27, 2023 3:23 PM
To: Regulations
Cc: Eric Ellman
Subject: Comment of the Consumer Data Industry Association (PR 02-2023)
Attachments: CDIA CPPA CPRA Preliminary Rulemaking Comments - Audit, Risk, Automated Decisionmaking.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

To whom it may concern:

Attached is the comment of the Consumer Data Industry Association (CDIA) in response to the CPPA's Invitation for Preliminary Comments (PR 02-2023).

Webb McArthur
Partner | Admitted in the District of Columbia, Maryland, and Virginia
Hudson Cook, LLP
Direct: [REDACTED] | Cell: [REDACTED]
1909 K St., NW | 4th Floor | Washington, DC 20006



**HUDSON
COOK**

The information contained in this transmission may be privileged and may constitute attorney work product. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact Webb McArthur at [REDACTED] or [REDACTED] and destroy all copies of the original message and any attachments.

* * * *



Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

P 202 371 0910

CDIAONLINE.ORG

March 27, 2023

Via Electronic Delivery to
regulations@coppa.ca.gov

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

RE: Invitation for Preliminary Comments on Proposed Rulemaking on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking (PR 02-2023)

To whom it may concern:

The Consumer Data Industry Association submits this comment letter in response to the invitation of the California Privacy Protection Agency ("CPPA"). In this invitation, the CPPA seeks input on proposed rulemaking under the California Privacy Rights Act ("CPRA") relating to cybersecurity audits, risk assessments, and automated decision-making.¹

CDIA strongly urges the CPPA to limit cybersecurity audit and risk assessment requirements to processing that presents significant consumer risk and to craft requirements that are flexible and permit businesses to appropriately identify and address their unique risks. CDIA also urges the CPPA to clarify that their requirements will apply directly only to CCPA businesses so that businesses can address particular risks with their service providers by contract within the context of the business' data processing activities. Finally, CDIA urges the CPPA to clarify that consumer rights other business requirements related to automated decision-making do not apply to personal information processed for security and integrity activities.

CDIA members have been complying with laws and regulations governing the consumer reporting industry for decades. Members have complied with the Fair Credit Reporting Act ("FCRA"), which is often viewed as the nation's first national consumer privacy law. The FCRA governs the collection, assembly, and use of consumer report information and provides the framework for the U.S. credit reporting system. The FCRA incorporate fair information principles, like access, notice, choice, consent, correctability, and accountability.

¹ The Consumer Data Industry Association ("CDIA") is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumers' access to financial and other products suited to their unique needs.

In particular, the FCRA outlines many consumer rights with respect to the use and accuracy of the information contained in consumer reports. Under the FCRA, consumer reports may be accessed only for permissible purposes, and a consumer has the right to dispute the accuracy of any information included in his or her consumer report with a consumer reporting agency (“CRA”).

Our members are at the forefront of consumer privacy protection in ways that protect consumers and meet their expectations for fast, friction-free transactions. Fair, accurate, and permissioned use of consumer information is necessary for consumers and businesses to do business effectively. As we describe in greater detail below, CDIA members provide identity verification and fraud prevention services to their customers, and such services involve the processing of personal information. Identity verification and fraud services providers may offer their services to CCPA businesses as service providers.

To assist the agency in promulgating clear and effective regulations that allow businesses to best support customers and consumers, CDIA offers the following comments on the topics as presented in the Invitation for Preliminary Comments:

I. Cybersecurity Audits and Risk Assessments

The Invitation for Preliminary Comments raises questions related to existing laws that require cybersecurity audits and risk assessments. The Invitation also poses the following questions:

5. What else should the Agency consider to define the scope of cybersecurity audits?

First and foremost, CDIA encourages the CPPA to limit the scope of required cybersecurity audits to personal information processing that presents significant risk to consumer privacy or security. The CPRA authorizes the CPPA to issue regulations requiring cybersecurity audits for the processing of personal information *that presents significant risk to consumers’ privacy or security*. Cal. Civ. Code § 1798.185(a)(15)(A). Because of this qualifier, it is clear that not all personal information processing would present significant consumer risk to privacy or security, so the CPPA should consistently limit any regulatory requirements.

Additionally, CDIA urges the CPPA to establish cybersecurity standards that are flexible and permit businesses to implement cybersecurity audit procedures specific to the risks present with their businesses, systems, and data. This includes permitting businesses to undertake such audit efforts internally rather than through a third party, which could still ensure independence in audit functions while mitigating any additional privacy and security risks caused by a third-party audit-related disclosures.

Further, CDIA urges the CPPA to clarify that the CPRA’s cybersecurity audit

requirements apply directly to CPPA businesses and only by service provider agreement to service providers. This flexibility will allow businesses to both protect consumers and better meet their needs. Among other products and services, CDIA members provide fraud, identity theft, and security incident detection and prevention services to clients. Such providers may offer these services as service providers under the CCPA, acting at the direction of and for the benefit of their clients that may be businesses directly subject to the CCPA.

Civil Code, § 1798.140(ag)(1)(D) of the CPRA contemplates business oversight of their service providers with regard to assessments, audits, and other technical and operational testing. CDIA members are acutely aware of the need for businesses to develop and implement cybersecurity protections tailored to the nature of their business, data, and systems. Especially where service provider services are related to the business' cybersecurity, businesses need to be empowered to set the standards, including audit requirements, that apply to their businesses.

Accordingly, CDIA believes that the CPPA should set standards for cybersecurity audits that are flexible and allow businesses to make decisions based on identifying specific risks to their business, systems, and data, and those businesses, instead of the CPPA, should set the oversight appropriate to their service providers. CDIA urges the CPPA to clarify that the audit requirements apply directly only to businesses as defined by the CCPA and to processing that presents significant privacy and security risks.

Finally, CDIA recommends aligning any proposed cybersecurity standards with existing and well-established industry standards and risk assessment models utilized broadly. Any new standards implemented should permit the continued use of these models. Examples include ISO 27001 and ISO 27002 and NIST.

II. Risk Assessments

The Invitation for Preliminary Comments poses questions related to existing laws requiring data processing risk assessments and further asks:

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

First and foremost, CDIA encourages the CPPA to limit the scope of required risk assessments to personal information processing that presents significant risk to consumer privacy or security. The CPRA authorizes the CPPA to issue regulations requiring risk assessments with respect to the processing of personal information *ersonal information that presents significant risk to consumers' privacy or security*. Cal. Civ. Code § 1798.185(a)(15)(A). Because of this qualifier, it is clear that not all personal information processing would present significant consumer risk to privacy or security, so the CPPA should consistently limit any regulatory requirements.

Further, like with cybersecurity audits discussed above, CDIA urges the CPPA to establish risk assessment requirements that are flexible so that businesses can identify and mitigate risks appropriately and efficiently based on the nature of the business, its systems, and its data. CDIA also urges the CPPA to clarify that the risk assessment requirements apply to businesses directly, not their service providers.

Just as data processing activities vary across different businesses, data processing risks to consumers, the business, and the public at large differ as well. As a result of these differences, the procedures needed to assess changing risks specific to the business's particular data processing activities may need to vary as well, and any need for service providers to participate should flow down to service providers rather than applying independently. Risks associated with data processing by a service provider, like a CDIA member, need be assessed within the context of the business's data processing, and it would not be effective to merely attempt to identify processing risks in a vacuum for a particular service provider.

III. Automated Decision-making

The Invitation for Preliminary Comments poses the following question:

4. How have businesses or organizations 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.

CDIA members provide a wide range of products and services that involve the automated processing of personal information, like identity verification and fraud detection services. Fraud prevention and detection services may provide information on known fraudsters and fraud strategies and identify potential fraud risks based on comparing applicant-supplied data with data available from third-party sources. Subscribers of these types of services use the information provided to mitigate against fraud loss. Businesses regularly need to engage in identity verification and fraud detection efforts, in some circumstances by law or collective standard but otherwise to reduce risk of harm to the business and to consumers. By preventing fraud and identity theft on consumers, such efforts further consumer privacy.

The proposal should not include identity theft and fraud detection services in the term “automated decisionmaking technologies.” Identity theft and fraud detection products and services are meant to confirm identity or identify fraud or other related risks in a proposed transaction; they are not meant to make a decision as to whether an individual is eligible for a particular product or service. Thus, it does not appear that the term “automated decisionmaking technologies” describes identity verification and fraud detection efforts.

Further, Civil Code, § 1798.140(z) defines the term “profiling” as automated processing “to evaluate certain aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, behavior, location or movements.” Efforts to detect fraud and verify identity are distinct from “profiling” activities because such efforts attempt to confirm what a consumer told the business and otherwise detect fraudulent activities in order to reduce risk.

The Invitation also asks:

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?

Even though identity theft and fraud detection services should not be considered “profiling” or otherwise an “automated decisionmaking technology,” CDIA encourages the CPPA to expressly exempt personal information processing for these purposes, “security and integrity” activities under the CPRA, from any access, opt-out, or other rights or requirements.

Civil Code, § 1798.140(ac) defines “security and integrity” to include activities related to detecting security incidents, detecting fraud or other illegal action, and verifying identity. Unlike other comprehensive state data privacy laws, the CCPA does not have a broad exemption for personal information processed for fraud detection or similar purposes, but the CCPA text reflects the drafter’s intent and desire to protect personal information processed for these purposes for consumer privacy purposes.

Civil Code, § 1798.120(d) provides that the right to delete does not apply to personal information reasonably necessary to be maintained to help ensure security and integrity. Civil Code, § 1798.130(a)(3)(B) provides that, for purposes of the right to know, “specific pieces of personal information” do not include “data generated to help ensure security or integrity or as prescribed by regulation.” And Civil Code, § 1798.140(e)(2) includes “security and integrity” purposes as “business purposes” distinct from commercial purposes like selling personal information.

If the CPPA were to include “security and integrity” activities in its conception of automated decision-making such that consumers would have access and opt out rights, businesses would be impeded from appropriately engaging in fraud detection and identity theft efforts. Consumers intending to commit fraud could simply opt out of automated

processing, and a business might not be able to prevent the intended fraud. Fraudsters could also exercise access requests in order to learn how such business detects fraud, which if shared, could prevent such business from appropriately detecting fraud not only for the consumer making such a request, but for consumers generally.

Accordingly, in light of the law's recognition of the importance of security and integrity activities and the current lack of clarity around the scope of "automated decisionmaking technologies" for a rule, CDIA urges the CPPA to clarify that personal information processed for "security or integrity" purposes is not subject to automated decision-making rights or requirements.

* * *

Thank you for the opportunity to share our views on the anticipated rulemaking under the CPRA. Please contact us if you have any questions or need further information based on comments.

Sincerely,

A solid black rectangular box used to redact the signature of Eric J. Ellman.

Eric J. Ellman
Senior Vice President, Public Policy & Legal Affairs

From: Edwin Portugal [REDACTED]
Sent: Monday, March 27, 2023 3:48 PM
To: Regulations
Cc: Danielle Arlowe; Matt Kownacki
Subject: PR 02-2023 preliminary rulemaking - AFSA letter
Attachments: AFSA comment letter - CA CPPA Prelim Comments Automated Decisionmaking.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear Mr. Sabo,

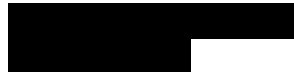
Attached is a letter from the American Financial Services Association on the CPPA's invitation for comment on additional privacy rules.

Please let us know if you have any questions.

Best,
Edwin



Edwin Portugal
Manager, State Policy & Regulatory Affairs



[@AFSA_DC](#) | [Linkedin](#) | [@AFSA_SGA](#)

March 27, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

Re: PR 02-2023 Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking

Dear Mr. Sabo:

On behalf of the American Financial Services Association (AFSA),¹ thank you for the opportunity to provide comments on the California Privacy Protection Agency's (Agency) February Invitation for Preliminary Comments on Proposed Rulemaking Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking. AFSA members share the state's goal of protecting the privacy of consumers, promoting understanding by consumers of the personal information about them that is collected, sold, and shared for a business purpose, and guarding personal information from unauthorized access. We appreciate the Agency's efforts to engage stakeholders to consider how various industries use these technological tools to interact with consumers and how such industry practices are currently regulated. We also appreciate the Agency's consideration of our comments on previous Agency rulemakings and look forward to engaging with and serving as a resource as the rulemaking process moves forward.

Consumer Benefits of Automated Decisionmaking

The financial services industry believes that technology holds tremendous opportunity to make financial services safer, more convenient, and more inclusive, and there are many everyday benefits that automated decisionmaking systems provide. As such, financial institutions are continuously evaluating ways to safely and responsibly integrate automated decisionmaking technology and algorithmic solutions to better serve customers and communities across the country. Algorithms make credit decisions more accurate, fair, faster and more affordable by judging applicants on their credit worthiness. Automated tools also eliminate some of the risk of the biases that can be found in human interactions and can help identify products and services designed to benefit communities, including historically underserved populations, helping close the racial wealth gap. Consumers want—and sometimes need—fast access to responsible credit approval.

The use of algorithms is also crucial for protecting all consumers and financial institutions alike from fraud. Fraudulent transactions annually amount to billions of dollars,² making the need for fraud prevention services greater than ever. Detecting fraudulent patterns is typically based on large multi-

¹ Founded in 1916, the American Financial Services Association (AFSA), based in Washington, D.C., is the primary trade association for the consumer credit industry, protecting access to credit and consumer choice. AFSA members provide consumers with many kinds of credit, including direct and indirect vehicle financing, traditional installment loans, mortgages, payment cards, and retail sales finance. AFSA members do not provide payday or vehicle title loans.

² See FTC, *New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021* at <https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0>.

country data sets, as fraudsters will use similar methods from one country to another and then attempt to take them globally. Human logic alone is slower and unable to identify such complex patterns. The use of artificial intelligence and algorithms makes this process more efficient and effective. Limiting the use of artificial intelligence (AI) to identify fraud would increase risks and costs for merchants, exposing them to potentially higher chargeback costs.

Many financial institutions also use technology-enabled tools to automate routine customer interactions, triage customer calls, provide tailored marketing, and customize trade recommendations. Customers want the convenience of online and mobile platforms, and companies are using algorithms to better connect with customers in their preferred channels. These technologies can also help customers manage budgets and make digital tools more accessible.

Existing Consumer Protections for Automated Decisionmaking

As noted above the financial services industry uses technology to benefit consumers and each use of technology is governed by a robust legal framework designed to prohibit discrimination. We believe that discrimination in the allocation of credit and financial services is wrong and is prohibited under existing federal and state laws. We support enforcement of fair lending laws at the federal, state, and local levels. These laws apply regardless of the use of technology. For decades, the financial services industry has worked with state and federal regulatory partners to combat and overcome historical discriminatory practices. Current law already provides increased transparency and consumer protections in all credit transactions, regardless of whether that transaction is conducted in person, manually, or involves an algorithm or automation.

Importantly, federal regulators have been active on this issue. The Consumer Financial Protection Bureau (CFPB), Board of Governors of the Federal Reserve System (FRB), Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA) all have been actively engaged on this topic.³ These agencies are also closely monitoring the work of the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce, and other government bodies in the U.S. and around the world, to assess the benefits and risks associated with emerging technologies and issue appropriate guidance. For example, in May 2022, the CFPB issued Circular 2022-03: Adverse action notification requirements in connection with credit decisions based on complex algorithms, which makes it clear that a creditor's obligations regarding discrimination and adverse action notices "apply equally to all credit decisions, regardless of the technology used to make them."⁴

The Equal Credit Opportunity Act (ECOA) has—for nearly 50 years—prohibited discrimination in credit transactions based on certain protected characteristics. ECOA's protections extend beyond just offers or denials of credit based on protected characteristics and also include the fairness of the terms of the credit. ECOA prohibits the use of protected characteristics in any credit decision making system, whether automated or manual. Importantly, ECOA also requires financial institutions to provide adverse

³ See, e.g., <https://www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence>

⁴ See CFPB, *Consumer Financial Protection Circular 2022-03* at <https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/>.

action notices explaining the principal reasons for a denial of credit or other unfavorable credit decision. Under ECOA, financial institutions face regulatory scrutiny from multiple federal agencies, including the Consumer Financial Protection Bureau (CFPB). Similarly, the Department of Housing and Urban Development (HUD) also enforces compliance with the Fair Housing Act for mortgage lending.

The Gramm-Leach-Bliley Act (GLBA) protects the privacy of consumer financial information held by financial institutions. Under GLBA and subsequent regulations, financial institutions are required to make clear and conspicuous privacy disclosures to both customers and consumers who are not customers. These notices must disclose what information is collected or shared and allow a consumer to opt-out of sharing. Similarly, the Fair Credit Reporting Act (FCRA) regulates the collection and use of consumers' credit information to ensure fairness, accuracy, and privacy. The FCRA only permits financial institutions to use credit information for specific purposes limited by the Act and also requires financial institutions to provide adverse action notices in instances where the credit information negatively affected an offer of credit. Special disclosures are also required when a decision is based in any part on a consumer's credit score. Importantly, consumers have a right to see their scores and their consumer reports and to dispute information they believe to be inaccurate.

Federal banking regulators also have oversight over the use of credit modeling that is used to inform decision making. The Office of the Comptroller of the Currency (OCC), Federal Reserve, and the FDIC have published model risk management guidance.⁵ These laws and regulations are in addition to numerous other broader laws, like the Federal Trade Commission Act and Consumer Financial Protection Act of 2010, which generally prohibit unfair, deceptive, or abusive acts or practices, and California's own laws that provide enforcement authority on specific protections to the Department of Financial Protection and Innovation (DFPI) or the Attorney General.

Federal Lending Programs

In addition to the uses for automated decisionmaking technology outlined above, many financial institutions participate in lending programs that are administered by federal agencies or government sponsored enterprises (GSEs) like Fannie Mae or Freddie Mac. Covered products include federally insured mortgages and those sold on the secondary market to GSEs. Many of these products rely on automated processes that financial institutions have no control of and are administered by the federal agency.

One such example comes from the Federal Housing Administration (FHA). FHA identifies its TOTAL mortgage scorecard process as: "a statistically derived algorithm developed by HUD to evaluate borrower credit history and application information."⁶ As with other federal affordability programs, this algorithm was developed and is maintained by a federal agency, but any financial institution

⁵ Office of the Comptroller of the Currency, Supervisory Guidance on Model Risk Management, OCC Bulletin 2011-12 (Apr. 4, 2011), <https://www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-12.html>; Board of Governors of the Federal Reserve System, SR Letter 11-7 (Apr. 4, 2011), <https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm>; Federal Deposit Insurance Corporation, Guidance on Model Risk Management, FDIC FIL-22-2017 (June 7, 2017), <https://www.fdic.gov/news/financial-institution-letters/2017/fil17022.html>.

⁶ See U.S. Department of Housing and Urban Development, *FHA TOTAL Scorecard*, at https://www.hud.gov/program_offices/housing/sfh/total.

participating in HUD programs has no control over the process. The TOTAL mortgage scorecard is one example, but similar issues exist with the Fannie Mae Desktop Underwriter, Freddie Mac Loan Product Advisor, and other federally administered Automated Underwriting Systems (AUS) such as those approved by the Department of Veterans Affairs. Given the scale of these various programs, and the potential impact to California consumers if these programs were unavailable, the Agency must take into account the federal use of automated tools for various financial services.

Thank you in advance for your consideration of our comments. If you have any questions or would like to discuss this further, please do not hesitate to contact me at [REDACTED] or [REDACTED].

Sincerely,

[REDACTED]
Matthew Kownacki
Director, State Research and Policy
American Financial Services Association

From: John Davisson [REDACTED]
Sent: Monday, March 27, 2023 4:09 PM
To: Regulations
Cc: Katharina Kopp; Jeffrey Chester; Susan Grant
Subject: PR 02-2023 - Comments of EPIC, CDD, & CF
Attachments: EPIC-et-al-comments-CCPA-rulemaking-March-2023.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear Mr. Sabo,

On behalf of the Electronic Privacy Information Center, the Center for Digital Democracy, and the Consumer Federation of America, please find attached comments in response to the agency's February 2023 invitation for public input concerning regulations under the California Consumer Protection Act as amended.

Best,
John

--

John Davisson
Director of Litigation & Senior Counsel
O: [REDACTED]
C: [REDACTED] | @johndavisson | epic.org



COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER,
CENTER FOR DIGITAL DEMOCRACY, AND CONSUMER FEDERATION OF AMERICA

to the

CALIFORNIA PRIVACY PROTECTION AGENCY

On Proposed Rulemaking re Cybersecurity Audits, Risk Assessments,
and Automated Decisionmaking

PR 02-2023

March 27, 2023

The Electronic Privacy Information Center, Center for Digital Democracy, and Consumer Federation of America submit these comments in response to the California Privacy Protection Agency (CPPA)’s February 2023 invitation for public input concerning the agency’s development of further regulations under the California Consumer Protection Act of 2018 (CCPA) as amended by the California Privacy Rights Act of 2020 (CPRA).

As we have conveyed in previous comments, we firmly support the CPPA’s efforts to establish robust protections for Californians against harmful commercial data practices. As the agency formulates regulations concerning cybersecurity audits, risk assessments, and automated decisionmaking, we renew our call to “protect consumers’ rights” and “strengthen[] consumer privacy” at every opportunity, consistent with the expressed will of California voters.¹ In particular, we urge the Agency to take account of the full spectrum of harms that can result from personal data processing and the use of automated decisionmaking systems (ADS); establish strong cybersecurity

¹ California Privacy Rights Act of 2020 §§ 3, 3(C)(1).

audit standards that draw on the strongest commonalities between existing frameworks; require businesses to routinely conduct robust risk assessments and to submit both unredacted and summarized versions to the CPPA; and ensure that consumers enjoy robust and effective ADS disclosures and opt-out rights.

I. Our organizations

The Electronic Privacy Information Center² is a public interest research center established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC has previously provided comments on the CCPA³ and published a detailed analysis of the CPRA before its approval by California voters.⁴

The Center for Digital Democracy⁵ is a public interest advocacy, research, and education organization with a mission to ensure that digital technologies serve and strengthen democratic values, and safeguard privacy, civil, and human rights.

The Consumer Federation of America,⁶ an association of nonprofit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education, promotes policies that protect consumers from unwanted and inappropriate use of their personal information.

² <https://epic.org/>.

³ Comments of EPIC to Cal. Privacy Prot. Agency (Nov. 20, 2022), <https://epic.org/wp-content/uploads/2022/11/EPIC-CPPA-Comments-Nov-20.pdf>; Comments of EPIC et al. to Cal. Privacy Prot. Agency (Aug. 23, 2022), <https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf>; Comments of EPIC et al. to Cal. Privacy Prot. Agency (Nov. 8, 2021), <https://epic.org/wp-content/uploads/2021/11/PRO-01-21-Comments-EPIC-CA-CFA-OTI.pdf> [hereinafter EPIC et al. 2021 CCPA Comments]; Comments of EPIC to Cal. Office of the Att’y Gen. (Feb. 25, 2020), <https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf>; Comments of EPIC to Cal. Office of the Att’y Gen. (Dec. 6, 2019), <https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Dec2019.pdf>.

⁴ EPIC, *California’s Proposition 24* (2020), <https://epic.org/californias-proposition-24/>.

⁵ <https://www.democraticmedia.org>.

⁶ <https://consumerfed.org/>.

II. Harms and use cases

The Agency asks several questions about the application and harms of personal data processing and automated decisionmaking technology. Before turning to our discussion of how the Agency should regulate harmful data practices, we address those questions here. In particular, we set out (a) the privacy, autonomy, physical, discrimination, data security, and other harms caused by the processing of personal information; (b) examples of how automated decisionmaking technology is already used in commercial settings; and (c) examples of consumer experiences with automated decisionmaking technology.

a. Harms from the processing of personal information

Responsive to question II.2

Consumers are persistently tracked online through the sweeping collection, processing, and use of their personal information.⁷ This personal data fuels online commerce and can be used in ways that consumers expect and welcome. But when these commercial surveillance systems enable online firms to build detailed profiles of consumers, often including sensitive personal characteristics, consumers are exposed to “ever-increasing risks of data breaches, data misuse, manipulation, and discrimination.”⁸ Even with the most effective notice and transparency

⁷ Comments of EPIC to the FTC Proposed Trade Regulation Rule on Commercial Surveillance & Data Security 7 (Nov. 2022), <https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf> [hereinafter EPIC FTC Comments on Commercial Surveillance]; *see also* FTC Office of Tech., *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, Fed. Trade Comm’n (Mar. 16, 2023), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking>; *Factsheet: Surveillance Advertising: How Does the Tracking Work?*, Consumer Fed. of America (Aug. 26, 2021), https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-how-tracking-works/.

⁸ *Hearing before the Subcomm. Consumer Prot. of the H. Comm. on Energy & Com.*, 117th Cong. (2022) (testimony of Caitriona Fitzgerald), <https://epic.org/documents/hearing-on-protecting-americas-consumers-bipartisan-legislation-to-strengthen-data-privacy-and-security/>; *see also* Consumer Fin. Prot. Bureau, *CFPB Issues Advisory to Protect Privacy When Companies Compile Personal Data* (Jul. 7, 2022), <https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-advisory-to-protect-privacy-when-companies-compile-personal-data/> (“Americans are now subject to round-the-clock surveillance by large commercial firms seeking to monetize their personal data.”).

requirements, consumers cannot meaningfully consent or protect themselves from complex commercial surveillance practices.⁹

Commercial systems that track individuals and process personal information can inflict a wide range of harms. Privacy scholars Danielle Citron and Daniel Solove have cataloged numerous harms resulting from the large-scale processing of personal information, including autonomy, physical, discrimination, and data security harms.¹⁰ The scale and scope of these harms is “especially acute for marginalized communities, where they foster discrimination and inequities in employment, government services, healthcare, education, and other life necessities.”¹¹ For example, physical harms facilitated by privacy violations—like stalking and assault—can pose a disproportionate risk to victims of domestic violence.

Other privacy harms include economic harms (e.g., a heightened risk of identity theft that would result in financial loss), reputational harms, relationship harms, and psychological harms (e.g., emotional distress from threats or harassment online). Psychological harm can result from a fear of exposure or misuse of sensitive data including medical records or intimate images.¹²

The violation of autonomy is another type of privacy harm. While autonomy harms can flow from the overcollection personal data processing itself, other mechanisms like manipulation, dark

⁹ EPIC FTC Comments on Commercial Surveillance, *supra* note 77, at 153 (“We have moved beyond the notion that notice and consent alone can legitimize commercial surveillance practices when those practices are too complex and numerous for even the most sophisticated consumer to understand.”); Mary Madden, Data & Society, *Privacy, Security, and Digital Inequality* (Sept. 27, 2017), https://datasociety.net/wp-content/uploads/2017/09/DataAndSociety_PrivacySecurityandDigitalInequality.pdf (“52% of those in the lowest-earning households say that not knowing what personal information is being collected about them or how it is being used makes them “very concerned,” compared with 37% of those in the highest-income households.”).

¹⁰ Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U.L. Rev. Online 793, 830–59 (2021), <https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf>.

¹¹ *Id.* at 7.

¹² Danielle K. Citron, *Sexual Privacy*, 128 Yale L. J. 1870, 1874–81 (2019), https://www.yalelawjournal.org/pdf/Citron_q8ew5jff.pdf.

patterns, or violations of contextual integrity can result a loss of autonomy online.¹³ For example, platform design can result in thwarted expectations when consumers are nudged to purchase certain items, divulge information, or exposed to profiling and targeted advertising from an unexpected secondary use of their data.¹⁴ Consumers do not have control over data collected without their knowledge or downstream uses of the data they knowingly provided to online companies. “The loss of control poses special concerns for sensitive data about individual consumers’ finances, health, intimate relationships, and precise location.”¹⁵

Commercial surveillance can also lead to discrimination harms.¹⁶ Troves of personal data fuel systems that target and profile consumers by dividing and scoring consumers based on their characteristics, demographics, and behaviors.¹⁷ Through mechanisms like targeted advertising, consumers are sorted in ways that “reflect and entrench systemic biases.”¹⁸ Targeted advertising can reinforce discrimination against marginalized groups and deprive those individuals of equal access to information about various economic opportunities including housing, employment, and education.¹⁹ For example, before changing their ad targeting system after a settlement with the Department of Justice, Meta “allowed discrimination in the targeting and delivery of ads for housing, credit service, and job openings based on sex, race, and age.”²⁰ Other examples include retail websites charging

¹³ EPIC FTC Comments on Commercial Surveillance, *supra* note 7, at 33.

¹⁴ *Id.* at 44–45.

¹⁵ EPIC FTC Comments on Commercial Surveillance, *supra* note 7, at 46.

¹⁶ *Id.* at 112–13.

¹⁷ *Id.* at 48.

¹⁸ *Id.*

¹⁹ Aaron Rieke and Corrine Yu, *Discrimination’s Digital Frontier*, The Atlantic (Apr. 15, 2019), <https://www.theatlantic.com/ideas/archive/2019/04/facebook-targeted-marketing-perpetuates-discrimination/587059/>.

²⁰ *Hearing before the Subcomm. Consumer Prot. of the H. Comm. on Energy & Com.*, 117th Cong. (2022) (testimony of David Brody), <https://docs.house.gov/meetings/IF/IF17/20220614/114880/HHRG-117-IF17-Wstate-BrodyD-20220614.pdf>.

different prices based on user demographics²¹ and consumer financial discrimination through payday loan ad targeting.²²

The collection and processing of personal information can also result in harmful data security violations.²³ The accumulation of data, whether “from the consumer directly, scraped from public sources, and purchased from data brokers, creates serious security risks.”²⁴ Specific categories of data collection and processing can heighten the security risks associated with an eventual breach, sale, or downstream use. A data breach or incident revealing sensitive information like health data, data collected from children or teenagers, or financial information can exacerbate the harm from exposure. For example, unauthorized secondary use of location data can reveal historical or real-time location, “exposing an individual to stalking and other physical threats, as well as doxing.”²⁵ Location data can illustrate sensitive information like visiting an abortion clinic, substance abuse support meeting, or place of worship.²⁶ Additionally, because location data is “available for purchase for a nominal fee,”²⁷ or accessible through hacking and security breaches, bad actors can purchase data to stalk, harass, or pose other threats to the wellbeing of individuals.

²¹ Jennifer Valentino-DeVries et al., *Websites Vary Prices, Deals Based on Users' Information*, Wall St. J. (Dec. 24, 2012), <https://www.wsj.com/articles/SB10001424127887323777204578189391813881534>.

²² Aaron Rieke and Logan Koepke, *Led Astray: Online Lead Generation and Payday Loans*, Upturn (2015), <https://www.upturn.org/reports/2015/led-astray/>.

²³ EPIC & Consumer Reports, *How the FTC Can Mandate Data Minimization Through A Section 5 Unfairness Rulemaking* 7 (Jan. 26, 2022), https://advocacy.consumerreports.org/wp-content/uploads/2022/01/CR_Epic_FTCDDataMinimization_012522_VF_.pdf [hereinafter *Data Minimization White Paper*].

²⁴ *Id.* at 29.

²⁵ EPIC FTC Comments on Commercial Surveillance, *supra* note 77, at 50.

²⁶ See Assoc. Press, *Priest Outed via Grindr App Highlights Rampant Data Tracking*, NBC News (July 22, 2021), <https://www.nbcnews.com/tech/security/priest-outed-grindr-app-highlights-rampant-data-tracking-rcna1493>; Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, Vice (Nov. 16, 2020), <https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x>; Corin Faife, *ICE Uses Data Brokers to Bypass Surveillance Restrictions, Report Finds*, The Verge (May 10, 2022), <https://www.theverge.com/2022/5/10/23065080/ice-surveillance-drag-net-data-brokers-georgetown-law>;

²⁷ EPIC FTC Comments on Commercial Surveillance, *supra* note 77, at 50.

b. Uses of automated decisionmaking technologies

Responsive to question III.4

The commercial use of automated decisionmaking systems (ADS) is rapidly growing.²⁸ From computer vision to recommendation systems, generative AI, and facial recognition, a vast array of ADS has been developed and deployed by companies just in the last several years.²⁹ Many of these systems are used in operations, supply chain management, risk assessment, marketing, and strategy.³⁰ This includes systems for automating product feature optimization, risk modeling, and customer service analytics.³¹ But companies also use automated systems to screen and score individuals and to make significant decisions that impact their health, welfare, and access to housing, employment, education, public benefits, and credit.

Despite the well-documented inaccuracy, discrimination, and opacity problems that characterize these systems (see below), automated decisionmaking technology has spread to a wide range of industries and applications, including:

- *Employment screening.* ADS has been used in all aspects of the job application process, including resume screening, interviews, and hiring determinations.³² For example, HireVue uses ADS to evaluate job applicants based on biometric data collected in automated interviews.³³

²⁸ McKinsey & Co., *The State of AI in 2022* (Dec. 6, 2022), <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review> (Annual State of AI survey of 1,500 companies, adoption of AI has doubled since 2017).

²⁹ *Id.*

³⁰ *Id.*

³¹ *Id.*

³² See, e.g., Sheridan Wall & Hilke Schellmann, *LinkedIn's job-matching AI was biased. The company's solution? More AI*, MIT Tech. Rev. (June 23, 2021), <https://www.technologyreview.com/2021/06/23/1026825/linkedin-ai-bias- ziprecruiter-monster-artificial-intelligence/>.

³³ See EPIC FTC Comments on Commercial Surveillance, *supra* note 7, at 76 (“HireVue—just one competitor in the employment screening field—has over 700 corporate customers[.]”); Complaint of EPIC, *In re HireVue* (Nov. 6, 2019), <https://epic.org/documents/in-re-hirevue/>.

- *Facial recognition.* The commercial use of facial recognition technology has proliferated in stores, stadiums, arenas, and other public accommodations across the country.³⁴
- *Health screening.* ADS has been used to make predictive determinations about patient outcomes and direct courses of treatment.³⁵
- *Education.* PowerSchool claims to hold data on over 75% of K-12 students in North America and provides schools with tools to generate predictions about graduation rates, SAT scores, and other outcomes.³⁶
- *Targeted advertising.* “[A]s AI-powered advertising grows more pervasive and sophisticated, it is doing so without guardrails.”³⁷
- *Housing.* Landlords and property management groups use tenant screening algorithms,³⁸ and Airbnb has used automated risk assessment tools to rate potential guests.³⁹

³⁴ See, e.g., Georgia Gee, *Here Are the Stadiums That Are Keeping Track of Your Face*, Slate (Mar. 14, 2023), <https://slate.com/technology/2023/03/madison-square-garden-facial-recognition-stadiums-list.html>; Sara Morrison, *The World’s Scariest Facial Recognition Company is Now Linked to Everybody From ICE to Macy’s*, Vox (Feb. 28, 2020), <https://www.vox.com/recode/2020/2/26/21154606/clearview-ai-data-breach>.

³⁵ See, e.g., Donna M. Christensen et al., *Medical Algorithms are Failing Communities of Color*, HealthAffairs (Sept. 9, 2021) <https://www.healthaffairs.org/doi/10.1377/forefront.20210903.976632/> (“From consultation programming for glaucoma to automated intake processes in primary care to scoring systems that evaluate newborn’ health conditions, patients regularly encounter these technologies and algorithms whether they know it or not.”); Andrew Wong et al., *External Validation of a Widely Implemented Proprietary Sepsis Prediction Model in Hospitalized Patients*, 181(8) JAMA Intern Med. 1065 (June 2021), <https://pubmed.ncbi.nlm.nih.gov/34152373/>; Tom Simonite, *How an algorithm blocked kidney transplants to Black patients*, WIRED (Oct. 26, 2020), <https://www.wired.com/story/how-algorithm-blocked-kidney-transplants-black-patients/>; Casey Ross & Bob Herman, *Denied by AI: How Medicare Advantage plans use algorithms to cut off care for seniors in need*, Stat (Mar. 13, 2023); <https://www.statnews.com/2023/03/13/medicare-advantage-plans-denial-artificial-intelligence/>.

³⁶ See, e.g., Todd Feathers, *This Private Equity Firm Is Amassing Companies That Collect Data on America’s Children*, The Markup (June 11, 2022), <https://themarkup.org/machine-learning/2022/01/11/this-private-equity-firm-is-amassing-companies-that-collect-data-on-americas-children>; Todd Feathers, *Major Universities Are Using Race as a “High Impact Predictor” of Student Success*, The Markup (Mar. 2, 2021), <https://themarkup.org/machine-learning/2021/03/02/major-universities-are-using-race-as-a-high-impact-predictor-of-student-success>); Daan Kolkman, *“F**k the algorithm?” What the world can learn from the UK’s A-level grading fiasco*, London Sch. Econ. Impact Blog (Aug. 26, 2020), <https://blogs.lse.ac.uk/impactofsocialsciences/2020/08/26/fk-the-algorithm-what-the-world-can-learn-from-the-uks-a-level-grading-fiasco/> (grading algorithms).

³⁷ See, e.g., Harriet Kingbay, *AI and Advertising A consumer perspective* 7 (2020) https://www.harrietkingaby.com/_files/ugd/435e8c_3f6555abb25641be8b764f5093f1dd4f.pdf.

³⁸ See, e.g., Lydia X. Z. Brown, *Tenant Screening Algorithms Enable Racial and Disability Discrimination at Scale, and Contribute to Broader Patterns of Injustice*, Ctr. for Democracy & Tech. (July 7, 2021), <https://cdt.org/insights/tenant-screening-algorithms-enable-racial-and-disability-discrimination-at-scale-and-contribute-to-broader-patterns-of-injustice/>.

³⁹ See Mark Blunden, *Booker beware: Airbnb can scan your online life to see if you’re a suitable guest*, Evening Standard (Jan. 3, 2020), <https://www.standard.co.uk/tech/airbnb-software-scan-online-life-suitable-guest-a4325551.html>.

- *Access to credit.* Algorithms are routinely used to dictate creditworthiness and credit limits.⁴⁰
- *Insurance.* Health insurance companies analyze personal data to determine reimbursement decisions and risk scores.⁴¹

c. Consumers' experiences with automated decisionmaking

Responsive to question II.5

Whether they know it or not, consumers already have extensive experience with automated decisionmaking technologies, including many algorithms that are harmful, invasive, discriminatory, and unfair. Consumers are often unaware when they are subject to an automated decision or whether that determination is adverse, as many of these systems are opaque and hidden from view.

A recent Cisco study highlighted the discrepancy between consumers' and vendors' expectations concerning ADS:

It can be difficult for consumers to understand the algorithms and automated decisions that may impact them directly, such as when qualifying for a loan or getting a job interview. Ninety-six percent (96%) of organizations in our survey believe they have processes already in place to meet the responsible and ethical standards that customers expect, which is up from 87% last year. Yet, the majority of consumers don't see it that way. As reported in the Cisco 2022 Consumer Privacy Survey, 60% of consumers are concerned about how organizations apply and use [artificial intelligence (AI)] today, and 65% already have lost trust in organizations over their AI practices.⁴²

Recent surveys by the Pew Research Center echo these sentiments. A 2022 study found that a larger share of Americans are "more concerned than excited" than are "more excited than concerned" by the increased use of AI in daily life.⁴³ The same study found that consumer concerns

⁴⁰ See, e.g., Genevieve Smith & Ishita Rustagi, *When Good Algorithms Go Sexist: Why and How to Advance AI Gender Equity*, Stan. Soc. Innovation Rev. (Mar. 31, 2021), https://ssir.org/articles/entry/when_good_algorithms_go_sexist_why_and_how_to_advance_ai_gender_equity.

⁴¹ See, e.g., EPIC FTC Comments on Commercial Surveillance, *supra* note 7, at 90.

⁴² *Cisco 2023 Data Privacy Benchmark Study*, Cisco 15 (2023), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2023.pdf.

⁴³ Lee Rainie, Cary Funk, Monica Anderson, & Alec Tyson, *How Americans Think About Artificial Intelligence*, Pew Res. Ctr. (Mar. 17, 2022), <https://www.pewresearch.org/internet/2022/03/17/how-americans-think-about-artificial-intelligence/>.

include potential loss of jobs, privacy considerations, worries that AI's ascent might surpass human skills, a loss of human connection, misuse, and overreliance.⁴⁴ A 2023 survey explored public views on AI in health and medicine and found similar concerns, finding that “there’s significant discomfort among Americans with the idea of AI being used in their own health care.”⁴⁵ In the survey, 60% of U.S. adults expressed that they would feel uncomfortable if their own health care provider relied on AI for things like diagnosing disease or recommending treatments, and 57% said this use of AI would make the patient-provider relationship worse.⁴⁶ More Americans (37%) are concerned that this type of AI would make the security of patients’ records worse compared to the 22% who believed it would improve security.⁴⁷ The report cited a major factor in these views: “[a] majority of the public is unconvinced that the use of AI in health and medicine would improve health outcomes.”⁴⁸

Consumers have experienced numerous documented harms as a result of the use of commercial automated decisionmaking systems (as well as many harms that cannot be conclusively proven due to the opacity of the systems at play). For example:

- *Hiring and employment.* Workers pushed back against being “hired or fired by algorithm,” expressing concern that it could lead to widespread discrimination and unfair treatment.⁴⁹ HireVue, a pre-employment screening company, halted its use of facial recognition after criticism that it was unfair and unlawful (though the company continues to use voice analysis).⁵⁰

⁴⁴ *Id.*

⁴⁵ Alec Tyson, Giancarlo Pasquini, Alison Spencer, & Cary Funk, *60% of Americans Would Be Uncomfortable with Provider Relying on AI in Their Own Health Care*, Pew Res. Ctr. (Feb. 22, 2023), <https://www.pewresearch.org/science/2023/02/22/60-of-americans-would-be-uncomfortable-with-provider-relying-on-ai-in-their-own-health-care/>.

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ *Id.*

⁴⁹ *AI at work: Staff ‘hired and fired by algorithm’*, BBC News (Mar. 25, 2021), <https://www.bbc.com/news/technology-56515827>.

⁵⁰ EPIC, *Facing FTC Complaint From EPIC, Halts Use of Facial Recognition* (Jan. 12, 2021), <https://epic.org/hirevue-facing-ftc-complaint-from-epic-halts-use-of-facial-recognition/>.

- *Criminal justice.* In 2016, ProPublica reported that an algorithm which purported to predict the likelihood of a person committing a future crime was biased against Black individuals.⁵¹ Facial recognition software misidentified an innocent Baltimore man as a match for a suspect in a crime captured by CCTV, and he remained in jails for days due to the algorithmic error.⁵² A Detroit man was wrongfully arrested after facial recognition misidentified him in January 2020.⁵³ A New Jersey man was arrested after a facial recognition system misidentified him as a “high-profile” match and considered pleading to a crime he did not commit after spending 10 days in jail.⁵⁴ Another Detroit man was wrongfully identified by facial recognition software, arrested in front of his children, and detained for 30 hours.⁵⁵
- *Education.* Students in the UK protested after the government proposed using an algorithm to determine their higher education scores during the COVID-19 pandemic.⁵⁶ Students pushed back against harmful and invasive use of remote proctoring AI that purported to determine whether students were cheating during schoolwork.⁵⁷
- *Housing.* Tenants in a rent-stabilized apartment complex in Brooklyn fought back against their landlord’s proposal to subject them to facial recognition for building access.⁵⁸ EPIC warned the Federal Trade Commission (FTC) that AirBnB’s use of an algorithm to determine a renter’s “trustworthiness” was likely unfair and posed a high risk of disparate and unfair impact.⁵⁹

⁵¹ Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, *Machine Bias*, ProPublica (May 23, 2016), <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

⁵² Khari Johnson, *Face Recognition Software Led to His Arrest. It Was Dead Wrong*, WIRED (Feb. 28, 2023), <https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/>.

⁵³ Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives*, WIRED (Mar. 7, 2022), <https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/>.

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ Ammara, “*F*ck the Algorithm*”; *a Rallying Cry For the Future*, Medium (Aug. 17, 2020), <https://medium.com/digital-diplomacy/fuck-the-algorithm-the-rallying-cry-of-our-youth-dd2677e190c>.

⁵⁷ Todd Feathers, *Schools are Abandoning Invasive Proctoring Software after Student Backlash*, Vice (Feb. 26, 2021), <https://www.vice.com/en/article/7k9ag4/schools-are-abandoning-invasive-proctoring-software-after-student-backlash>; see EPIC, *In re Online Test Proctoring Companies* (2020), <https://epic.org/documents/in-re-online-test-proctoring-companies/>.

⁵⁸ Ginia Bellafante, *The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?*, N.Y. Times (Mar. 28, 2019), <https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html>; Erin Durkin, *New York tenants fight as landlords embrace facial recognition cameras*, The Guardian (May 30, 2019), <https://www.theguardian.com/cities/2019/may/29/new-york-facial-recognition-cameras-apartment-complex>.

⁵⁹ Letter from EPIC to the Fed. Trade Comm’n, *In re Airbnb* (Aug. 18, 2022), <https://epic.org/wp-content/uploads/2022/08/EPIC-In-re-Airbnb-supplemental-FTC-letter-1.pdf>.

- *Taxes.* The IRS was forced to backpedal from its plan to use ID.me—a commercial verification tool that relies in part on facial recognition—as the exclusive means of confirming the identity of taxpayers seeking certain tax records.⁶⁰
- *Public Events and Venues.* The entertainment company which owns Madison Square Garden faced public backlash after the venue used facial recognition technology to identify and remove an attorney who worked at a law firm litigating against the company.⁶¹

d. Prevalence of algorithmic discrimination

Responsive to question III.6

It is difficult to precisely quantify the prevalence of algorithmic discrimination because individuals rarely know when they have experienced an adverse algorithmic decision, what factors went into such a decision, or whether the decision was influenced by a protected characteristic or proxy for a protected characteristic. Still, there is abundant evidence⁶² that such discrimination does occur. To take just a few examples:

- A recent study showed that an algorithm used to determine eligibility and prioritization for kidney transplants unfairly prevented Black patients from receiving transplants.⁶³

⁶⁰ Rachel Metz, *After face-recognition backlash, ID.me says government agencies will get more verification options*, CNN (Feb. 9, 2022), <https://www.cnn.com/2022/02/08/tech/idme-facial-recognition-bypass/index.html>.

⁶¹ Kashmir Hill and Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, N.Y. Times (Dec. 22, 2022), <https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html>.

⁶² See, e.g., Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. Mach. Learning Rsch. 1 (2018), <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>.

⁶³ Tom Simonite, *How an algorithm blocked kidney transplants to Black patients*, WIRED (Oct. 26, 2020), <https://www.wired.com/story/how-algorithm-blocked-kidney-transplants-black-patients/> (“One third of Black patients, more than 700 people, would have been placed into a more severe category of kidney disease if their kidney function had been estimated using the same formula as for white patients. . . . In 64 cases, patients’ recalculated scores would have qualified them for a kidney transplant wait list. None had been referred or evaluated for transplant, suggesting that doctors did not question the race-based recommendations.”); see also EPIC FTC Comments on Commercial Surveillance, *supra* note 7, at 69.

- Amazon stopped using a resume-reading algorithm after it discovered that the system taught itself that male candidates were preferable based on the patterns and information that the models were trained on.⁶⁴
- Automated tenant screening reports have wrongfully excluded applicants for housing.⁶⁵

For more examples of discriminatory automated decisionmaking technologies, we refer the Agency to EPIC’s recent comments to the Federal Trade Commission on commercial surveillance.⁶⁶

The White House, federal agencies, multiple states,⁶⁷ and the District of Columbia⁶⁸ have recognized the importance of protections against discriminatory automated decisionmaking technology. The White House’s Office of Science and Technology Policy issued an executive order to address the problem of algorithmic discrimination and equity in AI, explaining that “[a]lgorithmic discrimination occurs when automated systems contribute to unjustified different treatment or impacts disfavoring people based on their race, color, ethnicity, sex (including pregnancy, childbirth, and related medical conditions, gender identity, intersex status, and sexual orientation), religion, age, national origin, disability, veteran status, genetic information, or any other classification protected by law.”⁶⁹ In 2021, the Equal Employment Opportunity Commission launched an initiative to ensure that AI, machine learning, and other emerging technologies comply with federal civil rights laws.⁷⁰

⁶⁴ Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool that Showed Bias against Women*, Reuters (Oct. 10, 2018), <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>.

⁶⁵ Lauren Kirchner & Matthew Goldstein, *Access Denied: Faulty Automated Background Checks Freeze Out Renters*, Mark Up (May 28, 2020), <https://themarkup.org/locked-out/2020/05/28/access-denied-faulty-automated-background-checks-freeze-out-renters>.

⁶⁶ EPIC FTC Comments on Commercial Surveillance, *supra* note 77, at 67–151.

⁶⁷ See Pollyanna Sanderson, Sara Jordan, & Stacey Gray, *Automated Decision-Making Systems: Considerations for State Policymakers*, Future Privacy F. (May 12, 2021), <https://fpf.org/blog/automated-decision-making-systems-considerations-for-state-policymakers/>.

⁶⁸ Stop Discrimination by Algorithms Act of 2021, D.C. Council, B24-0558, 24th Council (D.C. 2021-2022), <https://legiscan.com/DC/bill/B24-0558/2021>.

⁶⁹ Office of Sci. and Tech. Pol’y, *Algorithmic Discrimination Protections*, White House (Oct. 2022), <https://www.whitehouse.gov/ostp/ai-bill-of-rights/algorithmic-discrimination-protections-2/>.

⁷⁰ *Artificial Intelligence and Algorithmic Fairness Initiative*, Equal Emp. Opportunity Comm’n (2021), <https://www.eeoc.gov/ai>.

The Federal Trade Commission has published guidance warning of the “risks, such as the potential for unfair or discriminatory outcomes or the perpetuation of existing socioeconomic disparities” from the use of AI technology.⁷¹ Recognizing that discrimination is common in automated decisionmaking systems, regulators and legislators have begun taking action to address the problem. We encourage the CPPA to do so as well.

III. Cybersecurity audits

The Agency asks what laws currently require cybersecurity audits, to what extent these laws’ requirements align with those of Civil Code § 1798.185(a)(15)(A), and what gaps or weaknesses there may be in these regimes. The Agency also asks about other related evaluations that are currently performed, again asking about alignment with § 1798.185(a)(15)(A) and any gaps or weaknesses in these models. The Agency’s rules will ultimately determine the scope of these audits and the recommended process and oversight mechanisms necessary to ensure that they are thorough and independent.

We make recommendations below for ways that the Agency can establish strong audit standards while respecting the potential for a harmonizing cross-compliance process. In short: there are significant commonalities among data security standards in existing regulatory and voluntary frameworks. Rather than endorse a single existing model, we urge the Agency to establish its own audit rubric based on the strongest common factors among existing standards. We note that the Center for Internet Security’s Critical Security Controls for Effective Cyber Defense (CIS Controls)

⁷¹ Andrew Smith, Dir., FTC Bureau of Consumer Prot., *Using Artificial Intelligence and Algorithms*, Fed. Trade Comm’n Business Blog (Apr. 8, 2020), <https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms>.

is the standard most likely to be in wide adoption by companies doing business in California,⁷² and we recommend that the Agency develop an audit rubric that builds upon the same principles.

a. Why annual cybersecurity audits matter

Consumers rely on the entities that collect their personal data to take the necessary steps to protect that data. These entities are in control of how much personal data they collect, how long they retain it, how (and whether) they dispose of it, and what safeguards they implement to prevent unauthorized access throughout the data lifecycle. There are cost-effective and well-established methods for reducing the likelihood of breaches and for mitigating the harm of unauthorized access when it does occur. Poor data security practices increase the likelihood and severity of breaches, which in turn increase the risk of identity theft and other downstream harms to consumers. Governing Magazine recently reported that California led the nation in data breaches in the five-year period 2017-2021, with more than 325,000 victims collectively losing more than 3.7 billion dollars (representing more than 18% of losses nationwide).⁷³

Downstream consumer harms resulting from data breaches can include identity theft and other forms of account compromise. The Federal Trade Commission (FTC) reported high levels of benefits fraud in 2020 and 2021, in addition to credit fraud increasing from 27% of identity theft

⁷² See Kamala D. Harris, Attorney General, *California Data Breach Report* 30 (2016), <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf> (“Recommendation 1: The 20 controls in the Center for Internet Security’s Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet.”). The most recent version of these controls were published two years ago. See Ctr. Internet Sec., *CIS Critical Security Controls Version 8* (May 2021), <https://www.cisecurity.org/controls/v8>.

⁷³ Kevin Smith, *California Had the Most Data Breaches in the Last Five Years*, Governing (July 26, 2022), <https://www.governing.com/security/california-had-the-most-data-breaches-in-the-last-five-years> (citing to Forbes Advisor report).

reports in 2020 and 2021 to 40% of reports in 2022.⁷⁴ In 2021, the Department of Justice found that 68% of victims of identity theft suffered \$1 or more in direct financial losses with their most recent incident of identity theft⁷⁵ and estimated that this fraud cost the U.S. economy more than \$15 billion.⁷⁶ For example, in late 2020, websites used to generate auto insurance quotes were exploited to obtain personal data later used to submit fraudulent claims for pandemic and unemployment benefits.⁷⁷

The impacts of identity theft can be far-reaching, discovered only after downstream harms have occurred (e.g., through a collections notice for a bill the consumer neither incurred nor knew of), and difficult to remedy after the fact. A Government Accountability Office report indicated that past victims have “lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft.”⁷⁸ Yet these harms do not appear on the victim’s bank statement or credit report and can be nearly impossible to control where a Social Security Number (SSN) is used (by virtue of the role the SSN plays as a government and private-sector identifier).⁷⁹

⁷⁴ FTC, *Consumer Sentinel Network: Data Book 2022* at 9 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf (calculating percentage by taking fraction of number of reports by theft type out of total identity theft reports); FTC, *Consumer Sentinel Network: Data Book 2021* at 9 (2021), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf (same methodology); FTC, *Consumer Sentinel Network: Data Book 2020* at 9 (2020), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf (same methodology).

⁷⁵ Bureau of Just. Stat., Dep’t of Just., *Victims of Identity Theft, 2018* at 9 (Apr. 2020), <https://bjs.ojp.gov/content/pub/pdf/vit18.pdf>.

⁷⁶ See *id.* at 1 (\$15.1 billion in total financial losses due to identity theft where the victim lost \$1 or more). This was also true in the DOJ’s two prior reports. See Bureau of Just. Stat., Dep’t of Just., *Victims of Identity Theft, 2016* at 1 (Jan. 2019), <https://bjs.ojp.gov/content/pub/pdf/vit16.pdf> (\$17.5 billion); Bureau of Just. Stat., Dep’t of Just., *Victims of Identity Theft, 2014* at 7 (Sept. 2015), <https://bjs.ojp.gov/content/pub/pdf/vit14.pdf> (\$15.4 billion).

⁷⁷ Industry Letter Re: Cyber Fraud Alert to N.Y. State Dep’t of Fin. Servs., Cybersecurity Div. (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert.

⁷⁸ U.S. Gov’t Accountability Office, GAO-14-34, *Agency Responses to Breaches of Personally Identifiable Information Need to be More Consistent* 11 (2013), <http://www.gao.gov/assets/660/659572.pdf>.

⁷⁹ Br. of Amicus Curiae EPIC at 14, *Storm v. Paytime, Inc.*, No. 15-3690 (3d Cir. Apr. 18, 2016), <https://epic.org/documents/storm-v-paytime-inc/>.

To make matters worse, a stolen SSN, unlike a stolen credit card, cannot be effectively cancelled or replaced.⁸⁰

Although it is difficult to remedy the harms of identity theft after the fact, preventing the underlying breach is neither difficult nor expensive. The California Attorney General's Office concluded that many of the hundreds of breaches it studied could have been prevented, or detected and corrected more rapidly, by implementation of its recommended data security controls.⁸¹ More broadly, the Department of Homeland Security has estimated that 85% of data breaches were preventable,⁸² and more recently the Internet Society has estimated 95% of breaches could have been prevented.⁸³ The FTC has often noted that reasonable security measures are relatively low-cost.⁸⁴ Security technologist and fellow at Harvard Kennedy School Bruce Schneier recently observed in the New York Times:

In all of these cases, the victimized organizations could have very likely protected our data better, but the reality is that the market does not reward healthy security. Often customers aren't even able to abandon companies with poor security practices, as many of them build "digital moats" to lock their users in. Customers don't abandon companies with poor security practices. Hits to the stock prices quickly recover. It's a

⁸⁰ *Id.* at 13.

⁸¹ See Harris, *supra* note 72, at 32.

⁸² Dep't of Homeland Sec. Comput. Emergency Readiness Team, TA15-119, *Alert: Top 30 Targeted High Risk Vulnerabilities* (2016), <https://www.us-cert.gov/ncas/alerts/TA15-119A>.

⁸³ Internet Society's Online Trust Alliance, *2018 Cyber Incident & Breach Trends Report 3* (July 9, 2019), https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf.

⁸⁴ See, e.g., Complaint, *In re Residual Pumpkin Entity, LLC, d/b/a CafePress*, FTC File No. 1923209 at ¶ 11(a), 11(i)(i) (Jun. 23, 2022), <https://www.ftc.gov/legal-library/browse/cases-proceedings/1923209-cafepress-matter> [hereinafter *CafePress*]; Complaint, *In re SkyMed International, Inc.*, FTC File No. 1923140 at ¶ 23 (Jan. 26, 2021), <https://www.ftc.gov/legal-library/browse/cases-proceedings/1923140-skymed-international-inc-matter> [hereinafter *SkyMed*]; Complaint, *In re InfoTrax Systems, L.C.*, FTC File No. 1623130 at ¶ 11 (Dec. 30, 2019), <https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3130-infotrax-systems-lc> [hereinafter *InfoTrax*]; Complaint, *In re LightYear Dealer Technologies, LLC*, FTC File No. 1723051 at ¶ 22 (Sept. 6, 2019), <https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3051-lightyear-dealer-technologies-llc-matter> [hereinafter *LightYear*]; Complaint, *FTC v. Equifax, Inc.*, No. 1:2019-cv-03297 at ¶¶ 23(A)(iv), 24 (N.D. Ga. Jul. 22, 2019), <https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3203-equifax-inc> [hereinafter *Equifax*]; Complaint, *FTC v. Ruby Life Inc. d/b/a AshleyMadison.com*, No. 1:16-cv-02438 at ¶ 42 (D.D.C. Dec. 14, 2016), <https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3284-ashley-madison> [hereinafter *AshleyMadison*]; Complaint, *In re Lenovo, Inc.*, FTC File No. 1523134 at ¶ 25 (Jan. 2, 2018), <https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3134-lenovo-inc> [hereinafter *Lenovo*].

classic market failure of a powerful few taking advantage of the many, and that failure is one that only representation through regulation can fix.⁸⁵

The burden represented by annual audits pales in comparison to the burdens consumers suffer from unauthorized access to their data. As such, the costs of harm to consumers and to the American economy (e.g., due to fraud facilitated by identity theft) that result from data breaches would be better internalized as preventative data security costs incurred by the entities best positioned to prevent the harm from occurring in the first place.

Cybersecurity audits can identify deficient practices and help companies to shore up vulnerabilities before a breach occurs, mitigating the damage or perhaps preventing it entirely. However, it is important to note that it remains the company's responsibility to maintain best practices in between annual audits.⁸⁶ If the audit process amounts to a standalone annual exercise in compliance, it is unlikely to meaningfully improve data security. The Agency has recognized this through its emphasis on the thoroughness and independence of audits and through its questions interrogating the weaknesses and gaps in existing data security assessment models. The Agency is not seeking to mandate completion of a box-checking chore; it has been tasked with identifying a methodology that can best address a core deficiency that persistently hurts trust in businesses and that could continue to leave consumers vulnerable. Although it is unfortunate that deficient data security has been such a needlessly persistent problem, the Agency can benefit from the lessons learned over the last decade to ensure that its audit requirements entail more than box-checking and blind approvals, but rather establish a new and robust standard for businesses entrusted with consumer data.

⁸⁵ Bruce Schneier, *The Uber Hack Exposes More Than Failed Data Security*, N.Y. Times (Sept. 26, 2022), <https://www.nytimes.com/2022/09/26/opinion/uber-hack-data.html>.

⁸⁶ In the context of credit card payments and data security, for example, Verizon consistently reports that 44% or more of organizations fail to maintain PCI-DSS compliance in between annual compliance validations (most recently more than 56% failed to maintain compliance). See Verizon, *2022 Payment Security Report* 82 (Sept. 2022), <https://www.verizon.com/business/resources/T38f/reports/2022-payment-security-report.pdf>.

b. Scope of audits

Responsive to questions 1.1, 2, and 5

The implicit goal of § 1798.185(a)(15)(A) is to mitigate risks to the privacy and security of consumers' personal information by establishing factors that will reduce that risk and by compelling businesses to address those factors through an annual audit process. Accordingly, the CPPA's audit requirements should identify the right factors for an audit to consider and ensure that the audit process is thorough and independent. There are several provisions common among current data security laws and frameworks which should inform the scope of the annual audit required under § 1798.185(a)(15)(A). These include access controls, secure password practices, user authentication, segmentation of systems, traffic monitoring, ongoing security reviews, data mapping, data minimization, staying current on known vulnerabilities, employee training, overseeing service providers and product integrations, and requiring additional security precautions where appropriate (e.g., remote access and storing and/or transmitting sensitive information).

These provisions are not exhaustive of all issues that could create or exacerbate system vulnerabilities,⁸⁷ but each of them should apply to companies at a level commensurate with the scope and scale of the type and volume of data they collect.⁸⁸ Just as heightened measures should be required for riskier processing or processing of more sensitive types of data, less stringent measures may be required for companies collecting smaller amounts of data or types of data that inflict less severe harms if breached (e.g., state of residence as opposed to Social Security Number). This “risk-based approach” to data security is already in place in the banking industry,⁸⁹ and has been enacted

⁸⁷ Device mapping and encryption, for example, were not addressed above.

⁸⁸ William McGeeveran, *The Duty of Data Security*, 103 Minn. L. Rev. 1135, 1179 (2018), https://www.minnesotalawreview.org/wp-content/uploads/2019/02/1McGeeveran_FINAL.pdf (noting that across multiple data security frameworks “the duty of data security scales up or down in proportion to the resources and risk profile of each data custodian”).

⁸⁹ See, e.g., David W. Perkins, *Tailoring Bank Regulations: Differences in Bank Size, Activities, and Capital Levels* (Dec. 21, 2017), <https://digital.library.unt.edu/ark:/67531/metadc1094396/>.

as data security policy at the state level.⁹⁰ It is likely that a cottage industry will emerge to assist companies with a data security regime that grows as the company's data collection and processing grows (or as those data practices become riskier). We have provided additional detail about how these issues are handled in current laws and frameworks in Appendix 1.

A number of current federal laws impose data security obligations, including the Health Insurance Portability and Accountability Act (HIPAA),⁹¹ Children's Online Privacy Protection Act (COPPA),⁹² Gramm-Leach-Bliley Act (GLBA) (specifically the Safeguards Rule),⁹³ and Federal Credit Report Act (FCRA).⁹⁴ Several states other than California also have data security laws, including Massachusetts,⁹⁵ New York,⁹⁶ and Oregon.⁹⁷ Existing frameworks include those proposed by the Financial Industry Regulatory Authority (FINRA),⁹⁸ National Institute of Standards and

⁹⁰ See, e.g., 201 Mass. Code Regs. 17.03(1) (2010), <https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the/download> (requiring a security program include “administrative, technical, and physical safeguards that are appropriate to: (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information”).

⁹¹ 45 C.F.R. pt. 160; 45 C.F.R. pt. 164.

⁹² 16 C.F.R. pt. 312; 16 C.F.R. §§ 312.3(e), 312.8.

⁹³ 16 C.F.R. pt. 314.

⁹⁴ 16 C.F.R. pt. 682.

⁹⁵ 201 Mass. Code Regs. 17.00 (2010).

⁹⁶ N.Y. Comp. Codes R. & Regs. tit. 23, § 500 (2022) (NYDFS regs); N.Y. Gen. Bus. Law, § 899-bb (2020) (SHIELD Act data security provisions).

⁹⁷ Or. Rev. Stat. tit. 50, § 646A.622 (2021).

⁹⁸ See, e.g., FINRA, *Report on Cybersecurity Practices* (Feb. 2015), https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf [hereinafter *FINRA 2015*]; FINRA, *Core Cybersecurity Threats and Effective Controls for Small Firms* (May 2022), https://www.finra.org/sites/default/files/2022-05/Core_Cybersecurity_Threats_and_Effective_Controls-Small_Firms.pdf [hereinafter *FINRA 2022*].

Technology (NIST),⁹⁹ Cyber and Infrastructure Security Agency (CISA),¹⁰⁰ and Federal Financial Institutions Examination Council (FFIEC),¹⁰¹ as well as industry standards such as the Payment Card Industry Data Security Standards (PCI-DSS).¹⁰²

Notably in 2016, then-Attorney General of California Kamala Harris set the expectation that businesses would conform their data security practices to the requirements of the Center for Internet Security (CIS) framework, stating that “[t]he set of 20 [CIS] Controls constitutes a minimum level of security—a floor—that any organization that collects or maintains personal information should meet.”¹⁰³ The 2016 CIS framework outlined explicitly parallel recommendations from NIST, International Organization for Standardization (ISO), HIPAA, FFIEC, and PCI-DSS frameworks. The FTC has also identified deficient data security practices in a number of its Section 5 enforcement actions over the last 10 years.¹⁰⁴ Cyber risk insurance guidance continues to play an important role in shaping data security practices and to indicate what priorities have been

⁹⁹ NIST, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1* (Apr. 16, 2018), <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> [hereinafter *NIST 1.1*]; NIST, *Getting Started with the NIST Cybersecurity Framework: A Quickstart Guide* (Updated Apr. 19, 2022), <https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide> [hereinafter *NIST Quickstart*] (providing a helpful high-level overview).

¹⁰⁰ CISA, *Cross-Sector Cybersecurity Performance Goals* (2022), https://www.cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf [hereinafter *CISA Goals*]. Currently CISA has only offered guidelines, but new breach reporting rules promulgated under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) may be mandatory.

¹⁰¹ See, e.g., FFIEC, *FFIEC Cybersecurity Assessment Tool: Inherent Risk Profile*, https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017_Inherent_Risk_Profile.pdf.

¹⁰² See, e.g., *Requirements and Testing Procedures Version 4.0*, PCI Security Standards Council (Mar. 2022), https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf.

¹⁰³ See Harris, *supra* note 72, at 31 (“The controls are intended to apply to organizations of all sizes and are designed to be implementable and scalable.”); *id.* at Appendix B. Note the numbering on these controls have been updated since the 2016 Data Breach Report—most recently in CIS Critical Security Controls Version 8 (May 2021), which is the version numbering we cite to in Appendix 1.

¹⁰⁴ See, e.g., First Am. Complaint, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015), <https://www.ftc.gov/legal-library/browse/cases-proceedings/1023142-x120032-wyndham-worldwide-corporation> [hereinafter *Wyndham*]; *CafePress*; *SkyMed*; *InfoTrax*; *LightYear*; *Equifax*; *AshleyMadison*; *Lenovo*; Complaint, *FTC v. D-Link Corp.*, No. 3:17-CV-00039-JD (N.D. Cal. Mar. 20, 2017), <https://www.ftc.gov/legal-library/browse/cases-proceedings/132-3157-x170030-d-link> [hereinafter *D-Link*].

emphasized by businesses with explicit incentives to mitigate the risks of breaches. For example, several cyber insurance companies ask prospective insured about firewalls, password strength, multi-factor authentication, and patching known vulnerabilities in their own risk assessment questionnaires.¹⁰⁵ Other laws and frameworks (e.g. GLBA) can fall short in a number of ways, including by assuming that a consumer who has not opted out of processing is aware of and accepts the risks of that processing, by allowing data sharing without concern for data security, and by having limited applicability, e.g. only governs health care providers, only protects current customers, etc.

Based on CIS controls, FTC actions, cyber insurance priorities, and other laws and frameworks, the audits required by § 1798.185(a)(15)(A) should include at a minimum:

- data mapping;
- data minimization;
- access controls;
- secure password practices;
- user authentication;
- segmentation of systems;
- traffic monitoring;
- ongoing security reviews;
- staying current on known vulnerabilities;
- employee training; and
- overseeing service providers and product integrations.

Additional security precautions may be necessary where appropriate (e.g., remote access or processing sensitive information).

¹⁰⁵ See McGeeveran, *supra* note 88, at 1172–73 (citing to Sample cyber insurance applications, IAPP, <https://iapp.org/resources/article/sample-cyberinsurance-applications/> (last visited Mar. 17, 2023)) (noting that all three companies inquire about firewalls, password strength, and multifactor authentication in their risk assessment questionnaires).

The Agency should also establish a set of best practices as benchmarks for its required audit categories that incorporates but is not necessarily limited to the list above. It may be helpful to present the recommended practices as basic cybersecurity hygiene for the modern threat environment.

c. Deficiencies in existing authorities

Responsive to question I.1

The Agency specifically asks about gaps or weaknesses in existing data security regimes. Many laws are limited in applicability: HIPAA only applies to health care providers (which may not include period tracker apps),¹⁰⁶ and although GLBA applies clearly to current customers, it is less clear whether its data security-focused Safeguards Rule applies to former customers.¹⁰⁷ Relatedly, several laws allow for disclosure of information to third parties who are not necessarily subject to the same data security requirements as the regulated entity.¹⁰⁸ Two recent breaches of AT&T subscriber data underscore the importance of extending data security requirements to third parties with access to consumer data.¹⁰⁹ Overseeing service providers and product integrations must be included within the scope of the Agency's annual audits if only for this reason.

¹⁰⁶ See, e.g., Charles Ornstein, *Federal Patient Privacy Law Does Not Cover Most Period-Tracking Apps*, ProPublica (July 5, 2022), <https://www.propublica.org/article/period-app-privacy-hipaa>.

¹⁰⁷ See Fed. Trade Comm'n, *How to Comply with the Privacy of Consumer Financial Information Rule the Graham-Leach-Bliley Act*, <https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act> (last visited Mar. 27, 2023) (data security rules apply to customers but it is possible for an organization to have consumers who do not maintain a customer relationship; former customers seem to be considered consumers not customers); 16 C.F.R. pt. 314.3 (protecting customer information); 16 C.F.R. pt. 314.2 (defining "customer information", "customer", and "consumer").

¹⁰⁸ As a few examples: FCRA/FACTA and GLBA allow for sharing with affiliates, HIPAA/HITECH allow exceptions for marketing and for collecting payments, GLBA allows exceptions for "necessary services" and allows contracts enforcing confidentiality but does not require contracts enforcing data security.

¹⁰⁹ See David Lumb, *AT&T Vendor Data Breach Exposed 9 Million Customer Accounts*, CNET (Mar. 9, 2023), <https://www.cnet.com/tech/mobile/at-t-vendor-data-breach-exposed-9-million-customer-accounts/>; see also Brian Krebs, *It Might Be Our Data, But It's Not Our Breach*, Krebs on Security (Aug. 11, 2022), <https://krebsonsecurity.com/2022/08/it-might-be-our-data-but-its-not-our-breach/>.

Additionally, GLBA and prescreening under FCRA are premised on an opt-out version of the notice and choice model of consumer consent, with notoriously difficult opt-out mechanisms.¹¹⁰ The Agency must include data mapping and data minimization within the scope of its annual audits to ensure the company is aware of what data it actually needs and how that data should be protected, rather than permitting companies to rely on outdated methodologies that attempt to shift the burden to consumers.¹¹¹

Some laws do not incorporate established best practices in their data security requirements. For example, the GLBA Safeguards Rule does not explicitly require segmentation of systems,¹¹² despite the prevalence of that best practice factor in CIS Controls, FTC enforcement actions, and voluntary frameworks developed by expert entities like CISA and NIST.¹¹³

d. Thoroughness and independence of auditors

Responsive to questions I.1, 2, and 4

Section 1798.185(a)(15)(A) requires audits that are thorough and independent. We understand “thorough” to require actual analysis and not merely a checkbox exercise. We understand “independent” to mean operating without the audited company’s influence. As one example, an audit should not merely report the audit subject’s response as to whether the organization has a strong

¹¹⁰ See, e.g., Elizabeth D. De Armond, A Dearth of Remedies, 113 Penn St. L. Rev. 1, 18 (2008) (noting that even a consumer who seeks to opt out may not have their decision respected if the consumer fails to precisely follow opt-out instructions); EPIC, *The Fair Credit Reporting Act (FCRA)*, <https://epic.org/fcra/> (2023) (discussing the problems with an opt-out model for prescreening).

¹¹¹ See, e.g., Remarks of Comm’r Rebecca Kelly Slaughter, FTC Hearing #12, The FTC’s Approach to Consumer Privacy (Apr. 10, 2019), https://www.ftc.gov/system/files/documents/public_statements/1513009/slaughter_remarks_at_ftc_approach_to_consumer_privacy_hearing_4-10-19.pdf; *Data Minimization White Paper*, *supra* note 23, at 5 (2022), <https://epic.org/documents/how-the-ftc-can-mandate-data-minimization-through-a-section-5-unfairness-rulemaking/> (“The current ‘notice and choice’ regime, in which consumers are expected to read extensive privacy policies and make ‘all or nothing’ decisions about whether to use an online service or app, makes it impossible for consumers to meaningfully participate in the market while protecting their privacy.”).

¹¹² *FTC Safeguards Rule: What Your Business Needs to Know*, FTC, <https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know> (last visited Mar. 17, 2023).

¹¹³ See Appendix 1.

password policy in place; rather, the auditor should actually attempt to set up access with a weak password to see if the policy has been implemented and works as intended.¹¹⁴

Twitter whistleblower Peter “Mudge” Zatko remarked in Congressional testimony last year:

“[H]ow was Twitter still operating like this? Since there was a 2011 consent decree that was aimed at addressing a fair amount of this? . . . One, there were a lot of evaluations and examinations, which were interview questions. So essentially, the organization was allowed to grade their own homework. Did you make things better? Yes, we did. Okay, check. There wasn’t a lot of ground truth. There wasn’t a lot of quantified measurements. And a fair amount of the interviews came from companies, auditors that Twitter themselves were able to hire. So I think that’s a little bit of a maybe conflict of interest.”¹¹⁵

Mudge suggested the solution include “accountability, and setting quantitative goals and standards that can be measured and audited independently” in order to “change management structures, and drive change in companies when it’s needed such as this.”¹¹⁶

We urge the Agency to establish quantitative goals and standards, requiring actual investigation and analysis and not merely interviews. We also encourage the Agency to establish processes that reduce the likelihood of a conflict of interest as described in Mudge’s testimony. For example, the Agency could certify auditors and randomize which get assigned to which company.

e. Triggers for the audit requirement and cross-compliance

Responsive to questions I.1, 2, and 3

The Agency asks about the benefits and drawbacks for consumers if it accept audits completed by businesses to comply with existing laws and asks how businesses should demonstrate that those audits comply with the CPPA’s requirements. Because laws like GLBA have significant gaps and weaknesses—including failing to incorporate best practice factors, failing to capture data

¹¹⁴ Kevin G. Coleman, *Security Assessment or Security Audit?*, infoTECH Spotlight (Sept. 21, 2009), <https://it.tmcnet.com/topics/it/articles/64874-security-assessment-security-audit.htm>.

¹¹⁵ Data Security at Risk: Testimony from a Twitter Whistleblower: Hearing Before the S. Comm. on the Judiciary, 117th Cong. (2022) (testimony of Peter Zatko), <https://www.judiciary.senate.gov/meetings/data-security-at-risk-testimony-from-a-twitter-whistleblower>.

¹¹⁶ *Id.*

security risks at third party entities, and allowing companies to rely on purported consumer consent rather than strengthening inadequate data security practices—the Agency should measure compliance against its own standards. The Agency should therefore not accept audits geared towards other legal frameworks as compliant with the CCPA cybersecurity audit requirement.

However, the Agency could establish supplemental requirements that would allow companies to use existing audits in conjunction with specific supplemental reviews to demonstrate compliance. For example, the GLBA Safeguards Rule does not explicitly require segmentation of systems,¹¹⁷ so a company seeking to demonstrate compliance with § 1798.185(a)(15)(A) through its GLBA reporting might need to provide supplemental information regarding practices such as internal firewalls. Similarly, the Agency could require companies to supplement their existing reporting to ensure data that will be shared with affiliates or third-party vendors (e.g., for marketing or payment collections purposes) will be appropriately secured. The Agency can get ahead of industry arguments that existing reporting is sufficient by clarifying upfront what supplemental information it will require if companies intend to rely on existing audits.

Additionally, if supplemental information is required, to the extent that the existing audit includes a holistic analysis component, that analysis should be revisited taking into account the supplemental information which was not required in the existing audit. The FFIEC framework for example concludes with an overall inherent risk profile rating, based on multiple factors that framework takes into account, such as number of devices, use of person-to-person payments, and access controls.¹¹⁸ Factors such as data minimization however are outside its scope. If the Agency decides to accept audits based on the FFIEC framework, it should require an updated inherent risk

¹¹⁷ *FTC Safeguards Rule: What Your Business Needs to Know*, *supra* note 112.

¹¹⁸ See FFIEC, *FFIEC Cybersecurity Assessment Tools ver. 1.1* at app. A, (May 2017), https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_Appendix_A_May_2017.pdf.

profile rating that reflects all of the key protocols of priority to the Agency, not merely those recommended in the FFIEC model. However, if an FFIEC-based audit already incorporates this “supplemental” information (e.g., data minimization), any revision to the audit would likely be unnecessary.

Audits must also provide detail sufficient to demonstrate that the auditor was thorough. Companies should not be able to merely certify that they have fully addressed the critical areas considered in a cybersecurity audit without actually improving their practices.¹¹⁹ The Agency should not deem an entity audit process compliant unless that entity clearly establishes that its audit process was sufficiently independent and that it thoroughly reviewed all of the best practice factors identified in the Agency’s regulatory framework.

How a business might demonstrate that existing audits comply with the requirements of § 1798.185(a)(15)(A) will likely depend upon what requirements the Agency actually imposes in its audits. Regardless of how the Agency chooses to define the scope of annual cybersecurity audits, we recommend that the Agency require companies to submit any audits intended to satisfy 1798.185(a)(15)(A). This will equip the Agency to analyze trends, propose new supplemental reporting requirements that better reflect the evolving threat landscape, and offer education and trainings for common weaknesses identified from reviewing the submitted audits.¹²⁰

¹¹⁹ See, e.g., R. Bradley McMahon, *After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why Is Identity Theft the Most Prevalent Crime in America?*, 49 Vill. L. Rev. 625, 644 (2004) (“Financial institutions have sent out billions of notices without any change in privacy materializing.”). Although the author discussed privacy concerns, the critique of compliance disconnected from reality is applicable to data security as well.

¹²⁰ Indeed Profs. Solove and Hartzog argue that “[g]overnment organizations could act proactively to hold companies accountable for bad practices before a breach occurs, rather than waiting for an attack. This strategy would strengthen data security more than the current approach of focusing almost entirely on breached organizations.” Daniel J. Solove & Woodrow Hartzog, *Data Vu: Why Breaches Involve the Same Stories Again and Again*, Sci. Am. (July 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4326723.

§ 1798.185(a)(15)(A) requires businesses to perform an annual cybersecurity audit when their processing of consumers’ personal information presents significant risk to consumers’ privacy or security. It also establishes that the size and complexity of the business and the nature and scope of data processing activities should inform whether that data processing may result in significant security risks, thereby triggering the audit requirement. We urge the Agency to err on the side of inclusion, especially as the Agency’s authority to require less frequent or less robust assessments from smaller and simpler organizations is ambiguous. This means that data held by organizations that do not satisfy the “significant risk” threshold could be stored or shared without adequate data security protections. As we have noted in a prior filing,¹²¹ “significant risk” should be understood to mean nontrivial risk rather than exceptional risk. We reiterate here that this interpretation not only aligns with the goals of the CPRA but also aligns with Civil Code § 1798.81.6, which defines “significant risk” as a risk that “*could reasonably result* in a breach of the security of the system . . . of personal information[.]”¹²²

We also maintain that Senator Kirsten Gillibrand’s Data Protection Act¹²³ offers a useful compilation of hazardous data processing activities. However, regarding the “nature and scope of data processing” language in § 1798.185(a)(15)(A), again the Agency should consider whether the processing could reasonably result in compromising the privacy or security of consumer data, not merely whether the data is particularly sensitive. For example, while a definition of sensitive information might not include the list of websites for which a consumer maintains a user account, publicizing that list could compromise the consumer’s privacy (as it may reveal religious, health, sexual, or other personal information) and expose the consumer to more sophisticated phishing

¹²¹ EPIC et al. 2021 CCPA Comments, *supra* note 3, at 3.

¹²² Civ. Code § 1798.81.6(c) (emphasis added).

¹²³ S. 2134 § 2(11), 117th Cong. (2021), <https://www.congress.gov/bill/117th-congress/senate-bill/2134/text>.

attacks. Not limiting the audits to sensitive data processing is also consistent with the risk assessment language of the statute, which requires risk assessments even when a business does not process special categories of personal data that qualify as “sensitive.”¹²⁴

Factoring in “the size and complexity of the business” should be secondary to the magnitude of the possible harm. An organization that is too undercapitalized to adequately safeguard consumer data should not be permitted to collect it, as that would expose the data to disproportionate risk of unauthorized access.

f. Other important principles

Responsive to questions 1.1, 2, and 3

We urge the Agency to prioritize best practice over harmonization, not only because it will result in the best protections for consumers but also because it is likely that subsequent regulations will complicate an approach primarily driven by harmonization. For example, new regulations will likely result from the recent Whitehouse National Cybersecurity Strategy¹²⁵ and the FTC’s rulemaking on commercial surveillance and data security.¹²⁶ In a breach reporting context specifically, new regulations could also include Cyber and Infrastructure Security Agency (CISA)

¹²⁴ Civ. Code § 1798.140(ae).

¹²⁵ See *FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy*, The White House (Mar. 2, 2023), <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/>.

¹²⁶ See Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (Aug. 22, 2022), <https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security>.

rules under CIRCIA,¹²⁷ an update by the Federal Communications Commission (FCC) to its CPNI rules,¹²⁸ and the Securities and Exchange Commission (SEC)’s rulemaking on cyber incidents.¹²⁹

IV. Risk assessments

A risk assessment, also known as a data protection impact assessment or privacy impact assessment, is an analysis of how and why personally identifiable information will be collected, processed, stored, and transferred. The term may also describe an assessment of the privacy and other data-driven risks posed by the use of an algorithm or automated decision-making system. The objective of a risk assessment is to “anticipate[] problems, seeking to prevent, rather than to put out fires.”¹³⁰ When implemented properly, risk assessments force institutions to carefully evaluate the full spectrum of privacy and data-driven risks of a contemplated processing activity, to identify and implement measures to mitigate those risks, and to determine whether the processing activity can be justified in light of any risks that cannot be fully mitigated. A risk assessment can also provide regulators and the public with vital information about processing activities that may pose a threat to privacy and civil rights.

A risk assessment should not be a simple box-checking exercise or a static, one-off undertaking. Rather, it is “a process which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project. It is a process that should continue until

¹²⁷ See *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*, Cybersec. & Infrastructure Sec. Agency (2022) <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia>.

¹²⁸ See *FCC Proposes Updated Data Breach Reporting Requirements*, Fed. Commc’ns. Comm’n (Jan. 6, 2023), <https://www.fcc.gov/document/fcc-proposes-updated-data-breach-reporting-requirements>.

¹²⁹ See *SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*, Sec. & Exch. Comm’n (Mar. 9, 2022), <https://www.sec.gov/news/press-release/2022-39>; *SEC Reopens Comment Period for Proposed Cybersecurity Risk Management Rules and Amendments for Registered Investments and Funds*, Sec. & Exch. Comm’n (Mar. 15, 2023), <https://www.sec.gov/news/press-release/2023-54>.

¹³⁰ *Privacy Impact Assessment* v (David Wright & Paul de Hert, eds., 2012) (foreword by Gary T. Marx).

and even after the project has been deployed.”¹³¹ Or as the Office of Management and Budget warns federal agencies, a risk assessment “is not a time-restricted activity that is limited to a particular milestone or stage of the information system or [personally identifiable information] life cycles. Rather, the privacy analysis shall continue throughout the information system and PII life cycles.”¹³²

As the Agency develops regulations concerning the scope, frequency, content, and availability of risk assessments under the CCPA, we urge you to bear these hallmarks of effective risk assessments in mind. Specifically, we recommend that the Agency (a) draw on the strongest risk assessment frameworks that have already been developed, including those in the Colorado Privacy Act and the General Data Protection Regulation; (b) adopt a definition of “significant risk” which is both inclusive and flexible enough to account for emerging data-driven risks; (c) direct businesses to include content analogous to what is required under the GDPR and recently-developed Colorado Privacy Act regulations; (d) not allow businesses to rely on risk assessments from another jurisdiction unless the assessments (and any necessary addenda) would independently satisfy CCPA requirements; (e) direct businesses to submit each risk assessment in full to the Agency and to prepare a summarized or redacted version for public consumption; and (f) not extend special treatment to businesses that have less than \$25 million in annual gross revenues if they otherwise qualify as a CCPA-covered business based on their processing of personal information.

a. Existing laws and frameworks.

Responsive to questions I.1

Although there are a variety of risk assessment frameworks in use, we highlight five in particular as valuable points of reference for the Agency:

¹³¹ *Id.* at 5–6.

¹³² Off. of Mgmt. & Budget, Exec. Off. of the President, *OMB Circular A-130: Managing Information as a Strategic Resource* app. II at 10 (2016).

- Article 35 of the General Data Protection Regulation¹³³ and implementing guidance;¹³⁴
- The Colorado Privacy Act¹³⁵ and implementing regulations;¹³⁶
- The Federal Chief Information Officers Council Algorithmic Impact Assessment tool;¹³⁷
- The Canadian Government’s Algorithmic Impact Assessment tool;¹³⁸ and
- The E-Government Act of 2002¹³⁹ and implementing guidance.¹⁴⁰

The relevant strengths and gaps of these frameworks are addressed throughout the remainder of this section.

b. Significant risk

Responsive to question II.3

Establishing a strong and effective definition of the term “significant risk” in the CCPA is vital.¹⁴¹ Under section 1798.185(a)(15), the Agency must issue regulations requiring “businesses whose processing of consumers’ personal information presents *significant risk* to consumers’ privacy or security” to conduct risk assessments.¹⁴² The CCPA does not define “significant risk,” but the Agency should interpret this term broadly to maximize the protection afforded to California residents and to ensure that businesses routinely evaluate the hazards of processing and storing personal information. A “significant risk” must be understood to mean a *material* or *nontrivial* risk rather than an exceptional or unusual one. Establishing too high a threshold for audits and risk

¹³³ Commission Regulation (EU) 2016/679, art. 35, 2016 O.J. (L 119).

¹³⁴ Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679* at (Oct. 4, 2017), <https://ec.europa.eu/newsroom/article29/items/611236>.

¹³⁵ C.R.S. § 6-1-1309.

¹³⁶ 4 CCR 904-3, <https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf>.

¹³⁷ *Algorithmic Impact Assessment*, CIO.gov (last visited Mar. 27, 2023), <https://www.cio.gov/aia-cia-js/>.

¹³⁸ *Algorithmic Impact Assessment tool*, Gov’t of Canada (Jan. 19, 2023), <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html>.

¹³⁹ E-Government Act, Pub. L. No. 107-347, § 208(b)(2)(B)(ii), 116 Stat. 2899, 2901 (Dec. 17, 2002).

¹⁴⁰ OMB, *OMB Circular A-130: Managing Information as a Strategic Resource* (2016), app. II at 10.

¹⁴¹ Civ. Code § 1798.185(a)(15).

¹⁴² *Id.* (emphasis added).

assessments would unduly limit the businesses from which a careful analysis of privacy and data-driven risks is required, make it easier for businesses to avoid assessment obligations by strategically downplaying the risks of their processing activities, and undermine the express data protection purposes of the CCPA as amended.

Not only is a broad reading of “significant risk” consistent with the aims of the CCPA; it also aligns with the meaning of the term in a related provision of the Civil Code concerning personal data. As noted above, section 1798.81.6 imposes various obligations on credit reporting agencies whose computer systems are “subject to a security vulnerability that poses a *significant risk* . . . to the security of computerized data that contains personal information[.]”¹⁴³ The term “significant risk” is defined in the same section as a risk that “*could reasonably result* in a breach of the security of the system . . . of personal information[.]”¹⁴⁴ Carrying this definition forward to the CCPA, the Agency should construe the phrase “presents significant risk to consumers’ privacy or security” as referring to data processing that *could reasonably result* in harm to consumers’ privacy or civil rights, not merely processing that is likely or certain to cause such harm. This also follows from the categories of information that the CCPA requires businesses to include in a risk assessment. Such assessments must specify “*whether* [their] processing involves sensitive personal information,”¹⁴⁵ which indicates that risk assessments are required even when a business does not process special categories of personal data that qualify as “sensitive.”¹⁴⁶

The Agency asks for views on whether its definition of “significant risk” should follow the approach outlined in the European Data Protection Board (EDPB)’s Guidelines on Data Protection Impact Assessments. Adopting this approach would require businesses to conduct a risk assessment

¹⁴³ Civ. Code § 1798.81.6(a) (emphasis added).

¹⁴⁴ Civ. Code § 1798.81.6(c) (emphasis added).

¹⁴⁵ Civ. Code § 1798.185(a)(15)(A) (emphasis added).

¹⁴⁶ Civ. Code § 1798.140(ae).

if a processing activity falls into two (and in some cases, just one) of nine categories: evaluation or scoring, automated-decision making with legal or similar significant effect, systematic monitoring, sensitive data processing, processing on a large scale, matching or combining of datasets, processing of data concerning vulnerable data subjects, processing involving innovative uses or new technologies, and processing that would impede an individual's exercise of rights or access to a service or contract.¹⁴⁷

We generally support the EDPB's approach, but with two caveats. First, as reflected in the Colorado Privacy Act,¹⁴⁸ we urge the Agency to add two additional processing categories to this list: (1) processing personal data for purposes of behavioral advertising and (2) selling, sharing, or transferring personal data to third parties. Although these categories may overlap in significant part with the categories set out by the EDPB, both forms of processing present sufficiently acute risks to individuals as to warrant separate inclusion.

Second, we urge the Agency to adopt an overarching definition of "significant risk" (consistent with the above discussion) as a backstop to any enumerated risky processing activities. As the EDPB notes of its own nine-criteria list: "There may be 'high risk' processing operations that are not captured by this list, but yet pose similarly high risks. Those processing operations should also be subject to [Data Protection Impact Assessments]."¹⁴⁹ Mindful of this possibility, the Agency should clarify that "significant risk" is present whenever a processing activity *could reasonably result* in harm to consumers' privacy or civil rights, and that any enumerated examples of such risky activities are non-exhaustive. This umbrella definition would account for emerging processing activities that may pose heightened risks to individuals not apparent from the current state of

¹⁴⁷ Article 29 Data Protection Working Party, *supra* note 134, at 9–11.

¹⁴⁸ C.R.S. § 6-1-1309(2).

¹⁴⁹ Article 29 Data Protection Working Party, *supra* note 134, at 9.

technology, and it would provide additional guidance for determining whether a processing activity that falls into one or more enumerated categories necessitates the completion of a risk assessment.

c. Content of assessments

Responsive to question II.4

With respect to the minimum content businesses should be required to include in risk assessments, we agree with the Agency’s focus on the GDPR and the Colorado Privacy Act. We believe these two frameworks, along with the guidance and regulations that implement them, provide the best template for the Agency to set out the categories of information and analysis that must be included in a business’s risk assessment. Further, we highlight specifically the Office of Management & Budget’s requirement that federal agencies’ impact assessments under the E-Government Act concerning “major information systems” must “reflect more extensive analyses of”:

1. the consequences of collection and flow of information,
2. the alternatives to collection and handling as designed,
3. the appropriate measures to mitigate risks identified for each alternative and,
4. the rationale for the final design choice or business process.¹⁵⁰

We also refer the Agency to EPIC’s recent comments to the FTC concerning commercial surveillance. Building on a proposed list of elements suggested by the Commission, EPIC recommended that impact assessments required under a trade rule include:

- The data [companies] use;
- How they collect, retain, disclose, or transfer that data;
- How they choose to implement any given automated decision-making system or process to analyze or process the data, including the consideration of alternative methods;
- How they process or use that data to reach a decision;
- Whether they rely on a third-party vendor to make such decisions;
- The impacts of their commercial surveillance practices, including disparities or other distributional outcomes among consumers;
- Risk mitigation measures to address potential consumer harms[;] ...
- The purpose(s) for which the company will collect, process, retain, or make available to third parties each category of personal data;

¹⁵⁰ *Id.* at 34.

- The sources of the personal data the company will collect, process, retain, or make available to third parties;
- Which third parties and service providers, if any, the company will make personal data available to;
- What notice or opportunities for consent will be provided to consumers concerning the company's collection, processing, or retention of their personal data or the making available of such information to third parties;
- The potential harms that might result from such processing, including but not limited to privacy, physical, economic, psychological, autonomy, and discrimination harms;
- The company's asserted need to engage in such collection, processing, retention, or transfer of personal information;
- Any alternatives to such collection, processing, retention, or transfer of personal information seriously considered by the company and the reason(s) why such alternatives were rejected;
- How the asserted benefits resulting from such collection, processing, retention, or transfer to the company, the consumer, other stakeholders, and the public compare to the risks to the consumer; and
- A plain language summary of the assessment that would be comprehensible to a reasonable consumer.¹⁵¹

EPIC also recommended that the Commission require companies using automated decision-making systems to make or inform determinations about individuals to disclose, at minimum, the following about each system:

1. A detailed description of the intended purpose and proposed use of the system, including:
 - a. What decision(s) the system will make or support;
 - b. Whether the system makes final decision(s) itself or whether and how supports decision(s);
 - c. The system's intended benefits and research that demonstrates such benefits;
2. A detailed description of the system's capabilities, including capabilities outside of the scope of its intended use and when the system should not be used;
3. An assessment of the relative benefits and costs to the consumer given the system's purpose, capabilities, and probable use cases;
4. The inputs and logic of the system;
5. Data use and generation information, including:
 - a. How the data relied on by the system is populated, collected, and processed;
 - b. The type(s) data the system is programmed to generate;
 - c. Whether the outputs generated by the system are used downstream for any purpose not already articulated;
6. Yearly validation studies and audits of accuracy, bias, and disparate impact; and

¹⁵¹ EPIC FTC Comments on Commercial Surveillance, *supra* note 7, at 163–64.

7. A detailed use and data management policy.¹⁵²

Finally, the Algorithmic Impact Assessments tools of the U.S. Federal Chief Information Officers Council¹⁵³ and the Canadian Government¹⁵⁴ provide a helpful example of the types of information that should appear in a risk assessment of an automated decision-making system. In addition to the content of these tools, the Agency should consider developing a similar web portal for businesses to submit risk assessment summaries as means of simplifying compliance, enforcement, and trend measurement.

d. Cross-compliance

Responsive to question II.5

As we note above with respect to cybersecurity audits, we believe that risk assessments completed in compliance with analogous data protection frameworks of other jurisdictions can serve as the basis for a CCPA-compliant risk assessment, subject to two conditions. First: the risk assessment must be supplemented with any content and analysis required by the CCPA that is not present in the original assessment. The Agency should not permit a substandard risk assessment to fulfill a business's CCPA obligations merely because it satisfies the laws of another jurisdiction. Doing so could encourage a race to the bottom, in which the least rigorous risk assessment rules would become the de facto national standard. Second (as we explain with respect to cybersecurity audits): if supplemental information is required, to the extent that the existing assessment includes a holistic analysis component, that analysis must be revisited, taking into account the supplemental information which was not found in the original assessment. Businesses cannot be permitted simply to drop in additional information and assume that the outcome of an assessment ostensibly based on that information will remain unchanged.

¹⁵² EPIC FTC Comments on Commercial Surveillance, *supra* note 77, at 84–85.

¹⁵³ Algorithmic Impact Assessment, *supra* note 137.

¹⁵⁴ Algorithmic Impact Assessment tool, *supra* note 138.

As set out below, we believe the best mechanism for businesses to demonstrate that their risk assessments are compliant is for CCPA regulations to require routine submission of such assessments into database maintained by the Agency. Although the Agency may not be in a position to fully review each assessment submitted, even the possibility that an assessment may be randomly selected for a CPPA audit would incentivize strict compliance.

e. Format and frequency

Responsive to questions II.6 and 8

The most effective way to implement the regular submission mandate of section 1798.185(a)(15)(B) is to require businesses to submit to the Agency both (1) a complete written record of each risk assessment mandated by the CCPA, and (2) a plain language summary of each assessment sufficient for both Agency personnel and interested members of the public to understand the nature, scope, purpose, risks, and asserted justification of each covered processing activity. Further, the Agency should require that each risk assessment and summary be submitted 14 days prior the processing activities it covers; updated and resubmitted 14 days prior to any material changes to covered processing activities; and reviewed—and if necessary, updated—no less than once every six months. Finally, the Agency should maintain a public database of summary risk assessments and require businesses to make such documentation directly available to interested individuals.

The Agency asks whether businesses should be required to submit a summary risk assessment to the Agency on a regular basis as an alternative to submitting every risk assessment. The answer is *both*. Summaries would assuredly be valuable for oversight purposes, as they would enable the Agency to readily identify trends, areas of concern, and data processing activities warranting further investigation across the private sector. To this end, the Agency should establish an online portal for businesses to submit summaries in a standardized format, one analogous to the

Algorithmic Impact Assessments tool of the Federal Chief Information Officers Council.¹⁵⁵ These standardized summaries should include sufficient detail—and be written in sufficiently plain language—for the average reader to understand the nature, scope, purpose, risks, and asserted justification of each covered processing activity.

Still, summaries are by their nature incomplete: they omit detail and can obscure (intentionally or not) critical information necessary to understand the full risk profile of business’s processing activities. They simply do not tell the full story. For these reasons, the Agency should also direct businesses to submit their full risk assessments to the CPPA at the time they are completed or updated. Just as a business operating in California must file a complete tax return with the Franchise Tax Board (FTB),¹⁵⁶ it must also file a complete risk assessment with the CPPA if it intends to engage in the processing of personal information that poses a significant risk. As with a tax return received by the FTB, the Agency’s receipt of a risk assessment would not imply that the Agency endorses the content of that assessment or open a safe harbor to a business for unlawful conduct; it would simply reflect a business’s own assertions concerning its processing activities. If the Agency later becomes aware of apparent CCPA violations by a business—whether through an audit of that business’s risk assessment or other means—the Agency would remain free to investigate and take appropriate enforcement action.

The fact that resource limitations may prevent the Agency from reviewing every risk assessment upon filing does not diminish the value of having at-will capability to retrieve and audit such assessments through a central, Agency-controlled database. Indeed, the knowledge that each risk assessment will be accessible to the Agency at its discretion will provide a powerful incentive

¹⁵⁵ *See id.*; Algorithmic Impact Assessment, *supra* note 137.

¹⁵⁶ *Doing business in California*, Franchise Tax Bd. (2023), <https://www.ftb.ca.gov/file/business/doing-business-in-california.html>.

for businesses to scrupulously evaluate, document, and mitigate the risks posed by their processing of personal data. This would reduce the need for the Agency to rely on the attestation of a corporate officer that a business’s “summaries are complete and accurate reflections of their compliance with CCPA’s risk assessment requirements.” And like the FTB, the CPPA can maintain such a database while protecting confidential business information from being “divulge[d]” or exposed to the public.¹⁵⁷

With respect to what should be considered “regular” submission, we renew our recommendation that businesses be required to conduct each risk assessment as soon as the business takes material steps toward data processing activities that may pose a significant risk to individuals. To be fully effective, a risk assessment must “begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project.”¹⁵⁸ A plausible outcome of a risk assessment should be a decision to abandon or significantly modify a proposed processing activity because it poses an unacceptable risk to individuals—an outcome that is far less likely to occur if a business completes an assessment at the last second. In the interests of establishing clear expectations for businesses and an enforceable standard for the Agency, we recommend that the Agency direct businesses to submit full risk assessments no less than 14 days before engaging in processing activities (or undertaking significant modifications to existing processing activity) that would trigger the assessment requirement.

We also recommend that businesses be required to review—and if necessary, update and resubmit—privacy risk assessments (1) 14 days in advance of any change to a business’s data processing activities that might reasonably alter the resulting risks to individuals, and (2) in any event no less than once per six-month period. In most cases, a six-month review requirement would

¹⁵⁷ Cal. Civ. Code § 1798.185(a)(15)(B).

¹⁵⁸ *Privacy Impact Assessment*, *supra* note 130, at 5–7.

not necessitate further documentation from a business, as such updates to an assessment would generally be due to the Agency before material changes are made to a business’s processing activities.

Finally, we urge the Agency to (1) establish a publicly accessible and searchable database that includes, at a minimum, the risk assessment summaries submitted by businesses; and (2) require businesses to disclose the same documentation in a conspicuous manner to interested members of the public. In addition to forcing an institution to evaluate and mitigate the harms of data processing, a risk assessment “also serves to inform the public of a data collection or system that poses a threat to privacy.”¹⁵⁹ Although the CPRA already requires the agency to “provide a public report summarizing the risk assessments filed with the agency,”¹⁶⁰ we believe it is critical to make more granular information presumptively public and enable interested individuals to learn more about specific products and services that may pose a risk to their privacy. To this end, the Agency should also explore the possibility of requiring presumptive public disclosure of the full underlying risk assessments, subject only to the narrow redactions necessary to protect data security and trade secrets.

f. Companies grossing less than \$25 million per year

Responsive to question II.7

The risk assessment compliance requirements for businesses with less than \$25 million in annual gross revenues should not differ materially from companies above that threshold. As the CCPA itself reflects, a business grossing less than \$25 million a year can pose meaningful risks to the privacy and civil rights of individuals if it “annually buys, sells, or shares the personal information of 100,000 or more consumers or, households” or “[d]erives 50 percent or more of its

¹⁵⁹ EPIC, *Privacy Impact Assessments* (2021), <https://epic.org/issues/open-government/privacy-impact-assessments/>.

¹⁶⁰ Civ. Code § 1798.199.40(d)

annual revenues from selling or sharing consumers’ personal information.”¹⁶¹ Differentiating risk assessment requirements based solely on revenue would fail to account for such risks. Further, businesses can experience rapid growth: a successful app or platform may gross \$300,000 one year and \$30 million the next. Depending on the required frequency of and triggers for risk assessments, such growth could enable a business to escape meaningful accountability for its processing activities for many months after it has crossed the \$25 million line.

To the extent that small businesses may fear added compliance costs from risk assessment requirements, it is important to note that the risk assessments for smaller-scale and lower-risk processing activities will generally be much less burdensome to complete (if they are required at all). But a small business that engages in large-scale, hazardous processing of personal information should not be able to do so without the careful evaluation and mitigation necessitated by a risk assessment. As we explain above: an organization that is too undercapitalized to adequately safeguard consumer data should simply not be permitted to process it.

¹⁶¹ Civ. Code § 1798.140(d)(1).

V. Automated decisionmaking

The use of opaque, untested, and unproven automated decisionmaking systems has exploded across contexts such as hiring,¹⁶² public benefits,¹⁶³ healthcare delivery,¹⁶⁴ insurance,¹⁶⁵ banking,¹⁶⁶ and student proctoring.¹⁶⁷ As set out above, these systems can cause bodily harm, loss of liberty, loss of opportunity, financial harms, dignitary harms, and discrimination harms.¹⁶⁸

The CCPA as amended gives consumers the opportunity to bridge the gap between knowledge and disclosure. Notably, several aspects of the CCPA overlap with other laws and regulations coming into force, in particular the Colorado Privacy Act. Drawing on Colorado's

¹⁶² See, e.g., Dinah Wisenberg Brin, *Employers Embrace Artificial Intelligence for HR*, SHRM (Mar. 22, 2019), <https://www.shrm.org/resourcesandtools/hr-topics/global-hr/pages/employers-embrace-artificial-intelligence-for-hr.aspx>; Sheridan Wall & Hilke Schellmann, *LinkedIn's Job-Matching AI was Biased. The Company's Solution? More AI.*, MIT Tech. Rev. (Jun. 23, 2021), <https://www.technologyreview.com/2021/06/23/1026825/linkedin-ai-bias-%20ziprecruiter-monster-artificial-intelligence>; Monica Montesa, *AI Recruiting in 2023: The Definitive Guide*, Phenom (Mar. 14, 2023), <https://www.phenom.com/blog/recruiting-ai-guide>; QuantumBlack, McKinsey & Co., *The State of AI in 2022—and a Half Decade in Review* (Dec. 6, 2022), https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review#; Drew Harwell, *A Face-Scanning Algorithm Increasingly Decides Whether You Deserve the Job*, Wash. Post (Nov. 6, 2019), <https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/>.

¹⁶³ See, e.g., Arnauld Bertrand & Julie McQueen, *Why AI and the Public Sector are a Winning Formula*, Ernst & Young Global Ltd. (Oct. 21, 2020), https://www.ey.com/en_gl/government-public-sector/why-ai-and-the-public-sector-are-a-winning-formula; Grant Fergusson, *Public Benefits, Private Vendors: How Private Companies Help Run our Welfare Programs*, EPIC (Jan. 26, 2023), <https://epic.org/public-benefits-private-vendors-how-private-companies-help-run-our-welfare-programs/>.

¹⁶⁴ See, e.g., Liz Kwo, *Contributed: Top 10 Use Cases for AI in Healthcare*, Mobi Health News (Jul. 1, 2021), <https://www.mobihealthnews.com/news/contributed-top-10-use-cases-ai-healthcare>.

¹⁶⁵ See, e.g., Insurance Europe, *AI in the Insurance Sector* (Nov. 2021), <https://www.insuranceeurope.eu/publications/2608/artificial-intelligence-ai-in-the-insurance-sector/>.

¹⁶⁶ See, e.g., Eleni Digalaki, *The Impact of Artificial Intelligence in the Banking Sector & How AI is Being Used in 2022*, Bus. Insider (Feb. 2, 2022), <https://www.businessinsider.com/ai-in-banking-report>.

¹⁶⁷ See e.g., Complaint and Request for Investigation, Injunction, and Other Relief, *In re Online Test Proctoring Companies* (Dec. 9, 2020), <https://epic.org/wp-content/uploads/privacy/dccppa/online-test-proctoring/EPIC-complaint-in-re-online-test-proctoring-companies-12-09-20.pdf>.

¹⁶⁸ See, e.g., EPIC FTC Comments on Commercial Surveillance, *supra* note 77; Rebecca Kelly Slaughter et al., *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission*, 23 Yale J.L. & Tech 1, 51 (2021); see also Citron & Solove, *supra* note 10, at 855; Buolamwini & Gebru, *supra* note 62.

recently adopted regulations and other similar frameworks, we urge the Agency to ensure that consumers enjoy robust access and opt-out rights with respect to ADS.

a. Existing laws and frameworks

i. Current and anticipated laws

Responsive to question III.1

As key points of reference for its rulemaking, we would point the Agency to the Colorado Privacy Act,¹⁶⁹ the New York City Hiring Law,¹⁷⁰ and regulatory controls on predictive policing around the country.¹⁷¹ Highlights of other relevant state laws include:

- Alabama Act 2022-420, which prohibits state and local law enforcement agencies (LEAs) from using facial recognition technology match results to establish probable cause in a criminal investigation or to make an arrest;
- Illinois Public Act 102-0047, which requires employers that rely solely on AI analysis of video interviews to determine whether an applicant will be selected for an in-person interview to collect and report demographic data about the race and ethnicity of applicants; and
- Vermont Act 132, which requires the Division of Artificial Intelligence to propose a state code of ethics on the use of artificial intelligence in state government, make recommendations to the General Assembly on policies, laws, and regulations of artificial intelligence in state government, and make annual recommendations and reports to the General Assembly on the use of artificial intelligence in state government and requires the Agency of Digital Services to conduct an inventory of automated decision systems developed, employed, or procured by state government.

¹⁶⁹ Colo. Rev. Stat. § 6-1-1301 *et seq.*

¹⁷⁰ N.Y. Local Law 144, Int. No. 1894-A (2021), <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9>.

¹⁷¹ *See, e.g.*, Exec. Order No. 14,074, 87 Fed. Reg. 32,945 (2022).

Sectoral regulations are also under development by the Colorado Department of Insurance,¹⁷² the California Civil Rights Council,¹⁷³ and the New York City Department of Consumer and Worker Protection¹⁷⁴ among others, and federal rulemakings are in progress at the Federal Trade Commission¹⁷⁵ and the Consumer Financial Protection Bureau.¹⁷⁶

Notable overseas laws include the General Data Protection Regulation,¹⁷⁷ the European AI Act,¹⁷⁸ China's AI laws,¹⁷⁹ and India's potential AI regulations.¹⁸⁰

ii. Other frameworks

Responsive to question III.1

There have been over 40 notable frameworks and guidance documents on the use of AI and automated decision-making systems published in recent years.¹⁸¹ We highlight four in view of their

¹⁷² Governance and Risk Management Framework Requirements for Life Insurance Carriers' Use of External Consumer Data and Information Sources, Algorithms, and Predictive Models, 3 Colo. Code Regs. § 702-4.

¹⁷³ Cal. Civ. Rts. Council, Proposed Modifications to Employment Regulations Regarding Automated-Decision Systems, Cal. Code Regs. tit. 2, § 11008 *et seq.* (2022), <https://calcivilrights.ca.gov/wp-content/uploads/sites/32/2022/07/Attachment-G-Proposed-Modifications-to-Employment-Regulations-Regarding-Automated-Decision-Systems.pdf>.

¹⁷⁴ New York City Dep't of Consumer & Worker Prot., Text of Proposed Rule on Automated Employment Decision Tools (2023), <https://rules.cityofnewyork.us/wp-content/uploads/2022/12/DCWP-NOH-AEDTs-1.pdf>.

¹⁷⁵ FTC, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (Aug. 22, 2022).

¹⁷⁶ Consumer Fin. Prot. Bureau, *Consumer Financial Protection Circular 2022-03* (May 26, 2022), <https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/>.

¹⁷⁷ Commission Regulation (EU) 2016/679, 2016 O.J. (L 119) 1 (EU).

¹⁷⁸ European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM(2021) 206 final (Apr. 21, 2021).

¹⁷⁹ See Translation: Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022, Digichina (Jan. 10, 2022), <https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/>.

¹⁸⁰ See Simon Sharwood, *India Teases AI Plan to 'Catalyse the Next Generation of the Internet,'* The Register (Mar. 8, 2023), https://www.theregister.com/2023/03/08/digital_india_bill_ai/.

¹⁸¹ Cf. Jessica Fjeld et al., Berkman Klein Center for Internet & Society, *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI* (2020), https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf.

comprehensiveness, their support by actors that have substantial influence, their focus on the individuals affected by automated systems, or the prominence of their authors.

A Blueprint for an AI Bill of Rights was released by the White House Office of Science and Technology Policy in January 2023.¹⁸² It sets out five major principles: Safe and Effective Systems; Freedom from Algorithmic Discrimination; Data Privacy; Notice and Explanation; and Human Alternatives, Consideration, and Fallback¹⁸³. The document lays out why these principles are critical, examples of how they are violated, and examples of how they have been implemented. The Blueprint notes that individuals must be protected from abusive data practices and calls for data minimization rules, stating: “You should be protected from violations of privacy through design choices that ensure such protections are included by default, including ensuring that data collection conforms to reasonable expectations and that only data strictly necessary for the specific context is collected.”¹⁸⁴

The AI Risk Management Framework by the National Institute of Standards and Technology (“NIST”) was developed pursuant to the National AI Initiative Act.¹⁸⁵ NIST describes the document as a “[voluntary] resource [for] the organizations designing, developing, deploying, or using AI systems to help manage the many risks of AI and promote trustworthy and responsible development and use of AI systems.”¹⁸⁶ Divided into four main aspects of AI lifecycles (Govern, Map, Measure, and Manage), the framework includes examples of how companies can adopt a more responsible approach to building and using AI tools. However, as the framework reminds readers, it is entirely nonbinding.

¹⁸² White House Office of Sci. & Tech. Pol’y, *Blueprint for an AI Bill of Rights: Making Automated Systems Work* (2022), <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>.

¹⁸³ *Id.*

¹⁸⁴ *Id.*

¹⁸⁵ 15 U.S.C. § 9411 *et seq.*; see also Nat’l Inst. of Standards & Tech., *NIST AI 100-1: Artificial Intelligence Risk Management Framework* (AI RMF 1.0) (2023), <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>.

¹⁸⁶ Nat’l Inst. of Standards & Tech., *supra* note 185.

The OECD AI Principles¹⁹ were adopted in 2019 and endorsed by 42 countries—including the United States and the G20 nations. The OECD AI Principles establish international standards for AI use:

1. Inclusive growth, sustainable development and well-being.
2. Human-centered values and fairness.
3. Transparency and explainability.
4. Robustness, security and safety.
5. Accountability.²¹

The OECD also urges governments to ensure the development of “trustworthy AI” and to focus on “AI-related social, legal and ethical implications and policy issues.” Governments are specifically urged to “review and adapt, as appropriate, their policy and regulatory frameworks and assessment mechanisms as they apply to AI systems to encourage innovation and competition for trustworthy AI.” The OECD AI Principle on Transparency and Explainability states: “AI Actors should commit to transparency and responsible disclosure regarding AI systems. To this end, they should provide meaningful information, appropriate to the context, and consistent with the state of art: . . . to enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation, or decision.” “AI Actors” are defined as those “who play an active role in the AI system lifecycle, including organisations and individuals that deploy or operate AI.”

The Universal Guidelines for Artificial Intelligence, a framework for AI governance based on the protection of human rights, were set out at the 2018 Public Voice meeting in Brussels, Belgium.²⁶ The Universal Guidelines for AI have been endorsed by more than 250 experts and 60 organizations in 40 countries. The UGAI comprise twelve principles:

1. Right to Transparency.
2. Right to Human Determination.
3. Identification Obligation.
4. Fairness Obligation.
5. Assessment and Accountability Obligation.

6. Accuracy, Reliability, and Validity Obligations.
7. Data Quality Obligation.
8. Public Safety Obligation.
9. Cybersecurity Obligation.
10. Prohibition on Secret Profiling.
11. Prohibition on Unitary Scoring.
12. Termination Obligation.¹⁸⁷

Among the key principles, the UGAI states: “All individuals have the right to know the basis of an AI decision that concerns them. This includes access to the factors, the logic, and techniques that produced the outcome” (Right to Transparency); “Institutions must ensure that AI systems do not reflect unfair bias or make impermissible discriminatory decisions” (Fairness Obligation); “An AI system should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks. Institutions must be responsible for decisions made by an AI system” (Assessment and Accountability Obligation); “Institutions must ensure the accuracy, reliability, and validity of decisions” (Accuracy, Reliability, and Validity Obligations); and “Institutions must establish data provenance and assure quality and relevance for the data input into algorithms” (Data Quality Obligation).

b. ADS access and opt-out rights

Responsive to question III.7

An opt-out allows users to avoid discrimination and other harmful consequences of an automated decisionmaking system by choosing not to be subject to it in the first place. To make this effective, the CPPA should require controllers to clearly explain the key parameters of each automated decisionmaking system, ensure that opting out of ADS is frictionless for the consumer, and establish strong protections to prevent discrimination based on opt-out status.

¹⁸⁷ The Public Voice, *Universal Guidelines for Artificial Intelligence* (Oct. 23, 2018), <https://thepublicvoice.org/ai-universal-guidelines/>.

These safeguards should enable users to grasp the difference between how certain ADS systems work, but it will likely take time for the public to understand the contexts in which automated decisionmaking technology is used and which systems may result in discriminatory outcomes. A recent Pew Research Center study showed that, while only 15% of Americans are more excited than concerned about increased use of AI in daily life, less than a third of Americans surveyed could accurately identify six instances where AI is used in common everyday experiences.¹⁸⁸ These regulations should start to bridge that gap and incentivize businesses to be more responsible with data collection and ADS adoption, as they will be forced to disclose key information about their tools that may steer concerned users toward other products.

c. ADS disclosures

Responsive to question III.9

When developing rules as to how controllers must provide information about the logic of their automated decisionmaking systems, the Agency should be attentive to both the content and the format of disclosures to make them effective.

We urge the Agency to mandate, at minimum, that a business disclose the purpose of an automated decisionmaking system; what decision the tool is making or supporting; the factors the system relies on; a plain-language explanation of the logic of the system;¹⁸⁹ the sources and life cycle of the data processed by the system, including any brokers or other third-party sources; and how the system has been evaluated for accuracy and fairness, including links to any audits, validation studies, or impact assessments.

¹⁸⁸ Brian Kennedy, Alec Tyson, and Emily Saks, *Public Awareness of Artificial Intelligence in Everyday Activities*, Pew Research Center (Feb. 15, 2023), <https://www.pewresearch.org/science/2023/02/15/public-awareness-of-artificial-intelligence-in-everyday-activities/>.

¹⁸⁹ For example, in a predictive profiling system or automated decisionmaking system, the explanation should include data sources and how particular inputs affect determinations (e.g., if a criminal arrest in the last three years increases a “risk” classification by two points).

Further, it is critical that the disclosure not be buried only in the business's terms service or other equally hard-to-find location. It must be easily accessible ahead of the consumer's interaction with the system so that opt-out and access rights can be exercised *prior* to an automated decision being rendered.

The Agency should consider publishing model disclosures and display formats for websites and mobile applications—templates that would enable clear and seamless display of ADS information at the consumer's request without (for example) swamping consumers with popups that take over the screen. There is good language to this effect in the Colorado Privacy Act, which requires “A controller [to] provide consumers with a reasonably accessible, clear, and meaningful privacy notice”¹⁹⁰ and provide a “clear, conspicuous method ... provided either directly or through a link, in a clear, conspicuous, and readily accessible location *outside the privacy notice*.”¹⁹¹

VI. Conclusion

We thank the Agency for the opportunity to comment on its further forthcoming CCPA regulations and are eager to continue working with the CPPA to protect the privacy of all Californians.

Respectfully submitted,

Electronic Privacy Information Center
Center for Digital Democracy
Consumer Federation of America

¹⁹⁰ Colo. Rev. Stat. § 6-1-1308(a).

¹⁹¹ 4 CCR 904-3 at § 4.03(b)(1)(a), <https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf>.

APPENDIX 1

New Baseline Expectations for Data Security: Consensus on Cybersecurity Hygiene for the Modern Threat Environment

Recommended Data Security Protocol	Non-Exhaustive List of Citations
Data minimization	<ul style="list-style-type: none"> • 16 C.F.R. pts. 314.4(c)(6), 682 • N.Y. Gen. Bus. Law, § 899-bb(2)(b)(ii)(C)(4) (2020) • Or. Rev. Stat. tit. 50, § 646A.622(2)(d)(C)(i), (iv) (2021) • N.Y. Comp. Codes R. & Regs. tit. 23, § 500.13 (2022) • CIS Critical Security Controls 3.1, 3.4 • Complaint, In re Drizly, LLC, FTC File No. 2023185 at ¶ 13(f) (Oct. 24, 2022) • Complaint, In re Chegg, Inc., FTC File No. 2023151 at ¶ 9(a) (Oct. 31, 2022) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 34 (Apr. 16, 2018) • PCI-DSS Principal Requirement 3
Data mapping	<ul style="list-style-type: none"> • N.Y. Comp. Codes R. & Regs. tit. 23, § 500.3 (2022) • CIS Critical Security Controls 3.1, 3.2, 3.7, 3.8 • Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 14 (Dec. 30, 2019) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(B) (N.D. Ga. Jul. 22, 2019) • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(g) (Feb. 1, 2021) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 24 (Apr. 16, 2018) • FFIEC Cybersecurity Assessment Tools ver. 1.1 5-6, 28-29 (May 2017) • PCI-DSS Principal Requirement 1
Access controls	<ul style="list-style-type: none"> • 201 Mass. Code Regs. 17.04(1)(d,3), 17.04(2) (2010) • Or. Rev. Stat. tit. 50, § 646A.622(2)(d)(A)(vii) (2021) • N.Y. Comp. Codes R. & Regs. tit. 23, § 500.07 (2022) • FTC Safeguards Rule: What Your Business Needs to Know, FTC, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (last visited Mar. 17, 2023) (citing to 314.4(c)(1) of Safeguards Rule) • Final Rule, FTC, Standards for Safeguarding Customer Information, 86 Fed. Reg. 70286 (Dec. 9, 2021) (noting that “[s]uch overbroad access could create additional harm in the event of an intruder gaining access to a system by impersonating an employee or service provider”)

	<ul style="list-style-type: none"> • CIS Critical Security Controls 3.3, 4.7, 5.1, 5.4, 5.5, 6.1, 6.2, 6.6, 6.8, 13.5 • First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24(j) (3d Cir. 2015) • Complaint, In re Chegg, Inc., FTC File No. 2023151 at ¶ 9(a) (Oct. 31, 2022) • Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 10(d) (Dec. 30, 2019) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(D), 23(C) (N.D. Ga. Jul. 22, 2019) • Complaint, FTC v. Ruby Life Inc. d/b/a AshleyMadison.com, No. 1:16-cv-02438 at ¶ 31(b) (D.D.C. Dec. 14, 2016) • Complaint, In re LightYear Dealer Technologies, LLC, FTC File No. 1723051 at ¶ 11(e) (Sept. 6, 2019) • Complaint, In re SkyMed International, Inc., FTC File No. 1923140 at ¶ 12(c) (Jan. 26, 2021) • Complaint at ¶ 13(c), In re Drizly, LLC, FTC File No. 2023185 (Oct. 24, 2022); • Complaint, In re Support King, LLC, FTC File No. 1923003 at ¶ 17(b) (Dec. 21, 2021) • Complaint, In re Uber Technologies, Inc., FTC File No. 1523054 at ¶ 18(a) (Oct. 26, 2018) • CISA, Cross-Sector Cybersecurity Performance Goals 9 (2022) (control 1.5) • FINRA, Report on Cybersecurity Practices 17-20 (Feb 2015) • FINRA, Core Cybersecurity Threats and Effective Controls for Small Firms 7 (May 2022) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 29, 30 (Apr. 16, 2018) • FFIEC Cybersecurity Assessment Tools ver. 1.1 16-20, 26 (May 2017) • PCI-DSS Principal Requirement 7
Secure password practices	<ul style="list-style-type: none"> • 201 Mass. Code Regs. 17.04(1)(b),(c) (2010) • CIS Critical Security Controls 5.2 • First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24(e)-(f) (3d Cir. 2015) • Complaint, FTC v. Ruby Life Inc. d/b/a AshleyMadison.com, No. 1:16-cv-02438 at ¶ 31(b)(i), (iii), (vi) (D.D.C. Dec. 14, 2016) • Complaint, In re Chegg, Inc., FTC File No. 2023151 at ¶ 9(b)-(c) (Oct. 31, 2022) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(D) (N.D. Ga. Jul. 22, 2019) • Complaint, In re Residual Pumpkin Entity, LLC, d/b/a CafePress, FTC File No. 1923209 at ¶ 11(c), (f) (Jun. 23, 2022)

	<ul style="list-style-type: none"> • Complaint, FTC v. D-Link Corp., No. 3:17-CV-00039-JD at ¶ 15(b),(c) (N.D. Cal. Mar. 20, 2017) • CISA, Cross-Sector Cybersecurity Performance Goals 8, 9, 10 (2022) (controls 1.2, 1.4, 1.6, 1.7) • FFIEC Cybersecurity Assessment Tools ver. 1.1 21 (May 2017) • PCI-DSS Principal Requirement 2
User authentication	<ul style="list-style-type: none"> • 201 Mass. Code Regs. 17.04(1) (2010) • N.Y. Comp. Codes R. & Regs. Tit. 23, § 500.12 (2022) • FTC Safeguards Rule: What Your Business Needs to Know, FTC, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (last visited Mar. 17, 2023) (citing to 314.4(c)(5) of Safeguards Rule) • CIS Critical Security Control 6.3, 6.4, 6.5, 6.6, 12.7 • Complaint, In re Residual Pumpkin Entity, LLC, d/b/a CafePress, FTC File No. 1923209 at ¶ 25 (Jun. 23, 2022) • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(d) (Feb. 1, 2021) • Complaint, In re LightYear Dealer Technologies, LLC, FTC File No. 1723051 at ¶ 11(e) (Sept. 6, 2019) • Complaint, In re Uber Technologies, Inc., FTC File No. 1523054 at ¶ 18(a)(iii), 24 (Oct. 26, 2018) • Complaint, In re Paypal, Inc., FTC File No. 1623102 at ¶ 40(c)(1) (May. 24, 2018) • CISA, Cross-Sector Cybersecurity Performance Goals 8 (2022) (control 1.3) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 30 (Apr. 16, 2018) • PCI-DSS Principal Requirement 8
Segmentation of systems	<ul style="list-style-type: none"> • CIS Critical Security Control 3.12, 4.4, 12.8 • First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24(a), 28 (3d Cir. 2015) • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(e) (Feb. 1, 2021) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(C)-(D), 23(B) (N.D. Ga. Jul. 22, 2019) • Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 10(e) (Dec. 30, 2019) • CISA, Cross-Sector Cybersecurity Performance Goals 22 (2022) (control 8.1) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 30 (Apr. 16, 2018)

	<ul style="list-style-type: none"> • Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4, at 39-40 (March 2022) (Requirement 1) • FFIEC Cybersecurity Assessment Tools ver. 1.1 8,16 (May 2017) • PCI-DSS Principal Requirement 10
Traffic monitoring	<ul style="list-style-type: none"> • 201 Mass. Code Regs. 17.04(4) (2010) • N.Y. Comp. Codes R. & Regs. Tit. 23, § 500.06 (2022) • 16 C.F.R. pt. 314.4(c)(8) • CIS Critical Security Control 13 • First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24(h)-(i) (3d Cir. 2015) • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(e) (Feb. 1, 2021) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(F), 23(A)(iii)-(iv), 23(C)(iii) (N.D. Ga. Jul. 22, 2019) • Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 10(f), 17 (Dec. 30, 2019) • Complaint, In re LightYear Dealer Technologies, LLC, FTC File No. 1723051 at ¶ 11(d) (Sept. 6, 2019) • Complaint, FTC v. Ruby Life Inc. d/b/a AshleyMadison.com, No. 1:16-cv-02438 at ¶ 35 (D.D.C. Dec. 14, 2016) • Complaint, In re Chegg, Inc., FTC File No. 2023151 at ¶ 9(g) (Oct. 31, 2022) • Complaint, In re SkyMed International, Inc., FTC File No. 1923140 at ¶ 12(f) (Jan. 26, 2021) • CISA, Cross-Sector Cybersecurity Performance Goals 8 (2022) (control 1.1) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 36, 38-39 (Apr. 16, 2018) • FFIEC Cybersecurity Assessment Tools ver. 1.1 16, 25-26 (May 2017) • PCI-DSS Principal Requirement 10
Staying current on known vulnerabilities and ongoing security reviews (e.g. penetration testing)	<ul style="list-style-type: none"> • 201 Mass. Code Regs. 17.03(2)(h),(i), 17.04(6),(7) (2010) • N.Y. Gen. Bus. Law, § 899-bb(2)(b)(ii)(B)(4) (2020) • Or. Rev. Stat. tit. 50, § 646A.622(2)(d)(B) (2021) • N.Y. Comp. Codes R. & Regs. tit. 23, § 500.05 (2022) • 16 C.F.R. pts. 314.4(b)(2), 314.4(d), 314.4(g) • FTC Safeguards Rule: What Your Business Needs to Know, FTC, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (last visited Mar. 17, 2023) (“assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside your information systems”)

	<ul style="list-style-type: none"> • CIS Critical Security Control 7, 13.5, 18 • First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24(d), 29 (3d Cir. 2015) • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(b) (Feb. 1, 2021) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(A), 23(A) (N.D. Ga. Jul. 22, 2019) • Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 10(b) (Dec. 30, 2019) • Complaint, In re LightYear Dealer Technologies, LLC, FTC File No. 1723051 at ¶ 10,11(c)-(d) (Sept. 6, 2019) • Complaint, FTC v. Ruby Life Inc. d/b/a AshleyMadison.com, No. 1:16-cv-02438 at ¶ 31(e) (D.D.C. Dec. 14, 2016) • Complaint, In re SkyMed International, Inc., FTC File No. 1923140 at ¶ 12(d) (Jan. 26, 2021) • Complaint, In re Residual Pumpkin Entity, LLC, d/b/a CafePress, FTC File No. 1923209 at ¶ 1(a), (d)-(e), (h) (Jun. 23, 2022) • Complaint, In re Paypal, Inc., FTC File No. 1623102 at ¶ 40(b) (May. 24, 2018) • Complaint, In re Drizly, LLC, FTC File No. 2023185 at ¶ 13(d)-(e) (Oct. 24, 2022) • Complaint, In re Support King, LLC, FTC File No. 1923003 at ¶ 17(c) (Dec. 21, 2021) • Complaint, FTC v. D-Link Corp., No. 3:17-CV-00039-JD at ¶ 15(a) (N.D. Cal. Mar. 20, 2017) • CISA, Cross-Sector Cybersecurity Performance Goals 17,18 (2022) (controls 5.1, 5.6) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 26, 33, 36, 39, 40, 43 (Apr. 16, 2018) • FINRA, Report on Cybersecurity Practices 21-22 (Feb 2015) • FFIEC Cybersecurity Assessment Tools ver. 1.1 6, 8, 24-28 (May 2017) • PCI-DSS Principal Requirement 5,6,11
Employee training	<ul style="list-style-type: none"> • 201 Mass. Code Regs. 17.03(2)(b)(1), 17.04(8) (2010) • N.Y. Gen. Bus. Law, § 899-bb(2)(b)(ii)(A)(4) (2020) • Or. Rev. Stat. tit. 50, § 646A.622(2)(d)(A)(iv) (2021) • N.Y. Comp. Codes R. & Regs. tit. 23, § 500.10, 500.14 (2022) • 16 C.F.R. pt. 314.4(e) • CIS Critical Security Control 14 • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(a) (Feb. 1, 2021)

	<ul style="list-style-type: none"> • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 23(E) (N.D. Ga. Jul. 22, 2019) • Complaint, In re LightYear Dealer Technologies, LLC, FTC File No. 1723051 at ¶ 11(b) (Sept. 6, 2019) • Complaint, FTC v. Ruby Life Inc. d/b/a AshleyMadison.com, No. 1:16-cv-02438 at ¶ 31(c) (D.D.C. Dec. 14, 2016) • Complaint, In re SkyMed International, Inc., FTC File No. 1923140 at ¶ 12(b) (Jan. 26, 2021) • Complaint, In re Chegg, Inc., FTC File No. 2023151 at ¶ 9(e) (Oct. 31, 2022) • Complaint, In re Uber Technologies, Inc., FTC File No. 1523054 at ¶ 18(b) (Oct. 26, 2018) • CISA, Cross-Sector Cybersecurity Performance Goals 15 (2022) (controls 4.3, 4.4) • Security Tip (ST04-014): Avoiding Social Engineering and Phishing Attacks, CISA (Aug. 25, 2020) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 31 (Apr. 16, 2018) • FINRA, Report on Cybersecurity Practices 31-32 (Feb 2015) • FINRA, Core Cybersecurity Threats and Effective Controls for Small Firms 10 (May 2022) • FFIEC Cybersecurity Assessment Tools ver. 1.1 11-12 (May 2017) • PCI-DSS Principal Requirement 5, 6, 9, 12
Heightened measures for high-risk activity (e.g. remote access, processing sensitive information, third-party integrations, etc.)	<ul style="list-style-type: none"> • 201 Mass. Code Regs. 17.03(2)(f) (2010) • N.Y. Gen. Bus. Law, § 899-bb(2)(b)(ii)(A)(6) (2020) • Or. Rev. Stat. tit. 50, § 646A.622(2)(d)(A)(vi) (2021) • N.Y. Comp. Codes R. & Regs. tit. 23, § 500.11, 500.12(b) (2022) • 16 C.F.R. pt. 314.4(f) • Standards for Safeguarding Customer Information, 16 C.F.R. § 314 (2021) (citing to 16 CFR 314.4(d), also citing to Kevin McCoy, Target to Pay \$18.5M for 2013 Data Breach that Affected 41 Million Consumers, USA Today (May 23, 2017)) • Complying with COPPA: Frequently Asked Questions, FTC L(1), https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (last visited Mar. 17, 2023) (referring to § 312.8) • CIS Critical Security Controls 6.3, 6.4, 12.7, 15, 16 • First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24(j) (3d Cir. 2015) • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(c) (Feb. 1, 2021)

	<ul style="list-style-type: none"> • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(E),23(D) (N.D. Ga. Jul. 22, 2019) • Complaint, In re LightYear Dealer Technologies, LLC, FTC File No. 1723051 at ¶ 11(b) (Sept. 6, 2019) • Complaint, FTC v. Ruby Life Inc. d/b/a AshleyMadison.com, No. 1:16-cv-02438 at ¶ 31(d) (D.D.C. Dec. 14, 2016) • Complaint, In re SkyMed International, Inc., FTC File No. 1923140 at ¶ 13 (Jan. 26, 2021) • Complaint, In re Uber Technologies, Inc., FTC File No. 1523054 at ¶ 18(d), 20 (Oct. 26, 2018) • Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 10(g) (Dec. 30, 2019) • Complaint, In re Support King, LLC, FTC File No. 1923003 at ¶ 17(a), (e) (Dec. 21, 2021) • Complaint, In re Lenovo, Inc., FTC File No. 1523134 at ¶ 24 (Jan. 2, 2018) • Complaint, In re Ascension Data & Analytics, LLC, FTC File No. 1923126 at ¶¶ 13, 14–17, 20 (2021) • Complaint, In re TaxSlayer, LLC, FTC File No. 1623063 at ¶ 14(d) (2017) • CISA, Cross-Sector Cybersecurity Performance Goals 14, 19 (2022) (controls 3.4, 6.1, 6.2, 6.3) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 28, 29, 39 (Apr. 16, 2018) • FINRA, Report on Cybersecurity Practices 26-30 (Feb 2015) • FINRA, Core Cybersecurity Threats and Effective Controls for Small Firms 6-7 (May 2022) • FFIEC Cybersecurity Assessment Tools ver. 1.1 17,20,28-32 (May 2017) • PCI-DSS Principal Requirement 2, 3, 7, 8 • Karen Scarfone, Security Concerns with Remote Access, https://csrc.nist.gov/CSRC/media/Events/HIPAA-Security-Rule-Implementation-and-Assurance/documents/NIST_Remote_Access.pdf (last visited Mar. 17, 2023) • Kristin Cohen, Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law against Illegal Use and Sharing of Highly Sensitive Data FTC Bus. Blog (July 11, 2022) • ABA Cybersecurity Legal Task Force, Vendor Contracting Project: Cybersecurity Checklist Second Edition 1 (2021)
--	---

From: Elizabeth Guillot [REDACTED]
Sent: Monday, March 27, 2023 4:14 PM
To: Regulations
Subject: PR 02-2023 CrowdStrike Comments
Attachments: CrowdStrike CPPA Cybersecurity Comments.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello,

Thank you for the opportunity to comment on the preliminary rulemaking regarding cybersecurity audits, risk assessments, and automated decisionmaking. Please find attached CrowdStrike's comments. If you have any questions, please do not hesitate to reach out.

Best,
Elizabeth

Elizabeth Guillot
Manager, Public Policy
CrowdStrike, Inc.

[REDACTED]
<http://www.crowdstrike.com>



INVITATION FOR PRELIMINARY COMMENTS ON PROPOSED RULEMAKING

CYBERSECURITY AUDITS, RISK ASSESSMENTS, AND AUTOMATED DECISION MAKING

March 27, 2023

I. INTRODUCTION

In response to the California Privacy Protection Agency's ("CPPA") invitation for preliminary comments on proposed rulemaking regarding cybersecurity audits, risk assessments, and automated decision making ("proposed rulemaking") CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

We appreciate the CPPA's efforts to better protect California citizens' data from cybersecurity threats through the California Privacy Rights Act of 2020 ("CPRA"). Although CrowdStrike submitted a response to the November 2021 invitation for preliminary comments on these same issues, we welcome the opportunity to provide additional feedback.¹

Cybersecurity threats are evolving and increasing. Illustrative of this, in CrowdStrike's *2023 Global Threat Report*, we observed a notable surge in identity-based threats and cloud exploitations. To name a few, we found a 112%

¹ CrowdStrike's response to the Invitation for Preliminary Comments on Proposed Rulemaking, pages 17-23: https://cppa.ca.gov/regulations/pdf/preliminary_rulemaking_comments_1.pdf

year-over-year increase in advertisements on the dark web for identity and access credentials, a 95% increase in cloud exploitation by threat actors, over 30 new adversaries and numerous new ways that eCrime actors weaponize and exploit vulnerabilities.² As adversaries continue to evolve and find new ways to target victims, organizations need to increase their emphasis on cybersecurity practices that leverage the most effective technologies.

The legal and regulatory environment surrounding cybersecurity is increasingly complex. This follows from: (i) growing reliance on globally-distributed infrastructure, and (ii) compliance obligations for national and international standards and procedures. In order to ensure the most robust cybersecurity methods and disclosure, and compliance obligations remain feasible, regulators must endeavor to create clear and future-flexible expectations.

While we do not have feedback on every aspect of the proposed amendment, we do want to offer several points that may be of value to the CPPA as it considers the proposed rule.

A. Cybersecurity Audits

Cybersecurity audits have significant limitations as a cybersecurity tool. They are a useful tool for an organization to capture a snapshot of the existence of cybersecurity plans, strategies, or controls; however, audit results are only reflective of a point in time and cannot reflect a real-time measure of the state of an organization's security practices. While we recognize that it is the CPPA's intention to create an auditing scheme, we would caution organizations against being overly reliant on the results. In addition to a cybersecurity audit, organizations should deploy cybersecurity best practices to continuously protect themselves from cyberattacks and data breaches and reevaluate if those technologies are working to the best of their ability more regularly than a yearly audit. Creating non-prescriptive mandates that nonetheless encourage organizations to analyze their risks, plans, and strategies is important for ensuring cybersecurity practices evolve with the threat landscape.

Incentivizing the adoption of effective cybersecurity practices and technologies is

² CrowdStrike Global Threat Report, 2023. <https://www.crowdstrike.com/global-threat-report/>

paramount to achieving the CPPA's goal of protecting citizen's data. CrowdStrike views the following strategies and technologies as best practices and recommends the best practices be deployed by entities in scope of the regulations.

- **Extended Detection & Response (XDR).** Cybersecurity threats are exceptionally broad, and for too long industry players have focused on narrow solutions. No box on a network or a single-purpose software agent will address the full scope of the problem. Security teams demand contextual awareness and visibility from across their entire environments, including within cloud and ephemeral environments. The next evolution of the **Endpoint Detection and Response (EDR)** concept, XDR seeks to leverage rich endpoint telemetry and integrate other security-relevant network or system events, wherever they exist within the enterprise, and generate intelligence from what otherwise may be an information overload. EDR is a great place for organizations to start with baseline security; however, XDR is an option for organizations with already advanced cybersecurity practices.
- **Identity Protection and Authentication:** As organizations embark on a digital transformation to work from anywhere models, Bring-Your-Own-Device policies become commonplace, cloud services multiply, and enterprise boundaries continue to erode. This trend increases the risk of relying upon traditional authentication methods and further weakens obsolescent legacy security technologies. Identity-centric approaches to security use a combination of real-time authentication traffic analysis and machine learning analytics to quickly determine and respond to identity-based attacks.
- **Logging Practices.** Organizations should collect and retain security-relevant log information to support proactive security measures, threat hunting, and investigative use-cases.
- **Threat Hunting.** Whether through supply chain attacks or otherwise, we know that adversaries periodically breach even very-well defended enterprises. Properly trained and resourced defenders can find them and thwart their goals. In our experience, whether organizations accept this premise – that cybersecurity involves not just a passive alarm, but a sentry

actively looking for trouble – is the leading indicator of the strength of their cybersecurity program. Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. And the better-instrumented the environment, the more chances defenders give themselves to intervene as a breach attempt progresses through phases, commonly referred to as the *kill chain*. Multiple opportunities for detection help avert “silent failures” – where a failure of security technology results in security events going completely unnoticed.

- **Speed.** We advise users that when responding to a security incident or event, every second counts. The more we can do to detect and stop adversaries at the outset of an attack, the better chance we have to prevent them from achieving their objectives. The reason for this is that adversaries move fast, especially when engaging in lateral movement through an enterprise. This means that measuring response time and severity, essentially a DEFCON for security, is critical to ultimately stopping a malicious chain of events and improving performance.
- **Machine Learning-Based Prevention.** The core of next-generation cybersecurity solutions is the ability to defeat novel threats. Machine learning and artificial intelligence are essential to this end, and leveraging these technologies is the best way to gain the initiative against adversaries.
- **Zero Trust.** Due to fundamental problems with today’s widely-used authentication architectures, organizations must incorporate new security protections focused on authentication. Zero Trust design concepts radically reduce or prevent lateral movement and privilege escalation during a compromise.
- **Consideration of Managed Service Providers.** Some entities lack the cybersecurity maturity to run effective security programs internally. Increasingly, such entities should rely upon managed service providers to achieve a reasonable level of security. These programs scale easily and are an increasingly affordable way for companies to achieve cybersecurity coverage 24 hours a day, 7 days a week, 365 days a year.

- **Cloud Security.** There are multiple benefits to deprecating legacy, on premises systems and leveraging cloud systems. These include operational efficiencies, enhanced visibility and security, and contracting efficiencies.

As the CPPA is creating audit metrics, the Agency should align with existing, widely adopted standards and guidelines. Splintering standards, across states and the federal government, will result in unintended short-term and long-term consequences. In the short term, different rules and standards will yield divergent results, complicate security training, negatively impact the use of shared resources and services, and complicate collaboration between organizations and agencies. In the long term, independently-developed approaches will lead to confusion with respect to emerging security controls and updates to best practices. Consequently, this increases the risk of cybersecurity incidents.

As such, cybersecurity audits should test compliance against established standards recognized by the Agency as most appropriate, whether that be NIST, ISO, or other widely-used and adopted standards. Currently, NIST is in the process of updating their Cybersecurity Framework. We recommend that the CPPA closely review the final version of the Cybersecurity Framework 2.0 and consider it as a framework organizations can follow during an audit.

B. Risk Assessments

Risk assessments are distinct from audits and should not be standards-driven. The fundamental question of a risk assessment is “how effectively does the security program address the cyber risks the organization faces?” Flexible frameworks are ideal for this type of evaluation as risk assessments need to be tailored for the organization completing it. The best risk assessments should combine the types of security measures but place them in an operational context—both in terms of what threat actors are likely to exploit and what defenders can realistically accomplish.

Risk assessments are an internal exercise, often done under client privilege with a third-party firm, and businesses should not be required to submit risk assessments to the CPPA. Instead, the CPPA should provide a resource of a draft risk assessment to organizations in scope to help them undertake the assignment internally. If organizations were required to submit risk assessments to an agency, it could move

the assessment from a thoughtful exercise to purely a checklist compliance measure. A risk assessment that is shared with an agency might also discourage or deter organizations from fully investigating problems, or digging deeper if an issue is spotted, in fear of repercussions once the assessment has been shared externally.

C. Automated Decisionmaking

From CrowdStrike's perspective, the proposed rulemaking is solely focused on consumers facing automated decisionmaking. CrowdStrike agrees with keeping the focus of the proposed rulemaking on consumer-facing automated decisionmaking or artificial intelligence (AI). In enterprise (B2B) technologies that use AI, a contract has been created and agreed to by both parties which includes privacy protections for individuals that are a part of the businesses entering into the contracts. This is different from consumer facing AI where there is not an agreement in place between the AI technology and every consumer that may come in contact with the technology.

CrowdStrike recommends adding a security carveout into the regulations for all business purposes. This would be in alignment with the exception under section 7050(a)(4) of the Chapter 1 regulations. In cybersecurity, AI is an advantage, especially when added to enterprise security solutions. Cybersecurity threats are exceptionally broad, and for too long industry players have focused on narrow solutions. Security teams demand contextual awareness and visibility from across their entire environments, including within cloud environments. To give an example, with the help of AI, CrowdStrike can stop an attack in its tracks because such technology works faster than conventional signature-based or indicator of compromise (IOC)-based prevention. Usually these use cases fall under the B2B agreements described above, but to ensure that security companies are able to continue protecting against the same threats the CPRA aims to, a cybersecurity technology exemption to the automated decisionmaking section is needed.

III. CONCLUSION

The CPPA's proposed rulemaking represents a thoughtful attempt to strengthen security outcomes in a complex legal and policy environment. As the CPPA moves forward, we recommend continued engagement with stakeholders. Finally, because

the underlying technologies evolve faster than law and policy, we recommend and emphasize that any proposed legislative updates focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike®, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: <https://www.crowdstrike.com/>.

CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E

VP & Counsel, Privacy and Cyber Policy

Elizabeth Guillot

Manager, Public Policy

Email: policy@crowdstrike.com

©2022 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are trademarks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service

marks, and may use the brands of third parties to identify their products and services.

From: Edwin A. Lombard III [REDACTED]
Sent: Monday, March 27, 2023 4:16 PM
To: Regulations
Subject: Comments
Attachments: CPPA Comments ADM (03.27.23).pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Attached please find our comments.

Edwin A. Lombard III



March 27, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Boulevard
Sacramento, CA 95834
Submitted via email: regulations@coppa.ca.gov.

Re: California Privacy Protection Agency (CPPA) Comments PR 02-2023

Mr. Sabo:

On behalf of our respective organizations and the California businesses we represent, we are submitting preliminary comments on the CPPA's proposed rulemaking on Automated Decision Making (ADM). We appreciate the opportunity to provide comments on a significant body of law that will have consequential impacts on the many small, diverse businesses we represent.

Balancing Consumer Protection, Innovation and Evolution of Business Practices

The businesses we represent are an integral part of California's growing economy, contributing to the state's status as the fourth largest economy in the world. Protecting consumers served by our business community is an important value that we share with the CPPA, policymakers and stakeholders as California attempts to shape privacy laws for all of us.

Many, if not most of the business owners we represent have permanently relied on technological innovation for their livelihood and the livelihood of their employees to exist in the reconfigured business platform that we operate in today. As we have previously communicated to the CPPA, under the immense burden of the pandemic, thousands of small businesses have moved more commerce online, dependent on their ability to use technology and keep pace with the cost of doing business to stay afloat, and that online

platforms have been the lifeline for many of these small businesses in serving underserved communities.

As CPPA attempts to draft ADM regulations, we reiterate the importance of achieving and adhering to the balance approach California voters approved in section 3 (c)1 of Proposition 24:

- The rights of consumers and the responsibilities of businesses should be implemented with the goal of strengthening consumer privacy while giving attention to the impact on business and innovation. (Emphasis Added)

Avoiding Potential Adverse Consequences

It is a fact that the traditional way of conducting day to day consumer activities and business platforms are now primarily online, and face to face consumer and business interaction still exist but are fewer today. Technological innovation including ADM plays an essential role in many of the day-to-day consumer activities and operations of the businesses we represent. ADM can seamlessly enhance consumer choice, access, and efficiency in how consumers find and connect with businesses to meet their needs. Similarly, businesses rely on ADM to operate, remain competitive, and build relationships with their customers.

Below are some examples of how our businesses may be negatively impacted if CPPA overreaches in regulating ADM:

- Sales: In plain language, our businesses cannot go back in time to the days of phone book listings or even a pre-pandemic mindset of owning or renting physical space in order to operate. If CPPA mandates consumer opt-outs beyond necessary and legally significant ADS technology, businesses of all lines will suffer and consumers will lose countless gains in choice, relevance and purchasing power they expect to continuously find in today's business environment. The result of overreaching on ADS could be catastrophic for a large number of the small businesses we represent.
- Memberships: Many of our businesses and affiliates rely on memberships, subscriptions, and loyalty programs which can be secured through ADM and consumer preferences. If prospective consumers lose the ability to discover relevant businesses due to overly broad opt-out requirements, such businesses, which are currently serving the needs of customers, could cease to exist. Keep in mind these businesses do not have the resources to change their business model

on the fly or to go back to how they used to operate, including the face-to-face activity with consumers. By the same token, consumers do not necessarily want to reach businesses via a non-online setting.

- Fundraisers: Many of our members, including not-for-profits, use online platforms to raise money for their organizations. They rely on the continuous and economical technology made possible by ADS to reach consumers who care about their cause. They do not have the resources to call or knock on the doors of all their contributors. That type of scale is simply not possible for many of our members – and countless other Californians who rely on ADS for everything from organizing class reunions and virtually connecting church congregations to raising money for youth sports and STEM activities and providing safety information to community members.

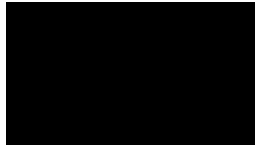
Achieving Balance in Reasonable ADM Regulation

We strongly urge CPPA to shape its rules consistent with the emerging standard of privacy laws. Virginia, Colorado, Connecticut and GDPR in the E.U. all are developing ADM regulations that strike a balance described in Proposition 24, section 3 (c)¹ regarding the regulation's impact on business and innovation. The opt-out rights are limited to profiling based on "solely automated systems that produce legal or similarly significant effects concerning an individual." These provisions are appropriately focused on decisions of significance to an individual's employment, financial status, health care or other basic necessities. California should adopt an opt-out right that mirrors this approach.

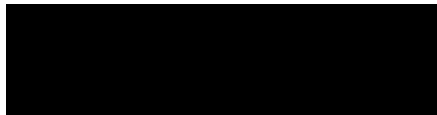
Going beyond what other states and jurisdictions have implemented puts California businesses at an unfair competitive disadvantage. We believe that stringent ADM regulations could be disastrous and could end small and diverse businesses who serve the very consumers that CPPA is attempting to protect. Despite California's current economic ranking, California's economy is fragile and CPPA needs to strike the right balance. Reasonableness on ADM regulation cannot be understated if many of our businesses are to survive.

We appreciate the opportunity to provide comments on a significant body of law that will have consequential impacts on the small, diverse businesses we represent. Our collective organizations are prepared to work with the CPPA in addressing these concerns discussed above.

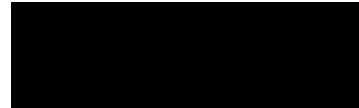
Sincerely,



JULIAN CAÑETE
President & CEO
California Hispanic
Chambers of Commerce
1510 J Street, Suite 110
Sacramento, CA 95814



EDWIN A. LOMBARD III
President/CEO
ELM Strategies
1079 Sunrise Avenue, Suite B315
Roseville, CA 95661



PAT FONG KUSHIDA
President & CEO
California Asian Pacific
Chamber of Commerce
1610 R Street, Suite 300
Sacramento, CA 95811

cc: Members of the Legislature

Dana Williamson, Executive Secretary; Office of Governor Gavin Newsom

Ann Patterson, Cabinet Secretary; Office of Governor Gavin Newsom

Christy Bouma, Legislative Affairs Secretary; Office of Governor Gavin Newsom

Dee Dee Myers, Senior Advisor & Director; Governor's Office of Business & Economic
Development

Tara Gray, Director; California Office of Small Business Advocate

From: Ryan Smith [REDACTED]
Sent: Monday, March 27, 2023 4:07 PM
To: Regulations
Cc: David LeDuc
Subject: PR 02-2023
Attachments: NAI Comments to CPPA re Cybersecurity Audits, Risk Assessments, Automated Decisionmaking.docx

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good evening,

Please find attached comments from the Network Advertising Initiative on the California Privacy Protection Agency's Preliminary Rulemaking Activities on cybersecurity audits, risk assessments, and automated decisionmaking.

Thank you,
Ryan C. Smith

Ryan C. Smith
Counsel, Compliance & Policy
Network Advertising Initiative
409 7th Street, NW, Suite 250, Washington, DC 20004
[REDACTED] | [REDACTED]

March 27, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

Dear Mr. Sabo,

On behalf of the Network Advertising Initiative (NAI), thank you for the opportunity to provide comments on the California Privacy Protection Agency (“CPPA” or “Agency”) Preliminary Rulemaking Activities on cybersecurity audits, risk assessments, and automated decisionmaking.¹

I. Introduction

A. Overview of the NAI

Founded in 2000, the NAI is the leading non-profit, self-regulatory association for advertising technology companies. For over 20 years the NAI has promoted strong consumer privacy protections, a free and open internet, and a robust digital advertising industry by maintaining and enforcing the highest industry standards for the responsible collection and use of consumer data. Our member companies range from large multinational corporations to smaller startups and represent a significant portion of the digital advertising technology ecosystem, all committed to strong self-regulation and enhancing consumer trust. As a non-profit organization, the NAI promotes the health of the digital media ecosystem by maintaining and enforcing strong privacy standards for the collection and use of data for digital advertising across all digital media.

All NAI members are required to adhere to the NAI’s FIPPs-based,² privacy-protective Code of Conduct (the “NAI Code”), which continues to evolve and recently underwent a major revision for 2020 to keep pace with changing business practices and consumer expectations of privacy.³ The NAI continues to monitor state and federal legal and regulatory changes, and our Code evolves to reflect—and in some cases exceed—those requirements. Member compliance with the

¹ https://cpa.ca.gov/regulations/pdf/invitation_for_comments_pr_02-2023.pdf

² See FED. TRADE COMM’N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy_online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

³ See NETWORK ADVERTISING INITIATIVE, 2020 NAI CODE OF CONDUCT (2020) [hereinafter “NAI Code”], https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf.

NAI Code is promoted by a strong accountability program. NAI attorneys subject each NAI member to a comprehensive annual review of their businesses and data collection and use practices for adherence to the NAI Code. In addition, NAI staff advises companies on an ongoing basis about how to best comply with the Code and guidance and how to implement privacy-first practices. Finally, the NAI team conducts technical monitoring and review of company opt outs and privacy tools. Enforcement of the NAI Code can include penalties for material violations, and potential referral to the Federal Trade Commission (“FTC”). Annual reviews cover member companies’ business models, privacy policies and practices, and consumer-choice mechanisms.

II. General Recommendations

The NAI supports the requirement for businesses that process personal information to conduct regular cybersecurity audits and data risk assessments. These risk assessments are also required by privacy laws in Virginia and Colorado—referred to as Data Protection Assessments (“DPAs”)—and are essential for responsible data processing that minimizes risk posed by the collection and processing of personal information. As the NAI considers the needs of our member organizations, we have begun the process of aligning our requirements with those found in the California Privacy Rights Act (“CPRA”) and in other state privacy laws. In response to the state requirements for risk assessments around various types of data and practices, the NAI has begun a process of mapping the requirements to digital advertising practices, with the goal to help companies tailor their own assessments building from core NAI compliance requirements as the foundation.

New state legal requirements for risk assessments can ultimately help level the playing field, extending privacy risk mitigation practices to the entire digital advertising ecosystem, rather than just companies who voluntarily comply with enhanced NAI requirements. However, a set of disparate requirements across multiple states threatens to create an environment where businesses are overwhelmed in their efforts to comply, with no discernable privacy benefit to consumers. The CPRA generally recognizes this by directing the Agency to cooperate with other states and countries “to ensure consistent application of privacy protections.”

Therefore, the NAI urges the Agency to develop and implement regulations that seek to harmonize to the greatest extent possible with the other state laws. We also offer the following recommendations regarding data risk assessments and cybersecurity audits.

Data Risk Assessments

First, in seeking to harmonize risk assessment requirements with other state laws, the Agency should identify a consistent set of criteria for assessments to provide for the performance of a single assessment by businesses. The Agency should maintain a clear emphasis on processing that presents a heightened risk of harm to consumers. The Colorado Privacy Act (“CPA”), Virginia Consumer Data Protection Act (“VCDPA”), and Connecticut Data Protection Act (“CTDPA”) are largely consistent in their identification of activities requiring the performance of

a risk assessment, so aligning with these two laws would not only be a practical step, but also a relatively efficient process. Similarly, Europe's General Data Protection Regulation ("GDPR") requires the performance of data protection impact assessments ("DPIA") for data processing that "is likely to result in a high risk to the rights and freedoms of natural persons." The law sets out three categories in which DPIAs are always required: systematic and extensive profiling with significant effects, processing of sensitive data on a large scale, and systematic monitoring of public areas on a large scale.

Second, while the CPRA makes references to submission of risk assessments on a regular basis, the NAI recommends that the Agency clarify the requirement for performance of annual risk assessments, and allow the Agency to request risk assessments when they are relevant to an investigation or inquiry. This approach would conform with Virginia's privacy law, which provides for submission to the Attorney General upon request when there is an ongoing investigation of a business, and the assessment is relevant to that investigation. This is also consistent with the approach taken under the GDPR, where businesses are required to conduct data impact assessments and to make these records available to a European data protection authority in the event of an audit or investigation arising from the controller's use of the data. Importantly, it helps the Agency balance its resources more effectively by not creating an unnecessary overburden through an automatic production without cause.

Third, while the CPRA appropriately requires businesses to conduct risk assessments only after the law comes into effect on July 1, 2023, the Act does not explicitly clarify that data in a businesses' possession *prior* to the effective date would also not be subject to risk assessments moving forward. We therefore ask that the CPRA regulations clarify by adopting language consistent with Colorado law, which explicitly clarifies the application of the requirement to personal data that a business "acquired on or after" the CPA's effective date. This approach is clear and efficient, providing businesses the opportunity to establish forward-looking assessments and have greater confidence in their compliance efforts.

Finally, the assessments should be confidential, and the rules should recognize that privileged information or trade secrets will be redacted. This presents a practical approach to help companies maintain confidentiality of business practices.

Cybersecurity Audits

The CPRA implementing regulations should clarify that businesses are required to conduct cybersecurity audits on an annual basis, and they should establish clear requirements for retention of audit records. The requirement for cybersecurity audits should maintain a risk-based approach, where businesses can certify that they have implemented and adhere to policies and procedures designed to identify types of personal information and processing practices that present the greatest risk for the consumer's privacy or security. It should be a priority for the Agency to maintain consistency with existing security requirements and practices in California law, as well as those promoted by the FTC, and requirements recently enacted in other state privacy laws.

The NAI recommends that the regulations align with current California law, and other relevant laws, enabling business to utilize existing certifications, such as the ISO 27000 series certification and those that leverage the NIST Cybersecurity Framework. Companies should retain the ability to develop and conduct their own internal cybersecurity program and engage third-party auditors. The Agency can also look to the programs established in cases where audits are required pursuant to consent decrees established by the FTC. Finally, businesses should retain the ability to either select independent third-party auditors of their choice in accordance with a set of qualifications established by the Agency or to conduct internal audits provided there are policies and other safeguards in place to ensure independence. On the latter point, California law already contemplates the ability of companies to conduct independent yet internal audits in the insurance context.

III. NAI Responses to Questions for Public Comment

A. Risk Assessments

The NAI supports the development of uniform, national standards for DPAs. As a self-regulatory body, we believe that standardized assessments are the best way to develop an understanding of emerging business practices, and they can serve as an important tool in compliance and regulation. The NAI's long-standing Code and compliance program is in essence a DPA program to identify and minimize risks surrounding the collection and use of consumer data for digital advertising purposes, predating the legal requirements established under the GDPR and newer U.S. state laws. The NAI's compliance team actively works with companies to assess practices, and as these practices evolve and new privacy risks are identified, we regularly update our Code and associated guidance documents, raising the bar to ensure that NAI members are upholding the highest standards among industry.⁴

The new state law requirements for DPAs can ultimately help level the playing field, extending privacy risk mitigation practices to the entire digital advertising ecosystem, rather than just companies who voluntarily comply with enhanced NAI requirements. Further, the ability of regulators to request access to the results of risk assessments in performing an audit provides enhanced transparency, provided that regulator audits provide essential protections of trade secrets and proprietary practices. Please see responses to some of the specific related questions below.

- ***Q2: What harms, if any, are particular individuals or communities likely to experience from a business's processing of personal information? What processing of personal information is likely to be harmful to these individuals or communities, and why?***

⁴ See NETWORK ADVERTISING INITIATIVE, *Annual Report* (2021), <http://thenai.org/wp-content/uploads/2022/08/2021NAIAnnualReport1.pdf>.

Harms that can arise from processing data depend both on the nature of the personal information, and more importantly, on the use of this information. Therefore, harms from processing personal information arise not from the processing of sensitive data per se, but by how that data is processed and utilized. Indeed, some instances of processing sensitive data actually benefit the marginalized groups and broader society.

The CPRA's requirements emphasize the need to balance the benefits and risks. The CPPA's goal with respect to requiring and assessing DPAs should therefore be to discourage and protect against harmful practices and outcomes, while promoting beneficial uses of data not solely classifying and regulating sensitive versus non-sensitive data. Specifically, in crafting regulations, the CPPA could identify and categorize types of harm instead of data, to promote good uses of data, prevent entities from using privacy law as a pretext to attack competition, while at the same time allowing marginalized individuals to be presented with advertisements and other services relevant to their specific communities. In other words, a functionalist, outcome-based approach to enforcement better protects the civil liberties and rights of consumers while the current typological system abjectly fails to do so.

While the NAI's 2020 Code of Conduct definition of sensitive data largely aligns with the definition established by California and other state privacy laws, there are some categories of data where we diverge; notably, on requirements that consider information about a consumer's race or ethnicity to be sensitive. We recognize and agree that many consumers have increased sensitivity around these data types, and that they could present an increased likelihood of harm to consumers depending on certain processing activities, including disparate outcomes, particularly if processed for purposes such as eligibility determinations. For this reason, the NAI prohibits the use of any data collected for advertising and marketing to be used for eligibility determinations. This approach preserves the ability of companies to tailor advertising based on these categories, and it places restrictions on companies who the data is shared with, further mitigating the potential for harmful outcomes.

The Agency's consideration of privacy and harms in automated decisionmaking should therefore focus on how to identify and regulate the resulting impact from certain processing activities, instead of seeking to create limits on data collection and processing broadly, or based on an expansive set of "sensitive information." The NAI encourages the Agency to fully recognize the beneficial uses of data, including that which could be considered "sensitive," and to craft rules that do not unnecessarily limit the collection and use of data broadly, and to preserve opportunities to benefit protected classes and at-risk populations.

- **Q3: To determine what processing of personal information presents significant risk to consumers' privacy or security under Civil Code § 1798.185(a)(15):**
 - **Q3d: What processing, if any, does not present significant risk to consumers' privacy or security? Why?**

As noted above, the NAI maintains a prohibition on the use of consumer data collected for advertising and marketing to be used for eligibility determinations. Using personal information to serve tailored advertising does not present a significant risk to consumers. Providing and serving advertisements related to an individual's interest in clothing or concerts for example,

In most instances, serving tailored ads for consumer goods and services does not present significant risk to consumers' privacy or security. Some harmful uses, like products and services involving eligibility determinations (such as for homes, jobs, or insurance) can be properly prevented with regulatory guardrails in place. For instance, as referenced above, NAI members are prohibited from using data collected for tailored advertising for these use cases.

B. Automated Decisionmaking

The NAI appreciates the Agency's dedication to determining the appropriate scope of regulations around automated decisionmaking. Because the CPRA does not define automated decisionmaking, we believe it is important to properly scope the definition, to ensure that harmful uses the law aims to prevent are captured, while allowing for uses that do not create harms to consumers.

The GDPR and regulations in the European Union have attempted to define automated decisionmaking and pinpoint when these decisions produce legal effects and when they do not. For example, automated decisionmaking can be used to extend an interview to a job applicant, based on a computer's reading of the applicant's resume, and an algorithm's ability to rank that resume against other applicants. However, decisions like these can carry legal effects—the algorithm may, for example, be biased in favor of white applicants compared to Black applicants, or be biased in favor of men compared to women.

While the CPRA's definition of profiling necessarily incorporates what the CPRA considers to be cross-context behavioral advertising ("CCBA"), the legal effects of this type of decisionmaking are de minimis. The CCPA also provides for consumers to opt out of sales of their personal information, which includes CCBA, so there is not a need to incorporate consumer opt-out rights to tailored advertising within automated decisionmaking. One of the key distinctions worth noting is that automated decisionmaking is a common practice for performance of measurement and attribution in programmatic digital advertising, both tailored advertising and even contextual advertising. Such use cases do not pose significant risk to consumers and therefore should not fall within the definition of automated decisionmaking as it is intended to apply under the GDPR.

The NAI supports the Agency's aims of preventing harmful outcomes from automated decisionmaking, but urges the Agency to be cognizant of already-existing regulatory frameworks, and the different use cases for automated decisionmaking. Please see responses to some specific related questions below.

- **Q2: *What other requirements, frameworks, and/or best practices that address access and/or opt-out rights in the context of automated decisionmaking are being implemented or used by businesses or organizations (individually or as members of specific sectors)?***

The NAI supports the CPRA’s opt-out requirement associated with automated decision making activities, which includes profiling and tailored advertising. The NAI has long required members to provide consumers the ability to opt-out of tailored advertising. Processing that produces legal effects—e.g., processing that affects an individual’s rights, status, or rights under a contract—or similarly significantly affects a data subject is the kind of processing that should be considered the most sensitive, where an opt out would be most necessary.

Most tailored advertising and ad delivery and reporting does not produce legal effects. As discussed above, a legal effect is one where an automated decision affects an individual consumer’s legal rights, such as the cancellation of a contract or granting or denial of a benefit guaranteed by law. Additionally, certain automated decisions could be covered by existing federal and state civil rights laws—such as a decision to extend a job interview to an applicant, where denial based on race would be in direct violation of the law. Comparatively, tailored advertising does not create a legal effect: an advertisement served on a website does not have an impact on an individual consumer’s legal standing.

- **Q3: *With respect to the laws and other requirements, frameworks, and/or best practices identified in response to questions 1 and 2:***
 - **Q3a: *How is “automated decisionmaking technology” defined? Should the Agency adopt any of these definitions? Why, or why not?***

The CPRA does not fully define “automated decisionmaking.” The text of the statute directs the Agency to include profiling in its regulations around automated decisionmaking. The CPRA defines profiling as “any form of automated processing of personal information... to evaluate certain personal aspects relating to a natural person and 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.” Other state privacy laws also reference automated processes in their definitions of profiling, including Colorado, Virginia, and Connecticut.

Outside the United States, the United Kingdom’s Information Commissioner’s Office (“ICO”) defines automated decisionmaking as “the process of making decisions without any human

involvement.”⁵ While this definition is issued in guidance (and does not carry the force of law), it is informative for considering the scope of what automated decisionmaking technology should be. Further, the GDPR defines automated decisionmaking as “automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her,” and 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 analyse [sic] or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour [sic], location or movements.”⁶ The NAI believes that this definition is in line with the text of the CPRA.

- **Q8: 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?**

As noted above, the CPRA already contains thoughtful, detailed requirements regarding CCBA, including requirements to comply with consumer opt-out rights, including honoring opt-out preference signals. Adding additional, differing requirements to the same activities, such as “profiling” through their inclusion as automated decisionmaking is likely to create confusion and extend this separate set of consumer rights more broadly than intended or desirable for policymakers and consumers.

Ultimately, a consumer’s right to opt out of automated decisionmaking technology, including profiling, should vary depending on certain factors. While it is not practical to consider a comprehensive set of factors in regulations, the benefits of automated decisionmaking in

⁵ Information Commissioner’s Office, *What is automated individual decision-making and profiling?*, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/>.

⁶ General Data Protection Regulation (GDPR), Article 22, <https://gdpr-info.eu/art-22-gdpr/>. (Other policymakers agree with the definition of ADM being decisions based without any human involvement: EC Working Party: “Solely [ADM] is the ability to make decisions by technological means without human involvement,” <https://ec.europa.eu/newsroom/article29/items/612053>; Irish DPC: “processing is ‘automated’ where it is carried out without human intervention . . .,” <https://www.dataprotection.ie/en/individuals/know-your-rights/your-rights-relation-automated-decision-making-including-profiling>; Australian Ombudsman: “. . .[AMA] make[s] decision without the direct involvement by a human being at the time of the decision,” https://www.ombudsman.gov.au/__data/assets/pdf_file/0030/109596/OMB1188-Automated-Decision-Making-Report_Final-A1898885.pdf; Grindr: “process of making a decision by automated means without human involvement,” <https://blog.grindr.com/blog/automated-decision-making-and-grindr>; Washington State SB 5116: “automated final decision system is ‘an automated decision system that makes final decisions, judgements, or conclusions without human intervention,’” <https://lawfilesexternal.wa.gov/biennium/2021-22/Pdf/Bills/Senate%20Bills/5116.pdf?q=20230327135742>).

certain circumstances counsel against an overly broad right to opt out of all automated decisionmaking. Therefore, the regulations should encourage companies to adopt a risk-based approach that focuses on outcomes from automated decisionmaking that could have a harmful impact on consumers. When a consumer is served an advertisement based on an inferred interest in cross-country skiing, the harm to the consumer is small to nonexistent. Conversely, when a consumer is subjected to tailored advertising that pertains to eligibility determinations, there is a greater risk of harm or disparate impact. This is where there is an essential intersection with the requirement for companies to provide DPAs. During this process, companies should consider the role automated decisionmaking plays and the potential increased risk to consumers, ultimately determining where human oversight of an automated decision would be beneficial.

The NAI's self-regulatory approach has always tried to maintain a harms-first mentality. For example, in our Precise Location Information Solution Provider Voluntary Enhanced Standards ("Enhanced Standards"), we focus on the harms that come from processing and sharing personal information about certain sensitive Points of Interest, rather than an outright bar on the collection of all location information.⁷ This allows for positive use cases—such as serving a consumer an advertisement for a local coffee shop when they search for “coffee shops near me”—while preventing negative, harmful outcomes, such as inferring a consumer is a part of the LGBT community based on a visit to a gay bar.

IV. Conclusion

Again, the NAI appreciates the opportunity to submit comments to the Agency on this important topic. If we can provide any additional information, or otherwise assist your office as it continues to engage in the rulemaking process, please do not hesitate to contact me at [REDACTED], or David LeDuc, Vice President, Public Policy, at [REDACTED].

Respectfully Submitted,

Leigh Freund
President and CEO
Network Advertising Initiative (NAI)

⁷ NETWORK ADVERTISING INITIATIVE, *NAI Precise Location Information Solution Provider Voluntary Enhanced Standards* (June 22, 2022), <https://thenai.org/accountability/precise-location-information-solution-provider-voluntary-enhanced-standards/#:~:text=The%20Enhanced%20Standards%20create%20restrictions,LGBTQ%2B%20identity%2C%20and%20other%20places.>

From: Ellithorpe, Katrina [REDACTED]
Sent: Monday, March 27, 2023 4:19 PM
To: Regulations
Subject: PR 02-2023 CCPA Preliminary Comments on Cybersecurity
Attachments: SAFE Credit Union-CPPA Public Comment Cybersecurity_03272023.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good evening,

SAFE Credit Union appreciates the efforts made by the Agency to seek input from stakeholders who very much want to aid in the protection of consumer data within reasonable guiderails to succeed in compliance.

Please see our attached comments on proposed rulemaking under the CPRA of 2020 regarding cybersecurity. Thank you for the opportunity to comment and for considering our views.

Best,

Katrina Ellithorpe (She/Her/Hers) | Compliance Analyst
Direct: [REDACTED]
safecu.org | Let us put YOU first.



Sacramento Business Journal Award

BEST PLACE TO WORK 2018-2022

FORBES 2022 BEST-IN-STATE CREDIT UNION

This e-mail contains information from SAFE Credit Union and may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient, be aware that any disclosure, copying, distribution, or use of the contents is strictly prohibited. If you have received this e-mail in error, please contact the sender immediately and delete all copies. This e-mail does not create a legally binding obligation of any kind. Any rates, terms, and conditions are subject to change. See SAFE for details.

Federally insured by NCUA | Equal Housing Opportunity



March 27, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

Re: PR-02-2023 [Invitation for Preliminary Comments on Proposed Rulemaking Cybersecurity Audits, Risk Assessments and Automated Decisionmaking](#)

Dear Kevin Sabo:

I am writing on behalf of SAFE Credit Union (SAFE), which serves 13 counties in Northern California. We have over 234,000 members and over \$4.5 billion in assets. SAFE respectfully submits the following preliminary comments on the proposed rulemaking under the California Privacy Rights Act of 2020 (CPRA).

As a stakeholder, SAFE is interested in providing input on rulemaking and the efforts made by the California Privacy Protection Agency (CPPA) to collect comments on new and undecided issues not already covered by the existing California Consumer Privacy Act (CCPA) regulations. We have gone through the topics you have formulated to guide our comments.

Cybersecurity and Risk Assessment

Regarding the requirement for businesses to perform annual cybersecurity audits and submit to the Agency regular risk assessments about their processing of personal information, we request an exemption for financial institutions. Financial institutions are already heavily regulated and dedicated to the privacy of consumers and should be exempt from requirements of performing additional cybersecurity audits and risk assessments to the Agency. Presently, there are 14 IT/cybersecurity related exams, audits, and risk assessments (collectively referred to as reviews) that SAFE conducts or undergoes annually. These reviews aim to ensure proper protection of consumer data, in accordance with the requirements and recommendations set forth by the National Credit Union Administration (NCUA) and the Federal Financial Institutions Examination Council (FFIEC). Below is a listing of those reviews:

1. Gramm-Leach-Bliley Act (GLBA) / IT Data Risk Assessment
2. FFIEC Cybersecurity Assessment Tool (CAT) / NCUA Automated Cybersecurity Evaluation Toolbox (ACET)
3. Online Banking Risk Assessment
4. Disaster Recovery Testing/Assessment
5. Cybersecurity Incident Response Testing/Assessment
6. External Penetration Testing/Assessment
7. External Vulnerability Testing/Assessment
8. Internal Penetration Testing/Assessment
9. Wireless Penetration Testing/Assessment
10. Social Engineering Testing/Assessment
11. Cybersecurity Threat Risk Assessment
12. CISA Ransomware Readiness Assessment
13. Information Technology General Controls Audit
14. NCUA/Department of Financial Protection and Innovations Exams

If no exemptions are afforded to financial institutions, then the following resources should be utilized as a framework for the creation of cybersecurity audit and risk assessment requirements:

- [FFIEC CAT](#)
- [FFIEC Information Security Booklet](#)
- [NCUA Cybersecurity Resources](#)
- [National Institute of Standards and Technology Cybersecurity Resources](#)
- [Financial Services Information Sharing and Analysis Center \(FS-ISAC\)](#)

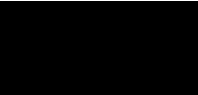
Automated Decisionmaking

While the CPRA provides for regulations governing consumers' "access and opt-out rights with respect to businesses' use of automated decisionmaking technology" and/or "profiling," we would like to help increase distance between these two terms. We do not believe automated decisionmaking and profiling are interchangeable terms. Many companies use automated decisioning to determine if a consumer qualifies for a product or service. Profiling is taking consumers characteristics and matching products. Under no circumstances should a consumer be privy to or have access to a business' automated decisionmaking technology or "logic." Each business determines their own risk-based criteria and logic for an automated decisionmaking tool and providing this type of proprietary information may expose a business' vulnerabilities.

SAFE appreciates the efforts made by the Agency to seek input from stakeholders who very much want to aid in the protection of consumer data within reasonable guiderails to succeed in compliance.

Thank you for the opportunity to comment and for considering our views.

Sincerely,



Sun Park
SVP, Enterprise Risk Management & Internal Audit
SAFE Credit Union

From: Robyn Mohr [REDACTED]
Sent: Monday, March 27, 2023 4:25 PM
To: Regulations
Cc: Robyn Mohr
Subject: PR 02-2023 - News/Media Alliance Preliminary Rulemaking Comments
Attachments: NMA CPPA Comments - Automated Decisionmaking (3.27.23).pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Attached please find the News/Media Alliance's preliminary rulemaking comments.

Thank you,
Robyn

Robyn Mohr (She/Her)

Senior Counsel



901 New York Avenue NW, Suite 300 East | Washington, DC 20001

Direct Dial: [REDACTED] | **Mobile:** [REDACTED] | **E-mail:** [REDACTED]

Los Angeles | New York | Chicago | Nashville | Washington, DC | Beijing | Hong Kong | www.loeb.com

CONFIDENTIALITY NOTICE: This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is STRICTLY PROHIBITED. If you have received this transmission in error, please immediately notify the sender. Please destroy the original transmission and its attachments without reading or saving in any manner. Thank you, Loeb & Loeb LLP.



March 27, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

regulations@coppa.ca.gov

Re: Comments Regarding the Preliminary Rulemaking Activities on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking

The News/Media Alliance (“N/MA” or “Alliance”) welcomes this opportunity to provide comments and feedback to the California Privacy Protection Agency (“CPPA” or “Agency”) in response to its invitation for preliminary comments on its proposed rulemaking on cybersecurity audits, risk assessments, and automated decisionmaking.

The N/MA is a nonprofit organization headquartered in Washington, D.C., representing the news and magazine media industries, and empowering members to succeed in today’s fast-moving media environment. The Alliance’s members represent nearly 2,000 diverse news and magazine publishers in the United States and internationally, ranging from the largest news and magazine publishers to small, hyperlocal newspapers, and from digital-only and digital-first outlets to print papers and magazines.

The Alliance diligently advocates for news organizations and magazine publishers on a broad range of current issues affecting them, including consumer privacy laws and regulations that relate directly to our members’ trusted relationships with their readers. The Alliance respectfully submits the following comments and urges the Agency to carefully consider the potential consequences any subsequent regulations on automated decisionmaking may have on the freedom of the press, and our readers’ ability to easily access a variety of news and content.

Any New Automated Decision Regulations Should Be In Harmony With Existing Laws and Legal Frameworks

The California Privacy Rights Act of 2020 (“CPRA”) provides for the issuing of regulations governing access and opt-out rights with respect to a business’ use of automated decisionmaking technology (including profiling). As the CPPA begins to consider such regulations, the Agency should look to existing data protection laws to inform its approach.

For example, Article 22 of the E.U.’s General Data Protection Regulation (“GDPR”) addresses automated individual decision-making and profiling. Article 22 provides that a data subject has the right not to be subject to a decision “based solely on automated processing” that produces “legal effects” concerning the data subject, or “similarly significantly affects” the data subject.¹ Virginia’s Consumer Data Protection Act (“VCDPA”) also treats automated decisionmaking and profiling somewhat similarly. Under the VCDPA, consumers can opt out of the processing of their personal data for purposes of “profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.”² Again, similar to the GDPR’s Recital 91, the VCDPA requires controllers to conduct a data protection assessment where the processing of personal data presents a reasonably foreseeable risk of: (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers.³ The Alliance believes that the GDPR and VCDPA approach to automated decisionmaking is a workable solution, and any additional CPRA regulations should aim to be consistent with these existing laws.

Consumers Should Have the Right to Opt-Out Where Automated Decisionmaking or Profiling Has Produced Significant Legal Effects

As with many businesses that are subject to the CPRA, news and media publishers use automated decisionmaking technologies for a number of important business purposes. For example, publishers may use automated decisionmaking to categorize or tag content, or to better understand how readers interact with the articles or content on their sites. Automated decisionmaking can help publishers recognize trends and reader preferences, allowing publishers to better deliver personalized experiences to their readers. With digital publications, news and media publishers are no longer constrained by the printed page. Publishers can tailor, reconfigure, and present content and advertising that is relevant and interesting to a particular reader – all of which can be done in the background, by using data the publishers already received permission to collect. In these instances, the use of automated decisionmaking enhances the reader experience, but does not pose significant legal harm to the consumer.

News and media publishers, also use automated decisionmaking to support their digital advertising practices. In crafting new regulations, the Agency should consider excluding the serving of advertisements from the types of decisions that are viewed as producing legal or

¹ General Data Protection Regulation (“GDPR”) Art. 22.

² Virginia Consumer Data Protection Act (“VCDPA”) § 59.1-577. The VCDPA defines “decisions that produce legal or similarly significant effects concerning a consumer” as a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water. VCDPA § 59.1-575.

³ GDPR Recital 91; VCDPA § 59.1-580.



similarly significant effects where the advertisement does not address a protected category (for example, employment, the extension of credit, etc.) or where the serving of the advertisement did not involve sensitive personal information. In the event that the consumer does not want the publisher to use automated decisionmaking to provide them with relevant advertising, the CCPA/CPRA already contemplates a remedy, and provides that consumer with the ability to opt-out of “selling” or “sharing.”

Automated Decisionmaking Regulations Should Focus on Transparency

In many instances where news and media publishers engage automated decisionmaking technologies, publishers are not the parties building or configuring these systems. This means that publishers often have limited insight into how an automated decisionmaking technology actually works, or the processes or formulas used to generate results. As such, regulations should focus on increasing the transparency required of the entities that create and control these technologies, such that users of these technologies can better understand and clearly communicate the necessary information to consumers through privacy policies and access requests.

Similar to the GDPR and VCDPA, the Agency could consider requiring data protection assessments (“DPAs”) where a risk of processing personal information is “likely to result” from the use of automated decisionmaking technology. As with the DPA requirements under other privacy frameworks, additional regulations or restrictions on automated decisionmaking – including the data subject’s ability to opt-out – should be triggered only once a controller has concluded that the automated processing or profiling is likely to produce a legal or similarly significant effect. In these circumstances, transparency from the providers of automated decisionmaking technologies (as discussed above) is critical, because it would enable publishers to properly fulfill these compliance obligations.

Where automated decisionmaking technology produces legal effects, consumers should be entitled to information about how their personal information is being used by these automated systems. When considering additional transparency requirements, we urge the Agency to consider the National Institute of Standards and Technology’s (“NIST”) principles on explained artificial intelligence. NIST’s principles include guidance on how systems should: (1) be explainable; (2) provide understandable explanations to the intended consumers; (3) be accurate; and (4) only operate under conditions for which the system was designed.⁴

The Alliance appreciates the opportunity to provide these comments on the preliminary rulemaking under the California Privacy Rights Act of 2020 (pursuant to Civil Code §

⁴ P. Jonathon Phillips et. al, “Four Principles of Explainable Artificial Intelligence,” U.S. Department of Commerce, National Institute of Standards and Technology, NISTIR 8312, (Aug. 2020)(available at: <https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8312.pdf>).



1798.185(a)(15)-(16)). We are grateful for your consideration, and welcome any further opportunities to provide information to assist the CPPA in this important effort. Should you have any questions regarding these comments, please contact Danielle Coffey, Executive Vice President and General Counsel at [REDACTED].

Sincerely,



Danielle Coffey
Executive Vice President & General Counsel
News/Media Alliance
4401 N. Fairfax Dr., Suite 300 Arlington, VA 22203



From: Ritter, Denneile [REDACTED]
Sent: Monday, March 27, 2023 4:28 PM
To: Regulations
Subject: PR 02-2023 - APCIA Comments
Attachments: APCIA CPRA Preliminary Comment FINAL.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Mr. Sabo,

On behalf of the American Property Casualty Insurance Association, attached please find our comments for the Agency's invitation for preliminary comments on proposed rulemaking on cybersecurity audits, risk assessments, and automated decisionmaking. We look forward to engaging with you and your staff as you work to implement the CPRA.

Best,
Denni

Denneile Ritter
American Property Casualty Insurance Association
Vice President State Government Relations, Western Region
1415 L Street, Suite 670, Sacramento, CA 95814
P: [REDACTED] | [REDACTED]



March 27, 2023

Sent via email

California Privacy Protection Agency
Attn. Kevin Sabo
2101 Arena Blvd., Sacramento, CA 95834
regulations@coppa.ca.gov

RE: APCIA Response to Request for Comments – Proposed Rulemaking Cybersecurity Audits, Risk Assessments, and Automated Decision Making.

On behalf of the American Property Casualty Insurance Association (“APCIA”),¹ thank you for the opportunity to provide these comments in response to the California Privacy Protection Agency’s (the “Agency”) Invitation for Preliminary Comment (the “Invitation”). The topics on which the Agency has invited preliminary comment — cybersecurity audits, risk assessments, and automated decision-making — are of particular interest to the insurance industry. The insurance industry is *already* subject to significant regulatory oversight on all these issues — in California and around the country. Our members appreciate that Agency staff is working diligently on the next steps to address so-called “Topic 21” — how the regulations adopted under the California Consumer Privacy Act (“CCPA”) affect the insurance industry — and we look forward to seeing the Agency move forward with a proceeding on that topic in the coming months, as previewed by Agency General Counsel Philip Laird during the March 3, 2023 Agency Board meeting. Nevertheless, APCIA urges the Agency to consider the significant potential overlap between existing regulations and policy making activities in the insurance industry, and the topics raised in the Invitation. Doing so now will put the Agency in the best possible position to address Topic 21 efficiently and effectively.

I. Existing laws specific to the insurance industry provide a robust set of privacy and cybersecurity requirements.

The insurance industry operates under robust privacy and cybersecurity requirements, including cybersecurity audit and risk assessment requirements. This regulatory framework ensures that insurance companies develop, implement, and maintain a strong set of security measures to continuously monitor and safeguard their information systems and personal information under their control against vulnerabilities and security risks. In California, many of these requirements

¹ The American Property Casualty Insurance Association (“APCIA”) is the primary national trade association for home, auto, and business insurers. APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers, with a legacy dating back 150 years. APCIA members represent all sizes, structures, and regions—protecting families, communities, and businesses in the U.S. and across the globe.

stem from the state's implementation of the federal Gramm-Leach-Bliley Act ("GLBA"), as well as state-specific laws applicable to insurance companies operating in California, such as the California Insurance Information and Privacy Protection Act ("IIPPA"). The CCPA exempts information that is subject to the GLBA and its implementing regulations, as well as the California Financial Information Privacy Act ("FIPA"),² but the examples of these and similar policy making activities should be helpful to the Agency as it moves forward.

The Privacy Rule and the Safeguards Rule of GLBA set forth standards for the development, implementation, and maintenance of privacy and data security practices by financial institutions, including insurance companies. For example, the Safeguards Rule requires covered financial institutions to implement a written information security program that includes administrative, technical, and physical safeguards to protect nonpublic personal information.³ The information security program must be based on a risk assessment that identifies "reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information," and assesses the sufficiency of any safeguards that the insurance company has implemented.⁴ Covered financial institutions must regularly audit the effectiveness of their information security procedures and policies, including by conducting continuous monitoring or annual penetration testing and vulnerability assessments of their information systems.⁵

California law, including IIPPA and FIPA, builds on these requirements. The California Department of Insurance explained in comments submitted in response to the Agency's September 2021 Invitation for Preliminary Comment that the Department's regulations already require insurance companies to implement a security program that is "designed around the CIA Triad of Confidentiality, Integrity, and Availability," based on a risk assessment conducted by the company, and regularly tested and monitored.⁶ In addition, IIPPA permits consumers to access, correct, or delete the personal information collected about them during insurance transactions, and prohibits insurance companies from disclosing personal information without written authorization of an individual or pursuant to another exception.⁷ Likewise, FIPA prohibits financial institutions from disclosing personal information to another entity, with some exceptions.⁸

Insurance companies that operate in California and other states may also be subject to privacy and data security requirements within those states, including laws and regulations based off

² See Cal. Civ. Code § 1798.145(e) ("This title shall not apply to personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code), or the federal Farm Credit Act of 1971 (as amended in 12 U.S.C. 2001-2279cc and implementing regulations, 12 C.F.R. 600, et seq.)").

³ 16 C.F.R. Part 314.

⁴ *Id.* at § 314.4(b).

⁵ *Id.* at § 314.4(d).

⁶ Comments of the California Dept. of Insurance, November 8, 2021, at 2, *available at* https://cippa.ca.gov/regulations/pdf/preliminary_rulemaking_comments_3.pdf (internal quotations omitted).

⁷ Cal. Ins. Code § 791.08–791.09, 791.13.

⁸ Ca. Fin. Code § 4053.5.

model laws drafted by the National Association of Insurance Commissioners (“NAIC”).⁹ The NAIC Insurance Data Security Model Law (“NAIC Model Law”), which has been enacted in 22 states,¹⁰ echoes many of the requirements already in place in California. Under the NAIC Model Law, licensees are required to conduct a risk assessment and develop, implement, and maintain a comprehensive, risk-based information security program based on the risks identified in the risk assessment.¹¹ Further, licensees must subsequently conduct annual risk assessments against their information systems and any third-party service providers’ information systems that have access to personal information controlled by the licensee, to ensure that the licensee’s information security program continues to be properly calibrated to the risks faced by the licensee.¹²

Given the existing set of robust cybersecurity and data protection requirements that already apply to insurance companies, the Agency should seek to harmonize with and leverage existing regulatory regimes and standards. For example, on risk assessments the Agency could require attestations of compliance, as is the general approach under the General Data Protection Regulation (“GDPR”), rather than requiring all regulated entities to submit their entire portfolio of risk assessments. The latter creates significant operational, legal, and security issues – in particular, it would create an enormous “honeypot” for organizations seeking intelligence or insights about how to attack regulated entities.¹³ Likewise, the Agency should be willing to permit cybersecurity audits conducted consistent with other legal regimes or widely-accepted standards to satisfy its requirements. For example, some insurance companies also licensed to operate in New York are subject to additional, stringent cybersecurity requirements because they are subject to the New York Department of Financial Services (“NYDFS”) Cybersecurity Regulation (“Cybersecurity Regulation”), and NYDFS is considering a proposal that would require covered entities to conduct a cybersecurity audit.¹⁴

Moreover, any additional requirements the Agency imposes on already heavily-regulated industries like insurance are likely to create unnecessary conflicts and administrative burdens

⁹ The NAIC serves as a regulatory college and policy coordination body for the insurance commissioners of states and territories of the U.S. Founded in 1871, the organization is governed by the chief insurance regulators from the 50 states, the District of Columbia, and five U.S. territories to coordinate the regulation of multistate insurers.

¹⁰ These states include Alabama, Alaska, Connecticut, Delaware, Hawaii, Indiana, Iowa, Kentucky, Louisiana, Maine, Maryland, Michigan, Minnesota, Mississippi, New Hampshire, North Dakota, Ohio, South Carolina, Tennessee, Vermont, Virginia, and Wisconsin.

¹¹ See *NAIC Insurance Data Security Model Law*, NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS, <https://content.naic.org/sites/default/files/inline-files/MDL-668.pdf>, at Section 4(C) Risk Assessment and Section 4(D) Risk Management.

¹² *Id.* § 4(C)(5) (directing licensees to “[i]mplement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards’ key controls, systems, and procedures”).

¹³ See, e.g., Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, at https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711 (“Is there an obligation to publish the DPIA? No, but publishing a summary could foster trust, and the full DPIA must be communicated to the supervisory authority in case of prior consultation or if requested by the DPA.”).

¹⁴ See *Proposed Second Amendment to 23 NYCRR 500 Cybersecurity Requirements for Financial Services Companies*, NEW YORK DEPARTMENT OF FINANCIAL SERVICES, https://www.dfs.ny.gov/system/files/documents/2022/10/rp23a2_text_20221109_0.pdf. It would make little sense to require companies that already must undertake a cybersecurity audit for one regulator to undertake a completely separate one for a different regulator – such a result merely adds work and burdens to regulated entities without improving the security of consumer personal information.

that actually undermine security. The Biden Administration’s National Cybersecurity Strategy, for example, recognizes that duplicative regulation can actually be harmful to cybersecurity because of the extra burden on cybersecurity personnel, directing federal regulatory agencies to “leverag[e] existing international standards in a manner consistent with current policy and law.”¹⁵ At best, duplicative requirements add to the operational, legal, and administrative burdens of cybersecurity teams that are already stretched thin because of the shortage of qualified candidates.¹⁶ The Agency can avoid this by prioritizing harmonization with existing laws and standards, both in California and in other jurisdictions.

II. Policymakers around the country are already developing regulations and guidance that would govern the insurance industry’s use of automated decision-making.

As with cybersecurity audits and risk assessments, the Agency will not be writing on a blank canvas with respect to regulating the use of personal information in the context of automated decision-making. Topic 16 contemplates an approach to automated decision-making similar to that in GDPR, where data subjects have the right to not be subject to decisions that will negatively impact them and have no human intervention.¹⁷ A similar focus here is both consistent with the statute and a reasonable policy result; in contrast, expanding the scope of the Agency’s focus to capture decisions that could benefit the consumer or that already involve human intervention would unnecessarily increase tension with other aspects of the statute that expressly allow for opt-out rights only when personal information is being sold or shared.

Insurance companies already have extensive risk management frameworks in place to address oversight and assessment of automated decision-making systems, of which privacy considerations are one aspect when personal information is involved. In California, the insurance industry is *already* subject to laws that address concerns related to discriminatory uses of personal information in automated decision-making, as set forth in a bulletin published by the California Department of Insurance.¹⁸ The bulletin explains that insurance companies must “avoid both conscious and unconscious bias or discrimination that can and often does result from the use” of these automated technologies by conducting sufficient due diligence to ensure that its information collection methods, algorithms, and rating, underwriting, and marketing tools are fully compliant with applicable laws, including anti-discrimination laws.¹⁹

Insurers that also operate outside of California are subject to similar requirements that seek to address concerns about the use of personal information in automated decision-making tools. For example, Colorado enacted a law that prohibits insurers from using external consumer

¹⁵ White House, National Cybersecurity Strategy at 9, March 2023, available at <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.

¹⁶ *Id.* at 27 (“Today, there are hundreds of thousands of unfilled vacancies in cybersecurity positions nationwide, and this gap is growing.”).

¹⁷ See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art. 22.

¹⁸ *Bulletin 2022-5, RE: Allegations of Racial Bias and Unfair Discrimination in Marketing, Rating, Underwriting, and Claims Practices by the Insurance Industry*, CALIFORNIA INSURANCE COMMISSIONER (June 30, 2022), <https://www.insurance.ca.gov/0250-insurers/0300-insurers/0200-bulletins/bulletin-notices-commiss-opinion/upload/BULLETIN-2022-5-Allegations-of-Racial-Bias-and-Unfair-Discrimination-in-Marketing-Rating-Underwriting-and-Claims-Practices-by-the-Insurance-Industry.pdf>.

¹⁹ *Id.*

information and algorithms that unfairly discriminate based on individual's protected characteristics (e.g., race, religion, sex, sexual orientation, and disability) in any insurance practice.²⁰

In addition, NAIC has prioritized developing guidance about the use of personal information in automated decision-making. For example, NAIC established the Big Data and Artificial Intelligence (AI) Working Group to study and draft model regulations concerning the development of AI, big data, and machine learning (ML) as well as the use of AI in the insurance industry and potential impacts on consumer privacy and marketplace dynamics. The work of this group is ongoing.²¹ And in 2022, NAIC established the Collaboration Forum on Algorithmic Bias to promote discussion among insurance industry stakeholders on approaches to assessing and addressing potential algorithmic bias in the insurance industry. The Collaboration Forum discusses various AI-specific issues, including which types of algorithms should raise concerns for insurance regulators, how bias might arise in algorithms, which tools might be effective in minimizing bias and detecting bias, and potential regulatory frameworks for addressing algorithmic bias. The Collaboration Forum is guided by the NAIC's Principles on Artificial Intelligence, which emphasize that the insurance industry's use of AI should be fair and ethical, accountable, compliant with all applicable laws, transparent, secure, safe, and robust.

These efforts highlight the work and thought that has already been done on these issues, particularly in the context of the insurance industry, and reaffirm that the Agency should avoid any additional requirements that would create potentially conflicting requirements and more regulatory uncertainty that would not lead to better outcomes for consumers.

III. Conclusion

Insurance industry stakeholders and regulators have already invested significant time, energy, and resources on the questions presented by the preliminary invitation to comment with respect to cybersecurity audits, risk assessments, and the use of automated decision-making. We strongly encourage the Agency to keep these efforts in mind, and seek to harmonize its own efforts with these pre-existing efforts.

²⁰ Colorado Revised Statutes § 10-3-1104.9 (2021).

²¹ Recently, the Working Group has been conducting surveys to understand the use of AI/ML in insurance products to better develop appropriate regulatory evaluation. The Working Group is currently developing a model bulletin to provide a regulatory framework around the use of AI in insurance and hopes for adoption by the NAIC in 2023.

From: Jarrell Cook [REDACTED]
Sent: Monday, March 27, 2023 4:30 PM
To: Regulations
Cc: Lev Sugarman; Andrea Deveau; Alicia Priego
Subject: PR 02-2023 -- Workday Preliminary Comments on Proposed Rulemaking
Attachments: Workday -- Preliminary Comments on Audits, Risk Assessments, Automated Decisionmaking (March 2023) (PR 02-2023).pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hi,

Attached please find Workday's preliminary comments on the Agency's proposed rulemaking on cybersecurity audits, risk assessments, and automated decision making. We appreciate the opportunity the Agency has provided and would be pleased to answer any questions or offer more information at staff's convenience. Thank you!



Comments on Proposed Rulemaking under the California Privacy Rights Act

March 27, 2023

Workday appreciates the opportunity to comment on the California Privacy Protection Agency proposed rulemaking under the California Privacy Rights Act regarding cybersecurity audits, risk assessments, and automated decision making. [Workday](#) is a leading provider of enterprise cloud applications for finance and human resources, helping customers adapt and thrive in a changing world. Workday applications for financial management, human resources, planning, spend management, and analytics are built with artificial intelligence and machine learning at the core to help organizations around the world embrace the future of work. Workday is used by more than 10,000 organizations around the world and across industries – from medium-sized businesses to more than 50% of the *Fortune* 500.

We previously submitted comments on the CPPA's now near-final provisions on service providers in [August 2022](#), and on the proposed rulemaking under the CPRA in [November 2021](#). In this submission, we focus on incremental considerations related to the Agency's proposed rulemaking for cybersecurity audits, risk assessments, and automated decision-making draft regulations, and its related questions in its invitation for comments. We look forward to working with the Agency as it continues developing rules under the CPRA.

Please do not hesitate to contact Jarrell Cook at [REDACTED] if you have any questions or would like further information.

I. Cybersecurity Audits

Workday's top priority is keeping customer data secure. Workday employs security measures at the organizational, architectural, and operational levels to protect customer data, applications, and infrastructure. Because of our deep enterprise customer base and the highly regulated industries in which we operate alongside our customers, Workday completes in-depth enterprise audits and assessments, including ISO 27001, ISO 27017 and ISO 27018 certifications, as well as SSAE 18 SOC-1 and SOC-2 (security, confidentiality, availability, privacy and processing integrity) Type 2 audits. In our previous comments to the CPPA submitted in August 2022, we [recommended](#) that the Agency tailor the scope of audits that businesses can request from service providers, to account for practicality and ensure costs on service providers are proportionate to the policy objectives in question.

The Agency should (1) provide clarity with respect to key scoping terms, including the meaning of "significant risk to consumers' privacy and security," and (2) take a risk-based approach to cybersecurity audits based on a number of factors, while permitting companies to leverage already-existing and applicable cybersecurity standards and best practices.

(1) Clearly define key scoping terms, such as "significant risk to consumer privacy and security."

The CPPA should clearly define the concept of "significant risk to consumer privacy and security" and consider tying the definition – which would trigger the cybersecurity audit requirement – to the definition of "risk" under established cybersecurity standards and privacy laws. The phrase "thorough and independent," on the other hand, provides adequate flexibility to ensure that thoroughness is a case-specific analysis, and that businesses are responsible for defining both the scope of the audit, and "establishing a process to ensure that audits are thorough and independent." The reference to

independent can take many forms, including external independent auditors and internal independent auditors, depending on the context, processing, and other variables.

The CPPA may consider scoping “significant risk” to cover specific *businesses* that process personal information in ways that pose a significant risk to consumers’ privacy and security, as a significant processing activity (subject to potential thresholds). Those activities should be well-defined categories of processing, such as: the sale or sharing of personal information above a certain threshold; processing sensitive data for purposes other than providing a good or services; and automated decision-making, including profiling, on which decisions are based that produce legal effects concerning the consumer.

Recommendation #1: Clearly define “significant risk” and tie the definition to definitions under other data privacy and security laws and frameworks (see Recommendation #3 below, in Risk Assessments). Reaffirm the flexibility intended by the phrase “thorough and independent audits.” Consider defining “significant risk” to cover specific businesses that process personal information in enumerated ways that pose substantial risks to consumer privacy and security.

(2) Take a risk-based approach to cybersecurity audits based on a number of factors, while permitting companies to leverage already-existing and applicable cybersecurity standards and best practices. Specifically, regulations should confirm that the scope of the audit is to be based on a flexible, risk-based analysis of factors, applied by the business on a case-specific basis.

(a) Businesses should be able to leverage existing cybersecurity audits, in whole and in approach.

Cybersecurity audits are an important tool to keep pace with evolving cybersecurity challenges. Importantly, the content of the audits is a key consideration. A wide range of laws and regulations integrate the concept of cybersecurity assessments or audits, including GDPR, U.S. state privacy laws in Colorado, Virginia, and Connecticut, and sectoral regulations, such as the New York Department of Financial Services’ proposed amended Cybersecurity Regulation. The throughline across these examples is an approach consistently allowing businesses to determine the appropriate standards, and leverage industry standards and frameworks (e.g., ISO and NIST). In addition, cybersecurity-related audits, assessments, and/or evaluations are often contractually mandated. These audits may take place when a government contractor is required to abide by and show evidence of compliance with an industry framework (e.g., NIST), when a company chooses to comply with an information security certification program by an independent standards organization (e.g., ISO 27001), or when a data controller requests information, inspects or audits the systems of a data processor under the GDPR and/or current or upcoming U.S. state privacy laws.

Since many companies are already completing such audits, tests, assessments, and/or evaluations of their cybersecurity programs, the CPPA should allow companies to leverage their compliance with data security frameworks and standards to avoid duplication of efforts and inefficient use of resources. At Workday, we work to [ensure compliance](#) with widely-recognized cybersecurity frameworks, including the NIST Cybersecurity Framework, various ISO standards (including 27001, 27017, and 27018), and HIPAA. These frameworks contain a baseline of security controls that have been vetted, proven to address key security risks, and are flexible enough to take account of various types of processing and evolving cybersecurity challenges. The CPPA should allow businesses and service providers to satisfy the CPRA’s requirements by demonstrating compliance with established information security standards. Under this approach, businesses and service providers would have the responsibility to assess compliance against security standards that they deem applicable to their processing activities (such as HIPAA third-party

attestation for health data and the Payment Card Industry Data Security Standard if processing payment card information).

(b) Scope of audits should be based on a risk-based, case-specific approach.

When issuing regulations on the contents of cybersecurity audits, we encourage the CPPA to maintain a risk-based approach and provide covered businesses (and service providers) with sufficient flexibility with respect to implementation. Promulgating overly prescriptive standards may result in significant implementation costs, causing businesses to redirect resources from proactively preventing and mitigating cyber threats to compliance with duplicative requirements. Workday supports the CPRA's current approach of allowing audits to take into account the size and complexity of the business and the nature and scope of processing activities. In addition, an appropriate scope would consider: (1) assessing the existence of physical, administrative, and technical security controls, and (2) ensuring that such controls are tested for any systems or processes that store or transmit personal information.

(c) "Thorough and independent" should be subject to the same flexibility as the scope of the audit.

Businesses should have the flexibility to determine how and by whom independent audits are conducted and, where appropriate, leverage assessments by internal audit teams which typically operate independently from their information security personnel. Such risk-based principles are critical to helping companies determine how to balance significant costs and budget constraints while effectively managing cybersecurity programs.

Recommendation #2: Confirm that the scope of the audit is to be based on a flexible, risk-based analysis of factors, *applied by the business on a case-specific basis*, including: allowing companies to leverage their audits demonstrating compliance with existing industry frameworks; ensuring that service providers do not face audit requirements beyond contractual obligations already defined by CPRA regulations; tailoring the scope of audit requirements on specific factors to be considered by the business, such as the sensitivity of the data and processing, complexity and size of the business, and use of data outside the context of providing goods and services.

II. Risk Assessments

The Agency should (1) provide clarity with respect to key scoping terms, including the meaning of "significant risk to consumers' privacy and security", and (2) take a risk-based approach and permit companies to leverage already-existing and applicable risk assessments (and internal processes) that evaluate the privacy and security of processing activities involving personal information.

(1) Defining "significant risk to consumer privacy and security". The CPRA directs the Agency to issue regulations requiring businesses "whose processing of consumers' personal information presents significant risk to consumers' privacy or security" to regularly submit to the Agency a risk assessment with respect to their processing of personal information. At the outset, it is unclear whether only businesses whose processing activities *generally* present significant risk are required to regularly submit these assessments, or whether the assessments are required for processing activities *that specifically* present significant risk. We recommend the Agency consider our earlier recommendation to define "significant risk" to cover specific *businesses* that process personal information in ways that pose a significant risks to consumers' privacy and security, as a significant processing activity. To the extent that *specific* processing activities that present significant risk trigger the assessment, more clarity is needed as to this

threshold. Currently, the CPRA – unlike the GDPR, the Colorado Privacy Act (CPA), the Virginia Consumer Data Protection Act (VCDPA), and the Connecticut Data Privacy Act (CTDPA) – does not define the scope as to when a privacy risk assessment is required. A comparison to other laws is helpful:

Types of higher risk activities that trigger additional assessments	
GDPR	<ul style="list-style-type: none"> • Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; • Processing on a large scale special categories of data or personal data relating to criminal convictions and offenses; and • Systematic, large scale monitoring of a publicly accessible area. <p>EDPB Guidelines (if two or more are present in processing): Evaluation or scoring; Automated decision-making with legal or similar significant effect; Systematic monitoring; Sensitive data or data of a highly personal nature; Data processed on a large scale; Matching or combining datasets; Data concerning vulnerable data subjects; Innovative use or applying new technological or organizational solutions; and Where the processing prevents data subjects from exercising a right or using a service or a contract.</p>
VCDPA	<ul style="list-style-type: none"> • Processing of personal data for purposes of targeted advertising; • Sale of personal data; • Profiling, where such profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers; • Processing sensitive data; and • Processing activities involving personal data that present a heightened risk of harm to consumers.
CPA & CTDPA	<ul style="list-style-type: none"> • Processing personal data for targeted ads, or profiling, if the profiling presents a risk of (I) unfair or deceptive treatment or unlawful disparate impact, (II) financial or physical injury, (III) physical or other [tortious] intrusion, or (IV) other substantial injury; • Selling personal data; and • Processing sensitive data.

Recommendation #3: Define “significant risk to consumer privacy and security” with specificity and in line with existing legal frameworks that address risk assessments.

(2) Take a risk-based approach and permit companies to leverage already-existing and applicable risk assessments, certifications, and frameworks that evaluate the privacy and security of processing activities.

Since the application of GDPR in 2018, countless global companies, including Workday, have been required to conduct Data Privacy Impact Assessments, or DPIAs, to balance the benefits and bases of certain personal data processing activities with the associated risks. DPIAs are explicitly required under

GDPR for any processing activities that meet the threshold under the GDPR. In addition, companies are required to submit these DPIAs to their supervisory authority in cases necessitating prior consultation or upon request.

In the U.S., the CPA, CTDPA, and VCDPA include obligations for companies to complete data protection assessments in specific circumstances as well. Against this backdrop, the Agency should permit companies to leverage already-existing and applicable risk assessments that evaluate data processing for the purposes of complying with its rules. Importantly, the Colorado, Connecticut, and Virginia laws accept data protection assessments conducted for the purpose of compliance with other laws as satisfactory for compliance as long as the assessments have reasonably comparable scope and effect. The Agency should consider adopting a similar scope and effect approach in this context. In addition, rules should allow businesses to continue to leverage certifications and leading industry standards, such as ISO standards and TrustArc's privacy assurance certifications. Agency rules requiring new and unique risk assessments without a recognition of other comparable assessments as being acceptable for the purposes of compliance with CPRA would pose significant burdens on businesses by requiring unnecessary replication of efforts.

Recommendation #4: Recognize already-existing assessments with comparable scope and effect as acceptable for compliance with CPRA requirements.

(3) Define “regular basis” and “Submit to the CPPA” to mean ‘upon request.’

Conducting regular risk assessments is a key tenet of Workday's proposed approach to a comprehensive privacy framework. In our experience under a similar regulatory scheme in Europe, the Data Protection Directive, submission of risk assessments that companies conduct should be done on request, rather than on a specific timeframe. The Data Protection Directive required entities to file records of data processing with data protection authorities. Authorities were inundated with submissions and ultimately did little with them, with enforcement largely driven by complaints. For this reason, even as the GDPR enhanced privacy protections and toughened enforcement, it eliminated the filing requirement.

Given the number of companies subject to CPRA and the amount of data they process, the Agency would be overwhelmed with regular submissions that show good practices and compliant operations, needlessly drawing Agency resources away from more effective tools, like enforcement. The CPPA should take a similar approach and ask for risk assessments when needed for additional action.

Recommendation #4: Strengthen the rules' risk-based approach by clarifying that risk assessments should be submitted to the Agency upon request.

III. Automated Decision Making

The Agency should (1) ensure that its definition of automated decision making (“ADM”) is consistent with existing frameworks, rules, and widely-endorsed standards; and (2) endorse a risk-based approach to regulating ADM processes and technology that (a) differentiates the obligations and requirements imposed on developers and deployers of ADM, (b) mirrors the scope of access rights provided by existing cross-jurisdictional rules, and (c) provides opt-out rights only for certain high-risk contexts.

(1) Define ADM consistent with other laws. As there is no uniform definition for automated decision making (“ADM”), the Agency should define this term in a manner that is consistent with, and harmonizes, existing definitions in similarly-scoped privacy laws that businesses may already be subject to.

Specifically, the Agency should define “decision making” – which includes profiling (*i.e.*, “automated decision making technology, including profiling”) – by drawing from the definitions of “profiling” in several jurisdictions, including the European Union, Colorado, Connecticut, and Virginia, and define “ADM” as decision making that lacks human involvement or oversight. By mirroring definitions adopted by other states and countries, businesses and organizations will avoid duplicating efforts to characterize their processes and tools, and the scope of the application will be appropriately tailored. Notably, the Agency should ensure that to the extent it makes rules with respect to ADM, it does so in alignment with other initiatives underway in California, such as the Civil Rights Department’s [draft regulations](#) on automated-decision systems and proposed legislation like [AB 331](#).

The GDPR defines “profiling” as “any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject’s performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, *where it produces legal effects concerning him or her or similarly significantly affects him or her.*” (emphases added). The GDPR further provides data subjects with the right not to be subject to a decision based *solely* on automated processing, including profiling.

The CPA defines “profiling” slightly more broadly as “any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual’s economic situation, health, personal preferences, interests, reliability, behavior, location or movements,” but then similarly limits opt out rights only to profiling that is conducted in furtherance of decisions that produce “legal or similarly significant effects,” including the denial of financial or lending services, housing, insurance, criminal justice, employment opportunities, and health care. The CTDPA and the VCDPA follow nearly identical definitions to that of the CPA.¹

These definitions are broad enough to encompass various forms of automated processing while still being specific to providing rights surrounding actual decisions that produce legally significant effects. Leaving the current phrasing undefined could have the effect of inadvertently preventing common-sense business practices that may include automatic profiling, with or without decision-making (*e.g.*, suggesting a worker add certain skills to their HR system profile). Further, a “significant effect” on an individual (absent a “legal” effect), should similarly be limited to instances in which automated processing—without any human oversight or intervention (discussed further below)—tangibly impacts an individual’s material outcomes or status, and are not instances where the processing may be merely relating to a generic profile, advertising, internal processing, or other uses of profiling, artificial intelligence, machine learning, or other processing-only purposes. This would overly limit businesses’ ability to use automated processing or profiling and could result in constraining innovation without commensurate policy benefits.

Drawing from these definitions, the Agency should define “decision making” in the context of ADM with an emphasis on the most salient ADM technologies—those that have a “legal or similarly significant effect” on the user—and define ADM as decision making that lacks human involvement or oversight.

Recommendation #5: The Agency should define ADM in the CCPA through a definition of “decision making” that draws from the definition of “profiling” in several jurisdictions, including the European Union, Colorado, Connecticut, and Virginia, and is narrowly focused on ADM technologies that have a legal or significant effect on a user, as defined above, and lack human involvement.

¹ CTDPA, Conn. Pub. Act No. 22-15, Sec. 1(22) (defining profiling as “any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual’s economic situation, health, personal preferences, interests, reliability, behavior, location or movements”); VCDPA, to be codified in Va. Code tit. 59.1 § 59.1-575 (same).

(2) Risk-Based Approach with Respect to Various Aspects of ADM Technology. In light of the range of differing contexts in which ADM is used across businesses and organizations, the Agency should endorse a risk-based approach to appropriately categorize ADM and align with existing frameworks and rules. Businesses leverage ADM technology in numerous sectors, contexts, and risk profiles. For example, an ADM tool that automatically surfaces a worker's most-used tasks in an HR system presents materially different risks than an ADM tool used to automatically approve mortgage applications. It is important that the Agency develop rules that both manage risk where it is present in ADM processes, while avoiding establishing unnecessary legal obligations for ADM tools that pose minimal risk.

The risk-based approach has achieved consensus among leading proposed AI and ADM regulatory frameworks. The European Union's draft Artificial Intelligence Act expressly imposes differing requirements depending on the level of risk the AI system entails (e.g., unacceptable, high, limited, and minimal risk) and only high-risk systems are comprehensively regulated. Meanwhile, AI systems that are purely accessory in minor decisions such as translation for informative purposes or the management of documents are not covered. Similarly, the GDPR confers rights to individuals "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." In the U.S., the American Data Privacy and Protection Act's (ADPPA) provisions on algorithms set a high water mark for federal bipartisan agreement on AI, taking a similar risk-based approach, placing obligations on entities using algorithms "in a manner that poses a consequential risk of harm to an individual or groups of individuals."

Therefore, the regulations should at least be limited to applying to higher-risk processing, and should explicitly not cover automated decision-making, profiling, and/or automated processing that is not (1) used to make a decision relating to one of the enumerated characteristics about an individual, and (2) solely decided based on ADM. As a result, this means any use of automated processing for low-risk or internal purposes (e.g., cybersecurity threat detection), even if profiling in the general sense, or use of automated processes for decision-making without legal or significant effects on an individual, should not be subject to the CCPA's regulations.

Recommendation #6: The Agency should endorse a risk-based approach in the CCPA to appropriately categorize ADM technologies based on their respective risks in alignment with existing rules and frameworks, and the specific considerations identified in our further recommendations.

(3) Effective risk-based frameworks incorporate important distinctions with respect to roles of developers and deployers in ADM supply chains, the scope of access rights, and the contexts in which opt-out rights are provided to users.

(a) Developers vs. deployers. The Agency should distinguish—and make clear the distinction—between the requirements and obligations imposed on developers (under CCPA, likely to be service providers, contractors, or third parties), as compared to deployers (under CCPA, likely to be businesses) of ADM technology, in alignment with the European Union's proposed AI Act (differentiating between "providers" and "users"), GDPR (differentiating between "controllers" and "processors"), and the ADPPA (differentiating between "covered entities" and "service providers"). In the context of ADM technologies, developers are organizations that create ADM tools for use by enterprise customers and other third parties, whereas deployers maintain a direct relationship with individual end users, control and monitor the ADM tool and the data it relies on, and determine in part how the ADM tool is used with respect to end users.

Recommendation #7: The Agency should differentiate between the obligations and requirements imposed on developers and deployers of ADM technology given their differing responsibilities and access to data and users.

(b) Access Rights. The Agency should look to existing rules across several jurisdictions with respect to the information provided to users about the ADM technology upon request. GDPR provides that where ADM is involved, the data controller (*i.e.*, deployer) must provide data subjects with meaningful information about the logic involved as well as the consequences of data processing. Meanwhile, the CPA, CTDPA, and VCDPA require controllers to specify the purpose for which personal data are collected and processed, the categories of personal data processed, the manner in which individuals may submit a request to exercise their rights, and the categories of personal data that are shared with third parties, if any. In the context of ADM technologies in hiring and promotion decisions, New York City's Local Law 144 provides that upon a written request by a candidate or employee, an employer must provide information about the type of data collected, the source of the data, and the data retention policy. Of course, each of these requirements should be limited to instances where ADM is used to make decisions that have legal effects, which further highlights that any requirements should be imposed solely on the *business* who would have information to evaluate that threshold applicability question.

Recommendation #8: The Agency should follow existing rules across jurisdictions and require deployers of ADM technology to, upon request by a consumer, provide information such as the purpose of the data collection and processing, the categories of data collected, and whether the collected information will be shared.

(c) Opt-Out Rights. The Agency should align with existing frameworks with respect to opt-out rights, and only provide consumers with the right to opt out of data processing for specific purposes such as targeted advertising (already addressed by the CPRA, with respect to the opt out of "sharing"), the sale of personal data (already addressed by the CPRA), or profiling, only where it presents a reasonably foreseeable risk of legal harm such as an unlawful disparate impact, financial injury, intrusion upon seclusion, or includes sensitive data processing. This risk-based approach is appropriate for the CPRA as it will ensure that opt-out rights are appropriately tailored and proportionate to the context and purpose of the ADM technology. However, in contrast to the opt-out rights provided by the aforementioned privacy laws, opt-out rights in the context of ADM technology should allow a user to opt out from a decision being made about them solely based on an output from the ADM technology *rather than* opting out from the use of ADM tools entirely. A decision-focused opt-out enables minimal data processing necessary to, *e.g.*, allow the business to identify the consumer that requested an opt-out and continue to honor the request. In addition, the Agency should recognize several common sense exemptions to opt-out rights where the resultant decisions do not result in personal information being sold or monetized, such as with the execution of a contract. Importantly, the Agency should explicitly recognize multiple forms of opt-outs such as by phone, email, or in the ADM tool itself, to provide consumers with more than one method and to enable businesses to determine the appropriate mechanism to achieve the outcome.

Recommendation #9: The Agency should permit users to opt-out from decisions being made about them based on the outputs of ADM technology in specific, high-risk contexts such as when the use of ADM presents a reasonably foreseeable risk of potential legal harm and ensure that there are common-sense exemptions where decisions do not result in personal information being sold or monetized. The Agency should recognize multiple opt-out methods and avoid prescribing specific means businesses must use to honor them, given the widely varying types and uses of ADM tools.

From: Justin Kloczko [REDACTED]
Sent: Monday, March 27, 2023 4:41 PM
To: Regulations
Subject: PR-02-2023
Attachments: ADMletter.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello—attached are Consumer Watchdog's CPPA rulemaking comments. Thank you.



California Privacy Protection Agency
2101 Arena Blvd
Sacramento, CA 95834

Dear Agency members,

Consumer Watchdog writes to the new rules subcommittee on the topic of profiling and disclosure related to automated decision-making.

Algorithms are increasingly ubiquitous. The Equal Employment Opportunity Commission said in 2022 that 80 percent of businesses are using automated decision-making. However, 85 percent of algorithms throughout this decade will provide false analysis because of bias, according to the American Civil Liberties Union. Taking these two figures into account presents a frightening scenario of a society prioritizing cost and speed over fairness. The results are often a racist or classicist algorithm, a sort of digital redlining that occurs instantaneously and out of view.

The CCPA directs the Agency to issue regulations “governing access and opt-out rights with respect to businesses’ use of automated decision-making technology, including profiling and requiring businesses’ response to access requests to include meaningful information about the logic involved in those decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer.” The plain language of the law requires the agency to let Californians know how they are being profiled, and their right to opt out of automated decision-making. That was the intent of voters when they passed Proposition 24, which endowed Californians with unprecedented control over the use of personal data.

We address the agency’s questions regarding the proliferation of algorithmic discrimination of protected classes and beyond, prevailing European data privacy caselaw, and what consumers should know about algorithmic logic.

More evidence is emerging that discrimination is borne out when people seek a mortgage, apply for a job, credit, school, or government benefits. And it’s usually low-income individuals, people of color, females, religious groups, or those with disabilities who suffer the most as a result of automated decisions. In 2019, home mortgage lenders gave out loans 40%-80% more times to white people than people of color in scenarios where both groups had similar financial characteristics, according to *The Markup*. In addition, high-earning Black applicants with less debt were denied loans more than high-earning White applicants with more debt¹. In 2019, Facebook agreed to enter into a

¹ [“The Secret Bias Hidden in Mortgage-Approval Algorithms,” The Markup, Emmanuel Martinez and Lauren Kircher, August 25, 2021.](#)

settlement with the ACLU for deploying an algorithm that targeted men and excluded women from the audience for traditionally male job openings, like truck drivers².

But we are only beginning to flag the discriminatory flaws of algorithms. As we've seen in Europe and stateside, algorithms stand to categorize and rank people in many ways.

As a guide we reference the General Data Protection Regulation (GDPR), and how the courts and Data Protection Authorities in Europe applied the law. And we see they have come down in favor of college applicants, job seekers and gig economy workers regarding profiling and disclosing logic in automated decision-making.

How Rules Should Be Drawn and What Should be Disclosed

Consumer Watchdog recommends the privacy agency align automated decision-making rules closer to GDPR by writing regulations stating that any right to opt out of automated decision-making should apply to, “a decision based on fully or partially automated processing, including profiling, which produces legal or significant effects concerning the consumer.”

“Legal effects” would occur when someone’s legal rights are affected, such as the cancellation of a contract.

“Significant effects” would be a decision that impacted a person’s circumstances or behavior, such as decisions that affect someone’s financial situation, denies employment or access to education.

For example, the Amsterdam District Court ruled that automated decisions which imposed fines or reduce fares for drivers based on the performance data it collected on them “significantly” affected the driver, and therefore the automated decision was illegal.³

A Finnish data regulator enforcing GDPR found that a financial credit reporting company could not use age as an automatically excluding factor from having a credit application analyzed.⁴ CNIL, the data protection authority in France, looked at how French universities automatically ranked applications based on residence, the order of their wishes, and their family situation. Based on that ranking, the schools automatically made an offer.⁵ And it found this sort of automated ranking of prospective students by university admissions was illegal. This ruling was possible because automated decision-making that legally or significantly effects people was enshrined in the law.

² ["Facebook Agrees to Sweeping Reforms to Curb Discriminatory Ad Targeting Practices," ACLU settlement, March 19, 2019.](#)

³ [Rechtbank Amsterdam](#), Case C/13/689705/HA RK 20-258, March 11, 2021.

⁴ [“Automated Decision-making Under the GDPR,”](#) Future of Privacy Forum, Sebastião Barros Vale and Gabriela Zanfir-Fortuna, May 2022.

⁵ [“Automated Decision-making Under the GDPR,”](#) Future of Privacy Forum, Sebastião Barros Vale and Gabriela Zanfir-Fortuna, May 2022.

In another case, a job application assessment used by a German government entity automatically assessed and ranked job applicants according to predetermined criteria. Applicants' names, addresses, gender and severe disabilities were among the personal data used for the assessment, which was the only way applicants would be invited for interviews. A court concluded that there was profiling and automated decision-making, because the decisions made lacked meaningful human intervention and significantly affected applicants' rights.⁶ Under new regulations, this should be considered profiling and consumers should know about it and be able to stop it.

"Significant effects" generally would not encompass marketing, however, it depends on other factors such as intrusiveness, how people are tracked via other websites, and an individual's situation. For example, advertising could significantly affect someone in a difficult financial situation when that person is targeted with advertisements for high-interest loans because of their debts, signs up for the offer and incurs further debt. This sort of targeted, behavioral advertising, which is the main driver of our modern surveillance economy, should be considered automated decision-making because it significantly affects a person's finances. And consumers should know with specificity why they are seeing an ad that could have legal or significant effects and be given the choice to opt-out of such automated decision-making.

Similar "significant effects" can also be triggered by people other than the individual. For example, GDPR regulations state people should know when other people's personal data is used to make a decision about themselves. For example, a credit card company might lower the credit line for a person, based not on that person's own repayment history, but based on other customers living in the same area who shop at the same stores. This could result in people being deprived of opportunities based on the actions of others. People can be given credit lines who cannot afford it. This logic should be disclosed and allow for users to opt out of this sort of automated decision-making.

Every day uses that are also automated decision-making technology, such as GPS, spam filters, spellcheck, social media feeds, and other lower-risk, widely used tools, would not be subject to the opt out right under the "legal or significant effects" standard.

In Amsterdam, a fraud probability score created by rideshare company Ola was considered profiling, and had to be disclosed to drivers, even if an automated decision was not made based on that score. This was the ruling by the Amsterdam District Court in 2021 after drivers requested information about their fraud probability scores, earning profile, and assigned rides and fines. Regarding the fraud probability score, the court ruled that it was profiling under GDPR because, "through the automated processing of personal data of [applicants], a risk profile is drawn up with which a prediction is made about their behavior and reliability."⁷ The court did not determine automated decisions were made from this, but ruled, "This does not alter the fact that Ola must provide access to the personal data of [applicants] that it used to draw up the risk profile and provide information about the segments into which [applicants] have been classified." New CCPA regulations should state a data subject has a right to be informed by the controller about, as well as have a right to object to profiling, regardless of whether automated decision-making based on profiling takes place.

⁶ ["Automated Decision-making Under the GDPR,"](#) Future of Privacy Forum, Sebastião Barros Vale and Gabriela Zanfir-Fortuna, May 2022.

⁷ [Rechtbank Amsterdam](#), Case C/13/689705/HA RK 20-258, March 11, 2021.

The Italian Supreme Court in 2021, finding it violated GDPR's transparency obligations,⁸ ruled businesses cannot confuse a consumer uploading personal information as permission to score the consumer based on that data. The business in question, which assigned a "reputational rating" to people, still had a duty to disclose the logic of such a score. This distinction should be clear in the new CCPA regulations.

Many legal researchers believe a fundamental duty to explain automated decision-making exists instead of providing abstract information in favor of data controller secrecy⁹. If people are given a bunch of metadata they can't understand, then the regulation is useless. Consumers deserve not just meaningful information, but meaningful *explanation*. A consumer should know the personal data that was processed, the automated decision's consequences for the subject, the factors used to formulate a decision, and what impact on the decision each factor has. Disclosure should be in clear, explanatory terms before the decision happens. Such information is crucial for consumers to understand their situation and be empowered with the appropriate information if they choose to opt out.

Sincerely,

Justin Kloczko, Consumer Watchdog



⁸ [Corte Suprema de Cassazione, Civile Ord. Sez. 1 Num. 14381, May 25, 2021.](#)

⁹ ["The General Data Protection Regulation and Automated Decision-making: Will it deliver?" Bertelsmann Stiftung, Stephan Dreyer and Wolfgang Schulz, January 2019.](#)

From: Jennifer King PhD [REDACTED]
Sent: Monday, March 27, 2023 4:49 PM
To: Regulations
Subject: Stanford submission for PR 02-2023 (part 1)
Attachments: Stanford_ADM_Landscape_Analysis.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Greetings,

Attached please find the first of two submissions by Stanford University for PR 02-2023. This submission is a report, "Landscape Analysis: A Review of Automated Decisionmaking Regulation in and Adjacent to California" by a team of graduate students in the Program in Public Policy.

Thanks

Jen King

--

Jennifer King, Ph.D (she/her)
Privacy and Data Policy Fellow
Stanford Institute for Human-Centered Artificial Intelligence
hai.stanford.edu

<https://hai.stanford.edu/people/jennifer-king>

www.jenking.net/publications

Google Scholar profile: <https://scholar.google.com/citations?user=O5jENBMAAAAJ&hl=en>



Stanford University
Human-Centered
Artificial Intelligence

Via email: regulations@cppa.ca.gov

27 March 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd
Sacramento, CA 95834

RE: Submission of Preliminary Comments (PR 02-2023)

Dear California Privacy Protection Agency,

On behalf of the graduate students under my direction in the 2022-2023 Stanford University Program in Public Policy graduate practicum, I am pleased to submit the following report, "Landscape Analysis: A Review of Automated Decisionmaking Regulation in and Adjacent to California," to the California Privacy Protection Agency (CPPA)'s Preliminary Rulemaking Activities on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking. This report was produced by a team of four graduate students in Stanford's Program in Public Policy as a requirement for their Master's in Public Policy (MPP) degree. Under my supervision, the team researched and produced this report for their capstone project for consideration by the CPPA staff and board.

We appreciate the opportunity to address the CPPA's Invitation for Preliminary Comments on Proposed Rulemaking.

Thank you for your consideration.

Sincerely,



Dr. Jennifer King
Privacy and Data Policy Fellow
Stanford Institute for Human-Centered Artificial Intelligence


The Stanford Institute for Human-Centered Artificial Intelligence
Gates Hall, 323 Jane Stanford Way, Stanford, CA 94305-1234 T 650.725.4537 F 650.123.4567



Landscape Analysis

A Review of Automated Decisionmaking Regulation in and Adjacent to California

Graduate Practicum, Program in Public Policy

Advisor: Dr. Jennifer King

Stanford University

March 2023

1. Table of Contents

1. Table of Contents	2
2. Executive Summary	4
3. Introduction	6
3.1 Background	6
3.2 Problem Statement	6
3.3 Literature Review: Defining and Understanding ADM and Profiling	7
3.3.1 Automated Decisionmaking	7
3.3.1.1 ADM Legislation	8
3.3.1.2 ADM and Artificial Intelligence	8
3.3.2 Profiling	11
3.3.2.1 Profiling-Based Harms	13
3.3.3 Summary	14
4. Data Reviewed	16
4.1 U.S. Federal Regulations	16
4.2 State of California	17
4.3 Other U.S. States	18
5. Findings	18
5.1 Federal Analysis	18
5.1.1 Consumer Protection	18
5.1.1.1 Federal Trade Commission	19
5.1.1.2 Consumer Financial Protection Bureau	21
5.1.2 Civil Rights	23
5.1.2.1 Equal Employment Opportunity Commission	23
5.1.2.2 Department of Housing and Urban Development	26
5.1.3 Federal Synthesis	30
5.2 California State Regulations	31
5.2.1 Fair Employment & Housing	32
5.2.2 California Age-Appropriate Design Code Act	34
5.2.2.1 Summary	36
5.3 Other U.S. States	36
5.3.1 Introduction	36
5.3.2 Rulemaking and enforcement	37
5.3.3 Colorado	37
5.3.3.1 Definitions of Automated Processing	38
5.3.3.2 Profiling Opt-Out Rights — Human-Involved Processing	39
5.3.3.3 Notice and Opt-Out Rights	41

6. Summary of Findings	45
7. Appendix A: Overview of Regulatory Acts	47
8. Appendix B: Colorado Data Protection Assessments	56
8.1 Background	56
8.2 Analysis	58
8.2.1 Differences in Substantive Standards	58
8.2.2 Foreseeability	58
8.2.3 Risks Associated with the Processing Activity Posed by the Processing Activity	59
8.2.4 List of Harms	60
8.2.5 Large and Small Risks	64

2. Executive Summary

Our student practicum team was invited by the California Privacy Protection Agency (CPPA) to analyze legislative and regulatory acts governing automated decisionmaking (ADM) and profiling at the federal level, in California, and in other U.S. states. Definitions of automated decisionmaking vary, and automated decisionmaking has been the subject of various regulatory efforts in the United States and internationally. In this paper, we examine approaches by: U.S. federal agencies; California legislation spanning employment, housing, and child protection; and privacy and data protection statutes in other U.S. states.

Federal agencies take a spectrum of approaches to regulating automated decisionmaking. The Federal Trade Commission takes a broad approach. As part of its regulatory framework, it has articulated generalizable principles for regulating automated decisionmaking. In contrast, the Consumer Financial Protection Bureau and the Department of Housing and Urban Development's approaches are technologically agnostic and apply the similar substantive standards to automated decisionmaking systems that they do to traditional systems. Finally, the Equal Employment Opportunity Commission has adopted requirements for businesses to provide reasonable accommodations for job applicants with disabilities who require accommodations for automated decisionmaking systems to properly evaluate the qualifications of those applicants.

Within California, the California Civil Rights Council (CCRC) has published draft regulations governing automated decisionmaking in the context of employment. The CCRC's regulations provide a broad definition of automated decisionmaking, present specific examples of covered systems, and apply transparency and explainability rules on the use of those systems. Additionally, the legislature passed the California Age-Appropriate Design Code Act in 2022, which imposes considerable requirements on websites serving children. These requirements include a blanket prohibition on profiling based on certain types of data. Both the draft employment regulations and the child-focused statute focus on relatively narrow uses of profiling, and both lack specific criteria for identifying practices that pose an elevated risk of harm.

In addition to California, four states have enacted statutes focused on privacy and/or data protection: Colorado, Connecticut, Utah, and Virginia. Colorado is the only state to have adopted regulations implementing such a statute. The Colorado regulator considered but declined to adopt a definition of "Automated Processing", but it distinguishes between and applies different standards to "Human Involved Automated Processing" and "Human Reviewed Automated Processing". Colorado has also imposed "explainability" requirements for some classes of profiling, but it has not yet articulated specifics on how explainability can be achieved.

The various examined legislative and regulatory acts attempt to reduce ambiguity by enumerating harms that may require intervention, but they diverge in their level of specificity and applicability.

No single definition of automated decisionmaking has been broadly adopted. Substantive regulatory requirements differ due to varying policy goals pursued and constraints faced by different legislative and regulatory authorities.

3. Introduction

3.1 Background

In 2020, California voters approved Proposition 24 (the “California Privacy Rights Act” or CPRA), a ballot initiative which amended the state’s newly created consumer privacy law, the California Consumer Privacy Act (CCPA), and created a new regulatory agency to create and enforce new regulations. The statute describes the new California Privacy Protection Agency (herein, “CPPA”) as “an independent watchdog whose mission is to protect consumer privacy, ensuring businesses and consumers are informed of their rights and to act as enforcer against businesses who violate consumers’ privacy.” The CPPA was officially established with the passage of Proposition 24 and formally received rule-making authority as of April 21, 2022.

One particular focus of the CPRA has been automated decisionmaking (“ADM”). The CPRA delegated regulatory authority over ADM to the CPPA and specifically mandated that the Agency establish regulations governing consumers’ access and opt-out rights for services that use ADM. The CPRA directed the CPPA to consider the use of “profiling” (as defined in the CPRA) when drafting those regulations.¹

Within this developing policy area, various jurisdictions, both internationally and within the United States, have adopted multiple definitions of profiling and ADM. The CPPA is in a unique position to enter the rapidly evolving policy debate as the first dedicated privacy regulator in the United States. In light of a potential lack of consistency between various jurisdictions’ definitions of ADM, as well as the evolving nature of the policy space, the CPPA is seeking to gather more information about the current use and regulation of ADM.

3.2 Problem Statement

This report will seek to answer the following questions:

As the people of California have determined by approving the California Privacy Rights Act (CPRA) of 2020, consumers’ privacy is at risk due to businesses’ automated decisionmaking practices. The California Privacy Protection Agency must protect consumers from such risks, but presently definitions of automated decision-making are emergent and potentially varied. These definitions and requirements should enable regulators and businesses to evaluate whether a given system constitutes ADM. Similarly, they should address the consumer privacy goals of the CPPA with respect to potential options for requirements and/or prohibitions. Lastly, these definitions

¹ Cal. Civil Code § 1798.185(a)(16).

and the associated regulatory requirements and/or prohibitions should harmonize with other laws governing how businesses use ADM in California.

This paper conducts a landscape assessment of current ADM regulations. It does so by analyzing how regulatory authorities in California and across the United States define ADM and other key terms. Our goal is that this analysis will assist the CPPA with its information-gathering process, and will help them to assess the benefits and tradeoffs or gaps revealed by each approach.

Our landscape analysis proceeds as follows: first, we review existing literature discussing and defining both ADM and profiling. This review will guide our analysis of the different approaches a regulator can take when overseeing the use of such technologies, defining them and addressing the harms that stem from them. Next, we will consider existing regulations governing the use of ADM systems introduced by federal U.S. agencies and lawmakers, state regulators in California, and regulations from other U.S. states, with an emphasis on Colorado. Based on this analysis, we will identify common trends and regulatory schemes across jurisdictions, their impact on consumers, and their alignment with the goals of CPPA, as defined by the CPRA.

3.3 Literature Review: Defining and Understanding ADM and Profiling

As part of our literature review process of researching existing materials about consumer privacy regulations and discourse, we primarily focused on the topics of ADM and profiling as well as background materials on Proposition 24. Our research focused on materials within the state of California, other states leading consumer privacy regulation such as Colorado, and U.S. federal agencies.

3.3.1 Automated Decisionmaking

Scholars offer a range of definitions of ADM. Law professor Andrew Selbst describes ADM as an algorithmic system without significant human input specifically used to render judgments.² The judgments made by automated systems can be compared to equivalent judgments normally made by human decisionmakers, and the harms that emanate from them include harms to equality, dignity, autonomy, and safety.³ Cobbe et al. (2021) describe automated systems as those that can either directly produce a decision about the rights or interests of “natural or legal persons” or produce information which a human decision maker considers in making such a decision.⁴ Legal scholar Rashida Richardson describes ADM in her work broadly as: “any tool, software, system, process”, etc., that uses “computation” to “automate [...] decisions”, and in the context of

² Selbst, Andrew D. “An Institutional View of Algorithmic Impact Assessments.” *Harvard Journal of Law & Technology* Volume 35, Number 1 Fall 2021.

³ Ibid.

⁴ Cobbe, Jennifer, Michelle Seng Ah Lee, and Jatinder Singh. “Reviewable Automated Decision-Making: A Framework for Accountable Algorithmic Systems.” In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 598–609. FAccT ’21. New York, NY, USA: Association for Computing Machinery, 2021. <https://doi.org/10.1145/3442188.3445921>.

governmental decisionmaking, any computational tool to aid in the replacement of government decisions.⁵ These definitions are nuanced, where some offer a broader definition while others are more focused and specific.

3.3.1.1 ADM Legislation

Policymakers have introduced legislation at the federal and state levels that includes definitions of ADM. In the Algorithmic Accountability Act of 2022, a bill introduced to the U.S. Senate by Senator Ron Wyden, ADM is defined as “any system, software, or process (including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques and excluding passive computing infrastructure) that uses computation, the result of which serves as a basis for a decision or judgment.”⁶ In Pennsylvania, a proposed bill required that a “business operating artificial intelligence systems” must be registered in the state’s registry that includes information on each business, type of code the business is utilizing for artificial intelligence, and the intent of the software being used. The bill was not reported out of committee and ultimately was not enacted.⁷ Some of this suggested legislation is focused on the result of the automated decisions that would lead to a “decision or judgment”, whereas others are focused on obtaining enough information from businesses, in this case a registry, about the type of automated decision making processes, in order to better monitor their practices.

3.3.1.2 ADM and Artificial Intelligence

Importantly, while ADM systems do not necessarily imply the use of artificial intelligence, there is a significant overlap between the two areas, and laws governing ADM tend to be written to include AI-based systems without restricting definitions exclusively to AI.⁸ ADM systems automate an otherwise human process of decisionmaking, and might do so by using artificial intelligence and machine-learning based systems that have proven adept at identifying patterns and associations that human analysis alone may miss. In such a case, an ADM system could be considered as supported by artificial intelligence. Conversely, an artificial intelligence system might be asked to implement a result from an ADM system, in which case that AI system would act in accordance to decisions made by an ADM system.⁹ However, both types of systems can operate independently.

⁵ Richardson, Rashida. “Defining and Demystifying Automated Decision Systems.” SSRN Scholarly Paper. Rochester, NY, March 24, 2021. <https://papers.ssrn.com/abstract=3811708>.

⁶ Sen. Wyden, Ron. S. 3572. Algorithmic Accountability Act of 2022 <https://www.congress.gov/bill/117th-congress/senate-bill/3572>

⁷ AI Registry, *The General Assembly of Pennsylvania, House Bill No 2903*. Introduced October 26, 2022. <https://www.legis.state.pa.us/cfdocs/billinfo/BillInfo.cfm?year=2021&sind=0&body=H&type=B&bn=2903>

⁸ Neudert, Lisa-Maria, Aleks Knuutila, and Philip N. Howard (2020). *Global attitudes Towards AI, Machine Learning & Automated Decision Making*.

⁹ Araujo, T., Helberger, N., Kruijemeier, S. *et al.* In AI we trust? Perceptions about automated decision-making by artificial intelligence. *AI & Soc* 35, 611–623 (2020). <https://doi.org/10.1007/s00146-019-00931-w>

These definitions also differ based on their generality or specificity to address potential harms: general definitions cast a broad net, such as “a computational process...that makes a decision”, while narrower definitions often target high-risk applications.¹⁰ Definitions may include systems that output “legally significant” decisions as well as those that “assist human decision-making” versus those which “replace it”.¹¹ While the scope of potential harms from ADM systems can exceed those with a direct impact on information privacy, our focus here is on privacy-related ADM harms. To that end, the Future of Privacy Forum, a non-profit group that convenes industry, academic, and civil society groups to develop solutions for privacy policymaking and governance, published a report that seeks to distill down ADM-related privacy harms by providing extensive comparisons of harms and potential mitigations.¹² The report categorizes the harms identified in the literature into four main categories: loss of opportunity, economic loss, social harm, and loss of freedom/autonomy. It also specifies whether these harms affect individuals or groups, and whether they are illegal or unfair. As for potential mitigations, the report categorizes the various harms identified in the previous chart into five groups based on their similarities, with the aim of identifying mitigation strategies that could address each group of harms. As described in the report, “[t]hese groups include: (1) individual harms that are illegal; (2) individual harms that are simply unfair, but have a corresponding illegal analog; (3) collective/societal harms that have a corresponding individual illegal analog; (4) individual harms that are unfair and lack a corresponding illegal analog; and (5) collective/societal harms that lack a corresponding individual illegal analog.”¹³ Their chart includes a description of the mitigation strategies that are best positioned to address each group of harms. For example, the report defines individual harms that are illegal as “those for which American law defines outcomes that are not legally permissible. These harms typically become legally cognizable because they impact legally protected classes in a manner that is defined as impermissible under existing law. Notably, disparate impact may be relevant to illegality regardless of intent in some areas.”¹⁴ When discussing harms, it is noticeable that the discussion seeks to underscore the “context of interactions between individuals, companies, and governments.”¹⁵ We will discuss harms specifically related to profiling in greater depth in the later section on profiling harms.

¹⁰ Sanderson, Pollyanna, Sara Jordan, and Stacey Gray. “Automated-Decision Making Systems: Considerations for State Policymakers.” *Future of Privacy Forum* (blog). Accessed November 9, 2022. <https://fpf.org/blog/automated-decision-making-systems-considerations-for-state-policymakers/>.

¹¹ Ibid.

¹² The Future of Privacy Forum. “Unfairness by Algorithm: Distilling the Harms of Automated Decision-Making.” December 2017. <https://fpf.org/wp-content/uploads/2017/12/FPF-Automated-Decision-Making-Harms-and-Mitigation-Charts.pdf>

¹³ Ibid.

¹⁴ Ibid.

¹⁵ Ibid.

A lack of a consensus definition of ADM may create regulatory confusion among various regulated stakeholders, including consumers and businesses.¹⁶ Broad definitions may lead to an unintended expansion of authority over most computational technological development and a resulting chilling effect over the innovation and development of more advanced systems, as well as an increased regulatory burden for businesses and regulators alike. At the same time, ADM definitions can also risk being too specific. In Canada, for comparison, the Directive on Automated-Decision Making defines an automated decision system as including “any technology that either assists or replaces the judgment of human decision-makers. These systems draw from fields like statistics, linguistics, and computer science, and use techniques such as rules-based systems, regression, predictive analytics, machine learning, deep learning, and neural nets.”¹⁷

The narrowness of the definition in early rule-making processes created a lack of faith that future regulations may have a significant effect on the development of future technologies.¹⁸ According to an article in *The Logic*, a “working draft” of an internal review conducted by the Canadian federal government on its own use of artificial intelligence criticizes the “federal government’s rules for its own use of artificial intelligence and algorithmic tools” for being insufficiently comprehensive, risking the public’s trust in the government’s ability to regulate and use AI effectively.¹⁹ For example, the directive excludes hiring and promotion decisions in which AI systems decide what information human decision-makers see.²⁰ The article also suggests that the directive does not require testing for bias in the models used by algorithms or address what should happen to the results of AI decisions.²¹

Literature offering definitions of ADM describe the considerations which policymakers must address when choosing how to define such systems, and specifically when deciding whether to adopt a general definition, or a specific one. General definitions will usually include a broad definition of an ADM system, without providing a clear dividing line distinguishing such systems from non-ADM automated systems. Such an approach is effective since it provides regulators with maximum flexibility in applying the law to emergent systems. However, general definitions can create uncertainty with regards to future innovation since they lack specific criteria to assess

¹⁶ Winters, Ben. “What’s in a Name”, *Electronic Privacy Information Center*. Oct 27, 2022. <https://epic.org/whats-in-a-name-a-survey-of-strong-regulatory-definitions-of-automated-decision-making-systems/>

¹⁷ Directive on Automated-Decision Making. Government of Canada. 2021-06-28. <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592#appA>

¹⁸ Reevely, David. “Federal Rules on AI too narrow and risk damaging public trust : Internal Review.” *The Logic*. Oct 26 2021. <https://thelogic.co/news/federal-rules-on-ai-too-narrow-and-risk-damaging-public-trust-internal-review/>

¹⁹ Ibid.

²⁰ Ibid.

²¹ Ibid.

whether new algorithms will be subject to future regulation.²² This increases classification burdens on regulators, who will need to assess new innovations without clear criteria and determine whether they fall under existing rules.²³ Specific definitions, on the other hand, expand on a general definition of ADM by offering clear classification criteria or an exhaustive list of in-scope systems. This approach increases certainty for consumers and businesses, and eases regulators' enforcement efforts. However, regulators who adopt such an approach might find that their definition quickly becomes dated, as new technologies emerge and ambiguity surrounding the application of old standards to new innovations arises. A third approach providing a middle ground between general and specific definitions is to adopt a non-exhaustive list of in-scope systems. This method suffers from many of the same broad shortcomings as a general definition, but because enumerated harms can help businesses and enforcement agencies identify at least some criteria used to define ADM systems, the level of regulatory uncertainty is lower under this approach.

3.3.2 Profiling

The CCPA, as amended, defines profiling as “any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of § 1798.185, to evaluate certain personal aspects relating to a natural person and 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.”²⁴ As we discuss below, this definition is nearly identical to the one provided in the European Union’s General Data Protection Regulation (GDPR). Under this statutory definition, profiling is a subset of ADM, which itself is not restricted exclusively to profiling.²⁵ Consumers can experience harms both from profiling itself, as well as non-profiling based ADM. The literature we reviewed supports this conclusion: while profiling inherently relies upon automation, ADM need not include profiling, and consumer harms experienced from either may be distinct.

We reviewed definitions of profiling discussed by academics, as well as other regulatory authorities. Selbst and Barocas discuss current governmental concerns with ADM that include “address[ing] issues of fairness and equity in the commercial use of artificial intelligence (AI)” since “discrimination law as it exists is sector-specific, applying to employment, credit, housing,

²² Scherer, Matthew U., *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies* (May 30, 2015). *Harvard Journal of Law & Technology*, Vol. 29, No. 2, Spring 2016, Available at SSRN: <https://ssrn.com/abstract=2609777>

²³ Nordström, M. AI under great uncertainty: implications and decision strategies for public policy. *AI & Soc* 37, 1703–1714 (2022). <https://doi.org/10.1007/s00146-021-01263-4>

²⁴ Californians for Consumer Privacy. “Annotated Text of the CPRA with CCPA Changes.” Yes on Prop 24. Accessed November 3, 2022. <https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/>. Code 1798.175

²⁵ Californians for Consumer Privacy. “Annotated Text of the CPRA with CCPA Changes.” Yes on Prop 24. Accessed November 3, 2022. <https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/>. Code 1798.175

education, and a few other areas.”²⁶ However, as discussed above, “[s]ome applications of AI can fall outside these contexts and yet still cause significant and disparate harm to consumers. For example, consumer electronics with voice recognition may exhibit systematically worse performance for certain communities, denying these consumers the benefits they’ve paid for, forcing them to deal with the costs of failure, and likely harming their dignity in the process.”²⁷

The European Union’s GDPR defines profiling in Article 3 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 analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.”²⁸ According to an analysis by the European Data Protection Board (EDPB), an advisory body established by the GDPR, the GDPR’s definition of profiling comprises three key elements: “[1]) it has to be an automated form of processing; [(2)] it has to be carried out on personal data; and [(3)] the objective of the profiling must be to evaluate personal aspects about a natural person.”²⁹ This definition “refers to ‘any form of automated processing,’” rather than a more specific form of “‘solely’ automated processing”, and while some automation is necessary for processing to qualify as profiling, having a human in the process does not necessarily exclude the activity.³⁰ The EDPB concludes that “[p]rofilng is a procedure which may involve a series of statistical deductions. It is often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar.”³¹ Additionally, the EDPB notes that according to the GDPR, profiling is defined as the automated handling of personal data with the intent of evaluating particular personal features, including but not limited to the analysis or prediction of an individual’s behavior. Accordingly, classifying or evaluating individuals based on their characteristics, such as age, gender, and height, may qualify as profiling, even if there is no explicit predictive goal.

The Information Commissioner’s Office of the United Kingdom further supports the understanding of profiling as dependent on ADM, but not the other way around: “[a]utomated

²⁶ Selbst, Andrew D., and Solon Barocas. “Unfair Artificial Intelligence: How FTC Intervention Can Overcome the Limitations of Discrimination Law.” SSRN Scholarly Paper. Rochester, NY, August 8, 2022. <https://papers.ssrn.com/abstract=4185227>.

²⁷ Selbst, Andrew D., and Solon Barocas. “Unfair Artificial Intelligence: How FTC Intervention Can Overcome the Limitations of Discrimination Law.” SSRN Scholarly Paper. Rochester, NY, August 8, 2022. <https://papers.ssrn.com/abstract=4185227>.

²⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, Article 3.

²⁹ The European Data Protection Board (EDPB) (Replaced Article 29 Data Protection Working Party). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Directive 95/46/EC. 3 October 2017. http://ec.europa.eu/newsroom/document.cfm?doc_id=47742

³⁰ Ibid.

³¹ Ibid.

decision-making often involves profiling, but it does not have to.”³² Their analysis of ADM includes an example of an exam board that utilizes ADM for grading multiple choice test answer sheets. The system is preset with the specific number of correct responses necessary to achieve passing and outstanding grades. Based on the count of correct answers, the system automatically assigns scores to the candidates, and these scores are accessible on the internet. Importantly, this process of decision-making is automated and does not entail profiling of any kind. The system exclusively relies on the number of correct answers provided by the candidates to determine their scores and does not assess personal data or behavior in any way.

3.3.2.1 Profiling-Based Harms

Across all of these definitions is an assumption that profiling is an activity that inherently entails a set of information privacy-based risks and harms to consumers, from the activity itself as well as its application (e.g., profiles of consumers are applied to targeted advertising or other forms of ADM). Law professors Danielle Citron and Daniel Solove’s seminal article “Privacy Harms” (2022) is widely understood to definitively articulate the harms resulting from various information-based privacy violations. According to Citron and Solove (2022), while “our economy depends upon the collection and sharing of personal data”, the legal system has struggled to recognize many privacy harms as they frequently involve potential future applications or uses of personal data that differ significantly from the context in which data was collected.”³³ Courts have grappled with “recognizing cognizable privacy harms” beyond those resulting in direct economic harm.³⁴ As a potential solution, Citron and Solove recommend that courts adopt a comprehensive typology that, in addition to economic harms, includes privacy harms derived from: physical harms, reputational harms, psychological harms, autonomy harms, discrimination harms, and relationship harms, to make it easier for courts to identify them.³⁵ They note that an appropriate legal response to privacy cases should strike a balance between allowing “socially beneficial personal data practices while requiring robust protections for the handling of personal data.”³⁶ They argue that legislation should focus on deterring violations and encouraging compliance.³⁷ Further, they argue that “[p]rivacy law aims to ensure that personal data is used properly, that individuals have the ability to make decisions about their personal data, and that there are meaningful guardrails and boundaries about how data is collected, used, or disclosed.”³⁸ Lastly, the authors argue that “[w]ith the proper alignment, a broader recognition of privacy harms, a better understanding of privacy problems,

³² Information Commissioner’s Office (ICO). What is automated individual decision-making and profiling? <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/>

³³ Citron, Danielle Keats, and Solove, Daniel J. “Privacy Harms”. *Boston University Law Review*. 2022 <https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf>, pp. 1

³⁴ Ibid. pp. 70

³⁵ Ibid. pp. 3

³⁶ Ibid. pp. 69

³⁷ Ibid.

³⁸ Ibid. pp. 70

and a more flexible approach, the law can more effectively protect privacy in ways that are fair to all stakeholders.”³⁹

Other scholars describe profiling based harms to include consumers losing “consent privileges over their personal information...[they] cannot control who has access to data mines, or to whom information about them is sold. Additionally, there is no assurance that information collected about consumers is accurate or even kept up to date.”⁴⁰ According to law professor Ryan Calo, privacy harms present an acute challenge since in the courtroom it is demanded of privacy plaintiffs to “show not just harm, but concrete, fundamental, or ‘special’ harm before they can recover.”⁴¹ Calo summarizes by underscoring that the issue with “the state of the law around the Privacy Act: a person who was abjectly humiliated by the widespread release of highly personal information by the government would be entitled to no compensation... Whereas a person who suffered one dollar in damages due to a minor violation would recover a thousand dollars.”⁴² These scholars argue that a core issue with profiling and targeting based harms is that it is very difficult to prove them as such in courts under the current regulatory landscape of privacy laws.

In addition to profiling and targeted harms, there are harms that are combined with ADM. According to the National Institute of Standards of Technology in the U.S. Department of Commerce, both profiling and ADM pose an algorithmic bias issue, where the use or creation of data sets that exhibit biases in representation, “improperly utilize protected attributes, or use proxies for protected attributes” leading to discrimination by ADM systems.⁴³ Furthermore, there is ongoing legislation, since, despite the promise of combined ADM and human systems reducing biases and increasing the bandwidth and accuracy of outcomes in decision-making, both types of systems have well-documented biases. As such, there is active lawmaking in various jurisdictions attempting to restrict the potential uses of profiling in ADM systems.⁴⁴

3.3.3 Summary

Since ADM is such an emergent topic, the regulatory environment is not settled on a single definition of ADM. However, there is a clear deference to the GDPR’s definitions. The GDPR focuses on the legal and significant effects the ADM has on individuals, and less on the process of

³⁹ Ibid. pp. 71

⁴⁰ Wendy Netter. Data Profiling Introduction. Berkman Klein Center For Internet & Society at Harvard University. https://cyber.harvard.edu/privacy/Module2_Intro.html

⁴¹ Calo, Ryan. Privacy Harm Exceptionalism. University of Washington School of Law. 2014 <https://digitalcommons.law.uw.edu/faculty-articles/24/>

⁴² Ibid.

⁴³ Schwartz, Reva. “Towards a Standard for Identifying and Managing Bias in Artificial Intelligence.” *NIST Special Publication*, n.d., 86, Page 25.

⁴⁴ Mökander, Jakob, Prathm Juneja, David S. Watson, and Luciano Floridi. “The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: What Can They Learn from Each Other?” *Minds and Machines*, August 18, 2022. <https://doi.org/10.1007/s11023-022-09612-y>.

the ADM itself. As a result, the GDPR thus also focuses on requirements of businesses to provide consumers with specific rights and access, including the right to be informed about the existing ADMs, the logic behind them, and the potential outcomes of ADM. Academics, on the other hand, have provided a more inclusive approach, by highlighting the potential benefits and risks of ADM in a wide range of contexts, including those that may not have significant legal or social implications on individuals. These definitions are useful for researchers who focus on the impact of ADM on society as a whole, rather than on individual consumers who are affected by specific ADM. These different approaches are apparent in the analysis of the literature on the definitions of ADM, and provides an overview of the pros and cons of a general versus a specific definition of ADM. In the first, regulators are given maximum flexibility in classifying new innovations, but create uncertainty that might impact them, businesses, and consumers. In the second, uncertainty is minimized, but regulators might struggle when attempting to classify new technologies as ADM systems. However, the approaches to defining profiling are more aligned across the board. Both the GDPR and academics generally believe that profiling involves the use of personal information to gain insights into an individual's behavior, characteristics, or preferences. Additionally, the GDPR requires businesses to provide consumers with rights relating to profiling, including the right to opt-out of profiling and the right to request human intervention in the profiling process. These highlight the importance of protecting individuals' access and control over the use of their personal information in profiling processes. An analysis of the literature clearly shows the divergence in approaches to definitions of ADM and convergence in the approaches to profiling.

4. Data Reviewed

For the purpose of our landscape analysis, the principal sources of data we considered were existing statutory and regulatory schemes governing the use of automated decisionmaking in various jurisdictions (collectively, “ADM regulations”), these regulations’ definitions of ADM, profiling, and where applicable, analyses of their effectiveness in governing practices of ADM uses in society. In this section, we will briefly summarize the ADM regulations we analyzed arising from authorities spanning the federal government, California, and other state governments.

We present a more detailed overview of the surveyed ADM regulations in Section 7, “Appendix A: Overview of Regulatory Acts”, below.

4.1 U.S. Federal Regulations

A range of federal agencies have weighed in on the use of ADM by commercial actors, each attempting to address the use of such systems in distinct contexts. We identified four main federal agencies which have taken informal or formal regulatory actions concerning ADM: the Federal Trade Commission (FTC); the Consumer Financial Protection Bureau (CFPB); the Equal Employment Opportunity Commission (EEOC); and the Department of Housing and Urban Development (HUD). We will analyze how each of these regulatory bodies addresses ADM.

While the FTC is vested with rulemaking authority under Section 6(g) of the FTC Act, to date it has addressed the use of ADM systems through published guidelines that explain its approach to enforcing existing, non ADM-specific, rules. These guidelines serve as our main data sources regarding the definitions governing the FTC’s enforcement of the use of ADM systems. The two guidance documents we reference are “Using Artificial Intelligence and Algorithms” (2020)⁴⁵ and “Aiming for truth, fairness, and equity in your company’s use of AI” (2021)⁴⁶.

The Consumer Financial Protection Bureau has issued a policy circular concerning the use of “complex algorithms” to make credit decisions affecting individuals. We analyze the Bureau’s definition of ADM by examining the above-mentioned rule, detailed in the “Consumer Financial

⁴⁵ Smith, Andrew (2022) *Using artificial intelligence and algorithms*, Federal Trade Commission. Available at: <https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms> (Accessed: February 6, 2023).

⁴⁶ Jilson, Eliza (2022) *Aiming for truth, fairness, and equity in your company’s use of ai*, Federal Trade Commission. Available at: <https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai> (Accessed: February 6, 2023).

Protection Circular 2022-03” (2022).⁴⁷ As for the Equal Employment Opportunity Commission, we examine a technical guidance document issued by the Commission Chair in 2022 regarding the use of ADM systems when assessing job applicants titled “The ADA and AI: Applicants and Employees” (2022). This source includes guidance on using artificial intelligence in hiring and employment contexts.

Finally, we review a since-reversed “disparate impact” rule adopted by the Department of Housing and Urban Development (HUD) in 2020 which covers the use of algorithm-based tenant screening and clarifies how such use might be regulated by the Fair Housing Act of 1968 (FHA), as well as HUD’s subsequent regulatory actions.⁴⁸

4.2 State of California

In addition to the CCPA, we identified two statutory and regulatory texts governing the use of ADM systems in the state of California. The first is a set of draft regulations concerning employment and housing drafted by the California Civil Rights Council, and the second is the California State Legislature’s 2022 California Age-Appropriate Design Code Act.⁴⁹ We examine both these sources to analyze the extent to which existing California state regulations might impact CPPA’s own rulemaking process in this context.

We analyzed the regulations adopted by the California Civil Rights Council on the use of automated systems to make employment decisions on candidates and employees in 2022, when it was known as the California Fair Employment and Housing Council.⁵⁰

As for the Age-Appropriate Design Code Act, we examine the statute’s language relating to automated profiling of under age Californians. Importantly, this legislation, while adopted, has yet to enter into effect, and we did not identify more detailed guidance from any state official on the implementation of the Act. However, we consider how the language of the law itself might impact CPPA’s rulemaking process, even if the exact implementation of the law is still unclear.

⁴⁷ CFPB (2022) *Consumer Financial Protection Circular 2022 -03*. Available at: https://files.consumerfinance.gov/f/documents/cfpb_2022-03_circular_2022-05.pdf (Accessed: February 6, 2023).

⁴⁸ Foggo, V. and Villaseñor, J. (no date) *Algorithms, housing discrimination, and the new disparate impact rule*, *Science and Technology Law Review*. Available at: <https://journals.library.columbia.edu/index.php/stlr/article/view/7963> (Accessed: February 6, 2023).

⁴⁹ Assembly Bill No. 2273. “California Age Appropriate Design Code Act.” *Bill Resource*, 2022, https://custom.statenet.com/public/resources.cgi?id=ID%3AAbill%3ACA2021000A2273&ciq=ncsl&client_md=a4784fb5c57a6578104e764a8cfbaf33&mode=current_text.

⁵⁰ Fair Employment & Housing Council Draft Modifications to Employment Regulations Regarding Automated-Decision Systems Available at: <https://calcivilrights.ca.gov/wp-content/uploads/sites/32/2022/07/Attachment-G-Proposed-Modifications-to-Employment-Regulations-Regarding-Automated-Decision-Systems.pdf> (Accessed: February 6, 2023).

4.3 Other U.S. States

Four other states have, since 2021, enacted privacy or data protection legislation: Utah, Colorado, Virginia, and Connecticut. Legislation in each of these states includes language in common with the GDPR and is included in our analysis.

5. Findings

5.1 Federal Analysis

We identified four agencies with regulations addressing automated decisionmaking, as well as algorithmic decisionmaking and predictive models:

1. Federal Trade Commission (FTC);
2. Consumer Financial Protection Bureau (CFPB);
3. Equal Employment Opportunity Commission (EEOC);
4. Department of Housing and Urban Development (HUD).

In this section, we discuss the federal regulatory actions related to ADM promulgated by these four agencies and analyze how they respectively inform the ADM regulatory space. We further identify two contexts for these regulatory schemes: **consumer protection** and **civil rights/anti-discrimination**. The relationship between these contexts and privacy regulation is that information collected about individuals can enable discrimination, while consumer protection regulations are often used to stem information collection by commercial actors which can lead to privacy violations.

Congress has not enacted substantial privacy legislation since the 2000 Children's Online Privacy Protection Act (COPPA), and thus there is no omnibus federal level privacy law that provides guidance on this issue. In addition, any of the existing legislation to date focusing on artificial intelligence does not address the question of how to define commercial ADM systems. Accordingly, in this report we will focus on regulatory and rulemaking efforts grounded in existing statutory authority.

5.1.1 Consumer Protection

Congress has, by statute, conferred upon the FTC and CFPB considerable authority to protect consumers. Exercising this authority both agencies have initiated rulemaking processes and produced guidance related to automated decisionmaking.

5.1.1.1 Federal Trade Commission

The FTC has statutory authority to investigate and ‘prohibit unfair and deceptive practices’ under Section 5 of the FTC Act.⁵¹ The FTC is particularly concerned about the use of ADM technology by companies to make decisions about customers that may perpetuate or create unfair outcomes.⁵² To that end the FTC most recently issued guidance outlining specific principles that the FTC intends to enforce through lawsuits and other regulatory actions.⁵³ These principles include:

1. *Transparency*: notifying consumers about the use of data, collection of sensitive data, and the prohibition of deceptive or misleading claims around the use cases of automated tools;
2. *Explainability*: Providing information about automated decisions to ensure customers both understand why a negative decision was made and the factors that went into making the automated decision;
3. *Fairness*: Information about the inputs into automated decisions, outcomes, and omission of use of protected class information. Most significantly, consumers must have the ability to access and correct erroneous information about themselves;
4. *Empirical Soundness (accuracy)*: If a business provides data to various third party decisionmakers, the business has obligations regarding accuracy, compliance with existing laws, and notification. Beyond that, the AI models themselves should be validated on an ongoing basis for their correctness and outcomes. The guidance does not explicitly set forth specific benchmarks;
5. *Accountability*: Businesses are responsible for preventing unauthorized uses, as well as for their selection and representative nature of the datasets they use.

Analysis

Despite the fact that the FTC’s Guidance is preliminary in advance of any potential regulatory actions⁵⁴, given the broad mandate of the FTC and its history in influencing corporate behavior through both legal precedent and policy guidance, the Guidance is likely to shape businesses’ ADM practices. Because the FTC is subject to Moss-Magnuson rulemaking requirements, which can take in excess of five years to complete, the FTC has a history of issuing guidance to signal the kinds of practices that may lead to the Agency’s opening an investigation.

⁵¹ 5 USC § 45

⁵² Jilson, Eliza (2022) *Aiming for truth, fairness, and equity in your company’s use of ai*, Federal Trade Commission. Available at: <https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai> (Accessed: February 6, 2023).

⁵³ Smith, Andrew (2022) *Using artificial intelligence and algorithms*, Federal Trade Commission. Available at: <https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms> (Accessed: February 6, 2023).

⁵⁴ E.g., the Agency’s 2022 ANPR rulemaking.

The principles of transparency, explainability, and fairness as described in the Guidance place explicit ADM-related obligations on businesses, with explainability presenting the most challenging obligation for those using machine learning based forms of ADM given the known challenge of tracing the logic of decisionmaking within these systems. However, as we discuss in our literature review, not all ADM systems use machine learning, and despite this challenge, there is a considerable risk to consumers of being subject to ADM systems that produce discriminatory or unfair results with no means to interrogate the reasons why adverse decisions were rendered.

Because the FTC's Section 5 authority is concerned with deceptive and misleading business practices, the focus on the validity of the outputs of ADM models relative to any claims made by a business is key. And, to the extent that a business's ADM-based practices invoke "consumer access to credit, employment, insurance, housing, government benefits, check-cashing or similar transactions", the Agency warns that such practices may be also subject to the Fair Credit Reporting Act (FCRA). Accordingly, the Guidance warns businesses about the need to focus on both the inputs (data collected directly or purchased/exchanged) as well as outputs of ADM systems to ensure compliance with the FTC Act. In such a scenario where data inputs to ADM systems are used towards any of the above ends, then tracing them is required in order to provide consumers with information about how a decision was reached. Beyond this, in the event that the inputs are inaccurate or incomplete, the consumer must be given the opportunity to correct them. In this manner, ADM data inputs must explicitly be monitored and managed for compliance (and eventually regeneration of outputs if corrections are forthcoming). The FTC's seriousness on this point is exemplified by the FTC's recent enforcement actions against Everalbum and WW, in which the company opted individuals into facial recognition without their consent and then used this data to build facial recognition models.⁵⁵ As such, not only the data but the models used for facial recognition were required to be deleted. This action illustrates that the FTC is willing to force a company to disgorge both its data and models if data is acquired and used improperly.

With this Guidance, the FTC is attempting to prevent general consumer harms in ADM systems. The FTC's approach includes both profiling and non-profiling ADM based harms. The guidance and principles are not profiling-specific, but it clearly alludes to some specific profiling harms when detailing these principles. For this reason, we can consider the principles expansive across different types of ADM systems and inclusive of profiling since the five principles highlighted in the Guidance apply to harms that result from profiling-specific ADM systems. Preventing

⁵⁵ See generally: Staff, the Premerger Notification Office, and Stephanie T. Nguyen. "FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology." *Federal Trade Commission*, 18 Sept. 2021, <https://www.ftc.gov/news-events/news/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse-facial-recognition-technology>; <https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers-illegally-collecting-kids-sensitive>.

autonomy, discrimination, and economic harms are within the purview of the FTC given its broad unfairness mandate, including those with a direct impact on consumer privacy. Transparency and explainability rights both attempt to restore consumer autonomy, while fairness and explainability both have a meaningful impact on economic harms stemming from discrimination.

5.1.1.2 Consumer Financial Protection Bureau

The Consumer Financial Protection Bureau, established in 2011⁵⁶ in the wake of the 2008 financial crisis, is responsible for regulating consumer protection in the financial sector. Its authority to regulate automated decisionmaking arises from the 1974 Equal Credit Opportunity Act (ECOA, 15 U.S.C. § 1691)⁵⁷, which prohibits discrimination based on: a protected class; an exercise of rights under the Consumer Credit Protection Act; or “if the applicant receives income from a public assistance program.”

Regarding ADM, the Bureau issued a Rules Circular focused on transparency and notification in 2022⁵⁸. The Rules Circular provides that:

“Whether a creditor is using a *sophisticated machine learning algorithm* or more conventional methods to evaluate an application, the legal requirement is the same: Creditors must be able to provide applicants against whom adverse action is taken with an accurate statement of reasons. The statement of reasons “must be specific and indicate the principal reason(s) for the adverse action.”

The use of a Rules Circular is noteworthy given the CFPB’s position as the “principal federal regulator responsible for administering federal consumer financial law.”⁵⁹ However, it is not the only body that seeks to enforce such laws. State regulators as well as offices within the Department of Justice, FTC, and the Federal Reserve are some of the other regulators which regulate financial services companies. The Circular itself creates transparency and signals intent to these other bodies as well as to the broader CFPB staff, encouraging a consistent approach. That said, a Circular does not in and of itself have the force of law to focus the CFPB’s powers or create a legal obligation on any other party, and should be considered a declaration of intention for the CFPB’s current thinking and future actions.

Analysis

⁵⁶ CFPB (no date) *About Us*. Available at: <https://www.consumerfinance.gov/about-us/> (Accessed: February 6, 2023)

⁵⁷ Department of Justice (2018) *The Equal Credit Opportunity Act*. Available at: <https://www.justice.gov/crt/equal-credit-opportunity-act-3/> (Accessed: February 6, 2023).

⁵⁸ CFPB (2022) *Consumer Financial Protection Circular 2022 -03*. Available at: https://files.consumerfinance.gov/f/documents/cfpb_2022-03_circular_2022-05.pdf (Accessed: February 6, 2023).

⁵⁹ CFPB (no date), *About Consumer Financial Protection Circulars*. Available at: <https://www.consumerfinance.gov/compliance/circulars/about/> (Accessed March 18

ECOA and Regulation B have preceded the current discussion about ADM by nearly 50 years, establishing a legal framework focused on anti-discrimination. In the event of denial of credit or other adverse action by a credit provider, this framework has long required an explanation for denials of credit. In this manner, the Circular merely notes that algorithmic tools are not exempt from existing applicable legal requirements.

The principles motivating these requirements are based in consumer education. ECOA, for example, focuses on system inputs as a means to make decisions more transparent and to provide consumers with information about how a decision was made. For example, if a consumer understands what the factors are behind the denial of credit, they have the ability to challenge the use of the information, or in fact take steps to remedy the information or outcome. As an example, a small number of open credit lines is regularly used to negatively impact credit in part because it increases credit utilization.⁶⁰ Regardless of the consequences of this factor, knowledge of it is a first step by an individual to build better credit overall.

The Circular is focused on actions taken by creditors rather than on the methods the creditors use. The regulations are agnostic to whether a human or algorithm displays bias: the regulations are focused upon the fact of bias itself in the output of an ADM system. As a result, the narrowness of the Circular's focus on creditors will limit how generalizable the regulatory requirements and/or prohibitions may be for other regulators for a more broad set of potential ADM users.

As a potential regulation, this Rule is potentially resilient to changes in technology—in particular, it clarifies that the complexity of an algorithm does not excuse a creditor from these requirements. This clarity and neutrality can be attributed to the creditworthiness determination systems articulated in Regulation B, which address disparate impacts. In addition, the Circular notes the use of an ADM system does not reduce the requirements of knowledge about how the decision is made and what factors are involved.

To consider the applicability of the CFPB rules to the broader regulatory landscape, it is worth explicitly considering its approach to the ADM harms earlier identified in the Literature Review of particular interest in ADM and profiling systems. One of the CFPB's primary mandates is to prevent economic harms that result from discrimination in the financial services sector. It is for this purpose that protected characteristics are specifically called out in their Circular and prohibited as input. While the CFPB may be agnostic to the processing system used to make decisions, it is not agnostic to the inputs or the outcomes. While the existing law attempts to empower individual autonomy through its disclosure and notification methods, loss of autonomy is not a primary harm motivating the rules given that the harm itself is based on the economic opportunities presented. The CFPB's focus on economic harms clearly gives such harms precedence over autonomy harms:

⁶⁰ CFPB (2020). *How do I get and keep a good credit score?*. Available at: <https://www.consumerfinance.gov/ask-cfpb/how-do-i-get-and-keep-a-good-credit-score-en-318/> (Accessed: March 18, 2023).

measures to empower autonomy are only taken to address or remediate a potential economic harm. An alternative approach may include empowering the autonomy of consumers regardless of whether an economic or other harm were already identified such as a broader opt-out right of an ADM system regardless of the credit decision.

5.1.2 Civil Rights

Agencies have also begun to regulate the use of automated decisionmaking in the context of civil rights protections. In particular, the Equal Employment Opportunity Commission (EEOC) and the Department of Housing and Urban Development (HUD), two agencies tasked with civil rights enforcement, have issued relevant guidance documents.

5.1.2.1 Equal Employment Opportunity Commission

The EEOC has statutory authority to investigate violations of workplace discrimination laws. In particular, the EEOC has authority to enforce the Americans with Disabilities Act, which “makes it unlawful to discriminate in employment against a qualified individual with a disability”.⁶¹

The Chair of the EEOC has issued a technical guidance document entitled “The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees” (the Guidance). The Guidance is intended to “explain how employers’ use of software that relies on algorithmic decision-making may violate existing requirements under Title I of the Americans with Disabilities Act”.⁶² The Guidance was issued directly by the Chair of the EEOC and therefore lacks the force of law; however, it does indicate the position that the EEOC might take in enforcement and litigation. The Guidance requires that employers who use algorithmic tools to screen applicants must offer a reasonable accommodation for any evaluation performed by an algorithmic decision making system. The Guidance also determines that ADM systems that “screen out” applicants “because of a disability” are prohibited under the ADA:

“An example of screen out might involve a chatbot, which is software designed to engage in communications online and through texts and emails. A chatbot might be programmed with a simple algorithm that rejects all applicants who, during the course of their “conversation” with the chatbot, indicate that they have significant gaps in their employment history. If a particular applicant had a gap in employment, and if the gap had been caused by a disability (for example, if the individual needed to stop working to undergo treatment), then the chatbot may function to screen out that person because of the disability.”

⁶¹ EEOC (no date) *The ADA: Your Responsibilities as an Employer*. Available at: <https://www.eeoc.gov/publications/ada-your-responsibilities-employer> (Accessed: February 6, 2023).

⁶² EEOC (2022) *The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees*. Available at: <https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence> (Accessed: February 6, 2023).

Of particular note, the Guidance indicates that the following is important for employers:

“Ensuring that the algorithmic decision-making tools only measure abilities or qualifications that are truly necessary for the job—even for people who are entitled to an on-the-job reasonable accommodation. Ensuring that necessary abilities or qualifications are measured directly, rather than by way of characteristics or scores that are correlated with those abilities or qualifications.”

Analysis

While the Guidance explicitly lacks the force of law, it is suggestive of future enforcement against companies that act inconsistently with the requirements of the Guidance. Unlike the other regulatory acts we have discussed, the Guidelines’ “reasonable accommodation” provision requires businesses to ensure that the choice of *inputs* to their screening-out ADM systems avoids discriminatory effects.

Protected demographic characteristics cannot be used by employers or ADM systems used for employment due to potential disparate impact effects. While the Guidance does not specifically mention profiling, the Guidance’s recommendation that “necessary abilities or qualifications” should be “measured directly, rather than by way of characteristics or scores that are correlated with those abilities or qualifications”, serves to discourage certain forms of profiling in employment.⁶³

The EEOC’s requirements for direct measurement may have an unintended outcome of creating a *de facto* standard for certain kinds of educational qualifications, preventing the adoption of new or adapting forms of performance measurement. A mandate for direct measurement may prioritize existing and predominant forms of credentialing which are at present considered direct predictors of performance.⁶⁴ If such a mandate occurs, it will likely benefit traditional credentialing-based forms of education such as degrees and current certificate programs or performance evaluation. This may slow an expansion of credentials such as online degrees, new universities, or even practical forms of accreditation in the form of non-traditional apprenticeships where evaluation is more subjective and less standardized. There are clear benefits in the employment context with respect to creating stricter guidelines for the protection of applicants from discrimination. However, much care must be taken in non-employment contexts in attempting to generalize given specific peculiarities of the employment context.

⁶³ Lohr, Steve. “Millions Have Lost a Step into the Middle Class, Researchers Say.” *The New York Times*, The New York Times, 14 Jan. 2022, <https://www.nytimes.com/2022/01/14/business/middle-class-jobs-study.html>.

⁶⁴ Americans With Disabilities Act of 1990, 42 U.S.C. § 12101 et seq. (1990) *ADA.gov*, <https://www.ada.gov/law-and-regs/title-iii-regulations/>. (Accessed March 22, 2022)

Among the regulatory acts we discuss, the requirement for reasonable accommodation is unique because it requires ADM system users to affirmatively provide an alternative to an ADM system. Under the EEOC recommendations, the users of an ADM system (employers) must allow for an alternative form of input to make the same determination of employment. This is emphasized — though without example—when the Guidance specifically notes that one way an employer’s ADM hiring tools could violate the ADA is that “[t]he employer does not provide a “reasonable accommodation” that is necessary for a job applicant or employee to be rated fairly and accurately by the algorithm.” Because automated provision of "reasonable accommodations" is likely impractical, in some ways the "reasonable accommodation" right conferred by the Guidance resembles a stronger version of an opt-out right for applicants covered by the ADA. Specifically, applicants have the right to opt-out of the automated processing of their application, coupled with an affirmative right for their application to be treated on even or better terms as other applicants.

In this manner, it appears that the EEOC may create an opt-out and a requirement to accommodate through a non-ADM method on the provider of the ADM system as compared to merely prohibiting certain inputs. Removing an input from an ADM (or choosing not to collect a particular form of data in the first place) is technically fairly simple—but defining and sourcing an alternative which does not function as a proxy is more challenging. The input data is not removed only since that is considered an ‘unfair’ outcome. In doing so, the EEOC creates a new, more gray spectrum of regulatory outcomes for inputs by ensuring some representative data is used for making judgments. How these alternatives are defined leaves many options for definition and therefore tradeoffs for outcomes of applicants and employers.

In terms of ADM-based harms, the EEOC’s focus is on discrimination and economic harms. The primary economic harm is a loss of opportunity—which could be limited to a single job, but concerningly could be systematic if ADM systems perpetuate discrimination across protected categories. Harm to individual autonomy flows both from potential discrimination as well as an inability to understand on what basis why one has been rejected. However, the EEOC in particular focuses on inputs such as protected characteristics and other information directly tied to an individual to evaluate their past and future performance. This practice appears to align with current ADM profiling definitions. The EEOC’s approach to discriminatory harms therefore appears based on profiling—given the level of profile necessary in hiring decisions. The significance of a focus on profiling implies limitations for the applicability of this approach to non-profiling ADM harms. The EEOC has used its power to ensure that the profiles generated are – by its definition—more balanced and holistic. It is to be seen whether this action is significant enough to mitigate the discrimination harms motivating the action given that there are no such examples of this kind of mandate as they apply to automated decisionmaking systems.

5.1.2.2 Department of Housing and Urban Development

HUD is responsible for enforcement of laws relating to housing discrimination, including the Fair Housing Act of 1968 (FHA), which prohibits discrimination in various housing decisions based on “race, color, religion, sex, familial status, or national origin.”⁶⁵ Pursuant to 42 U.S. Code § 3614a, HUD has the authority to issue rules implementing the Act. HUD adopted a “disparate impact” rule for the adjudication of discrimination claims. The most recent form of this rule was adopted in 2013, under which a person is liable for unlawful discriminatory housing practices under the Fair Housing Act if those practices had a “disparate impact” on a specific group of persons due to protected characteristics, even if those practices were “facially neutral.”⁶⁶ In the event that this burden of proof was reached, the practice could be challenged based on whether a “substantial, legitimate, and non-discriminatory interest” is served by the practice, but even then the organization or individual whose system which used a given process may be required to change practices if an alternative process with a less discriminatory effect could be used.

However, as we explain below, since 2013 this standard has been repeatedly reexamined as exemplified in the following 2019/2020 rule making process. In 2019, HUD proposed a new rule for implementation of this standard, with a specific section devoted to algorithmic models:

“Paragraph (c)(2) provides that, where a plaintiff identifies an offending policy or practice that relies on an algorithmic model, a defending party may defeat the claim by: (i) Identifying the inputs used in the model and showing that these inputs are not substitutes for a protected characteristic and that the model is predictive of risk or other valid objective; (ii) showing that a recognized third party, not the defendant, is responsible for creating or maintaining the model; or (iii) showing that a neutral third party has analyzed the model in question and determined it was empirically derived, its inputs are not substitutes for a protected characteristic, the model is predictive of risk or other valid objective, and is a demonstrably and statistically sound algorithm.”⁶⁷

The defenses outlined above which would could defeat a claim by a plaintiff of discriminatory impact of an ADM system largely fall into three prongs:

- 1) Analyzing inputs and ensuring no protected characteristic is being used indirectly;
- 2) Demonstrating creatorship/maintenance responsibility belonging to a third-party;
- 3) Auditing of the system by a third-party.

⁶⁵ 42 U.S. Code § 3604. *Legal Information Institute*. Cornell Law School, <https://www.law.cornell.edu/uscode/text/42/3604> (Accessed February 6, 2023).

⁶⁶ Implementation of the Fair Housing Act's Discriminatory Effects Standard, 78 Fed. Reg. 11459 (February 15, 2013) (codified at 24 CFR 100).

⁶⁷ "HUD's Implementation of the Fair Housing Act's Disparate Impact Standard, 84 Fed. Reg. 42854 (proposed Aug. 19, 2019)."

In 2020, HUD adopted a final rule based on the 2019 proposed rule, which critics noted “risks erecting very high barriers to future FHA plaintiffs in light of the proprietary nature of the algorithms they will be challenging.”⁶⁸ The rule would have required plaintiffs to “sufficiently plead facts to support” a highly specific set of assertions, including that “that there is a robust causal link between the challenged policy or practice and the adverse effect on members of a protected class.” In order to argue this point, plaintiffs would require in-depth and complex knowledge of the decisionmaking process—and in an algorithmic context, specific details of the algorithmic systems in questions. These barriers could be so high as to prevent legitimate suits from being capable of being brought.

In September 2020, the Massachusetts Fair Housing Center (MFHC) and Housing Works, Inc. filed a complaint against HUD challenging the rule. In October 2020, a federal judge issued a preliminary injunction against it, noting that doing so was an extraordinary measure. The judge specifically noted that even should the rule go into effect and be repealed, the rule posed a “real and substantial threat” of harm and those harms would be “not be recoverable” given the rule’s introduction of “new, onerous pleading requirements on plaintiffs.”⁶⁹ The judge noted the rule’s “changes constitute a massive overhaul of HUD’s disparate impact standards, to the benefit of putative defendants and to the detriment of putative plaintiffs (and, by extension, fair housing organizations, such as MFHC)”.⁷⁰ In January 2021, President Biden issued a memorandum directing HUD to reconsider the rule on the basis of an examination of the potential effects including unjustified discriminatory effects of the rule.⁷¹ HUD has since rescinded the 2020 rule and restored the original 2013 “discriminatory effects” rule given that it “more effectively implements the Act’s broad remedial purpose of eliminating unnecessary discriminatory practices from the housing market”.⁷² The 2020 rule was enjoined prior to going into effect so there was no material impact in its rescission, thereby retaining the ‘disparate impact analysis’ standard previously in place which remains today.

⁶⁸ Foggo, V., and J. Villasenor. “Algorithms, Housing Discrimination, and the New Disparate Impact Rule”. *Science and Technology Law Review*, vol. 22, no. 1, Feb. 2021, pp. 1-62, doi:10.7916/stlr.v22i1.7963.

⁶⁹ *Massachusetts Fair Housing Center v. United States Department of Housing and Urban Development* (U.S. District Court for the District of Massachusetts). 3:20-cv-11765 (2020). Available at: <https://clearinghouse.net/doc/110686/>

⁷⁰ *Massachusetts Fair Housing Center v. United States Department of Housing and Urban Development* (U.S. District Court for the District of Massachusetts). 3:20-cv-11765 (2020). Available at: <https://clearinghouse.net/doc/110686/>

⁷¹ *Memorandum on redressing our nation's and the federal government's history of discriminatory housing practices and policies* (2021) *The White House*. The United States Government. Available at: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/26/memorandum-on-redressing-our-nations-and-the-federal-governments-history-of-discriminatory-housing-practices-and-policies/> (Accessed: February 6, 2023).

⁷² “HUD Restores 'Discriminatory Effects' Rule.” *HUD.gov / U.S. Department of Housing and Urban Development (HUD)*, 17 Mar. 2023, https://www.hud.gov/press/press_releases_media_advisories/hud_no_23_054.

On January 9, 2023, HUD and the Department of Justice filed a Statement of Interest in the aforementioned case interpreting the FHA. In particular, the Statement argues that:

- FHA covers algorithm-based tenant screening indirectly by focusing on the outcomes, not the specific processes (algorithm- or human-based) ;
- The standard used for adjudicating FHA algorithm cases is the traditional disparate impact standard; and
- FHA applies directly to “companies providing residential screening services” (including background check providers), not just the landlords.

Analysis

As demonstrated by these recent changes, HUD is the center of a significant amount of regulatory volatility. The wide range of recent rules proposed, enjoined, and subsequently overwritten demonstrates a willingness within the agency to identify methods for which algorithmic decisionmaking is clarified separately from past approaches to housing discrimination. Overall, the recent debate over the HUD rules is exemplified by who bears more of the burden in dis/proving potential disparate impact: tenants or landlords.

Implications of the 2013 Rule

The 2013 rules provide, as the judge who issued the preliminary injunction stated, “a relatively straight-forward burden shifting framework”.⁷³ These rules are the ones currently in effect. The current rules have reverted to a more cautious approach similar to that of the CFPB. The standards imposed on ADM systems follow by analogy to historic standards and focus far more on the disparate outcomes of organizations’ and processes’ decisions rather than the specific methods used to make those decisions.

The use of the 2013 rules maintains the status quo largely around allowing disparate impact to be identified and remediated. That said, such rules may slow the development of such ADM systems in housing contexts.

Implications of Rescinded 2020 Rule

The final 2020 rule, however, significantly shifted the burden of proof from landlords while significantly increasing the scope of their potential defenses. This shifting of burden is also a shifting of power to landlords from tenants.

⁷³ Massachusetts Fair Housing Center v. United States Department of Housing and Urban Development (U.S. District Court for the District of Massachusetts). 3:20-cv-11765 (2020). Available at: <https://clearinghouse.net/doc/110686/>

This shift of power may impair the ability to address disparate impact in housing based on protected characteristics.⁷⁴ Consider a fair housing non-profit (such as MFHC, the plaintiff in the HUD case) or an individual. To challenge a policy under the 2020 rule, the tenant or tenants' rights organization will have to prove a causal link between a given ADM system and its outcome, which would require sophisticated technical knowledge. Additionally, the tenant would require internal system information which could well be considered a trade secret.

Even if a tenant were able to meet this burden of proof, the defenses outlined above in the 2020 rules provide a lower barrier for defendants to defeat such a claim. From the perspective of a defendant—a real-estate broker, landlord, or a housing authority, even given this burden, the defendant may fully defeat a claim using merely one of the defenses outlined above. It is not difficult to imagine that an off-the-shelf ADM model developed by a technology company may be licensed by such a broker, landlord, or housing authority. If so, then they can avail themselves of the second defense—that a third-party is in fact the creator or maintainer of the ADM system. This scenario is increasingly plausible, and under the 2020 rule would have effectively insulated the defendant from a challenge had they gone into effect.

Practically, the effect of the higher barrier of proof on the plaintiff and lower barriers to defeat a claim would have significantly reduced the pressure on defendants like landlords and any ADM developers, while potentially making FHA's ability to prevent or remediate housing discrimination prohibitive. This reasoning was behind the judge's injunction.⁷⁵

Adoption of the 2020 rules without also specifying audit rights could have resulted in *de facto* immunity of developers of such ADM systems because without auditing mechanisms, the threshold for building a case against the developer or maintainer would have been difficult to prove. This example is informative with respect to the value of audit rights when considering ADM systems, given without such rights, the systems may effectively be black boxes to end users.

Implications of Current Rule based on Reinstated 2013 Rule

Beyond the specific measures, based on the position taken by HUD in the 2023 Statement of Interest, the FHA is likely to be applied to all service providers for landlords, not just the landlords themselves. This is an expansion on the 2013 Rule. As noted, this Statement of Interest provides clarification that, "the FHA's text and case law support the FHA's application to companies

⁷⁴ Foggo, V., and J. Villasenor. "Algorithms, Housing Discrimination, and the New Disparate Impact Rule". *Science and Technology Law Review*, vol. 22, no. 1, Feb. 2021, pp. 1-62, doi:10.7916/stlr.v22i1.7963.

⁷⁵ *Massachusetts Fair Housing Center v. United States Department of Housing and Urban Development* (U.S. District Court for the District of Massachusetts). 3:20-cv-11765 (2020). Available at: <https://clearinghouse.net/doc/110686/>

providing residential screening services.”⁷⁶ This change is actually in line with the 2020 Rule, in the sense that the creator/maintainer of a suspect model that offends the policy cannot simply defeat the claim as the user. The difference of course between the approaches is that the user of such a service remains on the hook. Yet despite its wide variation in approach, HUD’s current baseline standard still largely does not distinguish between ADMs and traditional systems.

HUD focuses primarily on discrimination as well. Housing is a means to economic opportunity and one’s autonomy is significantly affected by one’s ability to gain housing. However, the FHA deliberately outlines discrimination as the key factor of interest in the original legislation, and through the protected characteristics, clearly targets profiling in this manner. Overall, while there is little information about the impact of these recent regulatory requirements and/or prohibitions on private actors since none have gone into effect, HUD overall appears to require close monitoring given the potential for new ideas to be generated and elicit response. Given HUD’s intention to treat algorithmic systems with a much lighter touch and higher burden of proof, it is useful to recognize that while this tradeoff may be a function of politicization, the precedent for other regulatory regimes even in a regulatory agency ostensibly concerned with only disparate impact outputs, in response may significantly swing the regulatory conversation towards lower liability on real estate brokers, landlords, and housing authorities.

5.1.3 Federal Synthesis

Of the four specific agencies we considered, each has taken a different approach based on the history, mandate, and position of the agency. The FTC has a historically broad mandate based on its overall Section 5 authority specifically surrounding unfair and deceptive trade practices across industry. As such, it has the broadest guidance and outlines transferable principles that can be broadly applied across ADM systems. In contrast, the CFPB—despite being an umbrella organization for many forms of financial regulation—is one of multiple organizations within the federal government to enforce consumer financial regulation and accountability; they are not comprehensively in charge of enforcement of such regulations. In addition, the CFPB’s regulation is focused primarily on a subset of businesses: those that offer consumer credit. As such, their approach is largely one of telegraphing standards to the organization and other regulators. In particular, they do not distinguish between the differences between non-ADM and ADM systems given their focus on the disparate impact of the system itself. This approach establishes a baseline and one that is technologically agnostic. It is the most conservative approach, but in doing so, the one that is most flexible and creates the least uncertainty to industry writ large.

⁷⁶ “Justice Department Files Statement of Interest in Fair Housing Act Case Alleging Unlawful Algorithm-Based Tenant Screening Practices.” *The United States Department of Justice*, 10 Jan. 2023, <https://www.justice.gov/opa/pr/justice-department-files-statement-interest-fair-housing-act-case-alleging-unlawful-algorithm>.

This conservative approach is also largely practiced by HUD. Despite its wide variation in approach, HUD's current baseline standard still largely does not distinguish between ADMs and traditional systems. Given the volatility of its proposed rules in the past few years, likely as a result of politicization of the agency, it may be a useful barometer of the range of approaches but not a source of emulation for stable regulations.

Lastly, the EEOC is subject to the same vertical regulatory constraints as agencies like the CFPB and HUD—in that its jurisdiction applies only in a specific context and on specific actors (employers). However, its approach does show novelty around its rules around reasonable accommodation. While reasonable accommodation is required across many contexts by the EEOC, its application to ADM systems may have broader effects due to the necessity of ADM systems to potentially require significant changes to define and adopt alternative inputs. Unlike other jurisdictions, the EEOC does not restrain itself to merely examine outputs or bar certain inputs. Through its reasonable accommodation provision, it in effect requires certain characteristics to be taken into consideration (either directly or through a meaningful substitute) requiring technological changes to complex systems and without clearly specifying in advance what inputs are considered reasonable. This approach does present a new burden onto ADM system creators, but exercises a positive force on ensuring systems consider certain factors rather than merely a negative one against certain factors. While this approach has yet to be implemented and its consequences understood, it demonstrates a new avenue for ensuring fairness and accountability in ADM systems.

5.2 California State Regulations

The state of California has long spearheaded efforts to regulate online behavior to protect Californians from digital harms. However, there is presently a limited set of laws and regulations in the state that define and regulate the use of ADM systems.

Based on an analysis of existing laws and regulations, as well as pending rulemaking processes, we found that as of the beginning of 2023, California law refers to the use of ADM systems in only two contexts. The first is employment and housing through draft regulations imposed by the California Civil Rights Council. The second is child safety as specified in the California Age-Appropriate Design Code Act.

5.2.1 Fair Employment & Housing

California's Civil Rights Council⁷⁷ (CCRC) introduced an amendment to its regulations in March 2022 that addresses the use of automated systems as part of employment and hiring practices. The goal of this amendment is to ensure that the use of such systems does not result in intentional or unintentional violations of fair employment practices.⁷⁸ For example, the regulation aims to ensure that a resume screening system would not screen candidates based on a protected characteristic, since that could result in illegal employment discrimination.

The definition of ADM adopted by the CCRC is a specific one,⁷⁹ where the general definition is followed by examples that assist in discerning what type of algorithms are regulated by the rules. These include, but are not limited to: (1) algorithms that screen resumes for particular terms or patterns; (2) algorithms that employ face and/or voice recognition to analyze facial expressions, word choices, and voices; (3) algorithms that employ gamified testing that include questions, puzzles, or other challenges used to make predictive assessments about an employee or applicant, or to measure characteristics including but not limited to dexterity, reaction-time, or other physical or mental abilities or characteristics; (4) algorithms that employ online tests meant to measure personality traits, aptitudes, cognitive abilities, and/or cultural fit.⁸⁰

Adopting a regulatory scheme that focuses on system outcomes, the new rules regulate ADM by explicitly disallowing wrongful discrimination through its use. In order to ensure compliance, the regulation states that employers or agents that use such systems must provide notice to employees and applicants, provide an explanation of the system's decision-making processes, and keep records of the system's inputs and outputs.⁸¹ The rules do not elaborate on the specific records that should be kept.

Analysis

The CCRC's approach to defining ADM is one where the regulator offers a general definition which lacks detailed classification criteria, and provides specific examples of such systems to ensure specific uses are in scope, while clarifying that these examples are non-exhaustive.

⁷⁷ Fair Employment & Housing Council Draft Modifications to Employment Regulations Regarding Automated-Decision Systems Available at: <https://calcivilrights.ca.gov/wp-content/uploads/sites/32/2022/07/Attachment-G-Proposed-Modifications-to-Employment-Regulations-Regarding-Automated-Decision-Systems.pdf> (Accessed: February 6, 2023)

⁷⁸ Ibid.

⁷⁹ "A computational process, including one derived from machine-learning, statistics, or other data processing or artificial intelligence techniques, that screens, evaluates, categorizes, recommends, or otherwise makes a decision or facilitates human decision making that impacts employees or applicants" - Draft Modifications to Employment Regulations Regarding Automated-Decision Systems, Article 1 Section 11008 (d).

⁸⁰ Draft Modifications to Employment Regulations Regarding Automated-Decision Systems, Article 1 Section 11008 (d).

⁸¹ Ibid, Article 1 Section 11013.

The lack of classification criteria in these rules, and the uncertainty it can create, is limited when used by a sector-specific regulator such as the CCRC, but expanded when used by a cross-sector regulator. For the former, keeping up with new innovations that might affect the sector is easier to do since regulators must only track innovations that relate to the sector, rather than any and all ADM innovations. Thus, a sector-specific regulator would likely be more successful in providing guidance on new and upcoming innovations in a timely and effective manner. In contrast, a regulator with a broader mandate might struggle to track new innovations and maintain an effective list of uses needed to provide the clarity and certainty needed for both industry and government.

As for the requirements and prohibitions introduced by the CCRC, they are applied consistently to all in-scope ADM uses. CCRC does not expand requirements based on harm potential, and therefore it does not offer guidance on defining uses which create elevated harm. Rather, it seems the CCRC assumes that in the context of employment, any use of ADM systems poses a significant enough risk to justify regulation.

The CCRC's requirements focus on demystifying the operations of ADM systems, including data subject rights such as right to be informed and right of access. First, various sections, including §11017.1(d), ensure that individuals are notified when decisions regarding their employment are made using such systems. Second, §11013(c) requires employers to document the operation of the systems, ensuring they can offer explainability as to how decisions were made by these systems. Using this added transparency, the rules offer an avenue of accountability for illegal discrimination by allowing regulators or individuals to take legal action against employers and ensuring the information they need to prove discrimination exists.

The CCRC's rules do not offer employees or applicants opt-out rights or otherwise limit data collection. For example, not only does the law not prohibit collection of racial data on employees, it requires companies to collect this data⁸². However, employers will be penalized if such information is used as a factor in a decision made by an ADM system. We believe that this approach is appropriate for the employment context, since employers hold vast information on their employees for a wide range of legitimate reasons, including for tracking diversity and inclusion efforts.

In conclusion, the CCRC's approach to defining ADM is typical of many jurisdictions and rules, providing a broad definition with specific examples to ensure certain uses are in scope. While this approach offers regulators flexibility in applying the law to future systems, it creates uncertainty for businesses and may complicate regulatory classification, and is thus problematic when creating sector-agnostic regulations. The Council's rules focus on demystifying ADM system operations

⁸² The requirement is intended to allow oversight on outcomes of employment decisions and to identify statistical discrepancies that can be used to identify discrimination.

by requiring transparency and accountability, but lack emphasis on regulating the input fed into ADM systems. This approach may be effective in relation to the employment context, but to regulate other types of ADM systems, limiting the collection of user information would be essential for safeguarding users' privacy.

5.2.2 California Age-Appropriate Design Code Act

In August of 2022, the California Legislature passed AB2273, the California Age-Appropriate Design Code Act (Cal-AADC), which will require businesses that provide online services, products, or features likely to be accessed by children under the age of eighteen to comply with specific requirements, including default settings that provide a high level of privacy.⁸³ The Act will take effect on July 1, 2024.

The bill includes a discussion of profiling and specifies that businesses “should offer strong privacy protections by design and by default, including by disabling features that profile children using their previous behavior, browsing history, or assumptions of their similarity to other children, to offer detrimental material.” Profiling is defined as: “any form of automated processing of personal information that uses personal information to evaluate certain aspects relating to a natural person, including analyzing or predicting aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.”⁸⁴

The bill also prohibits businesses from profiling a child by default unless two specific criteria are met: “(i) Profiling is necessary to provide the online service, product, or feature requested and only with respect to the aspects of the online service, product, or feature with which the child is actively and knowingly engaged. (ii) The business can demonstrate a compelling reason that profiling is in the best interests of children.”⁸⁵ It is not clear how this section of the bill might be enforced, and how businesses will be able to “demonstrate” or prove that profiling as defined by the bill is “necessary” to provide the services, products, or features.

Analysis

In the Cal-AADC, ADM is not defined while profiling is defined in line with definitions introduced by other U.S. states, including Colorado.⁸⁶ As was the case with the California Civil Rights Council's rules, the legislation includes examples of harmful profiling, all of which focus on targeted advertising and personalized recommendations. These examples serve to clarify the types

⁸³ “California Age Appropriate Design Code Act.” *Bill Resource*, 2022, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202120220AB2273.

⁸⁴ Ibid, 1798.99.30(b).

⁸⁵ Ibid, 1798.99.31.

⁸⁶ See next chapter

of practices this act regulates. The law does not describe which types of profiling, if any, pose an elevated risk of harm to children, or if they all inherently pose a risk.

In the case of the AADC, we assess this approach was effective in achieving legislators' goals since they had the narrow intention of dealing with the two specific above-mentioned types of profiling.⁸⁷ However, once again, this approach poses a challenge for rulemaking intended to govern a broader and continuously expanding list of practices, since the lack of specific classification criteria would not allow businesses and regulators to easily identify new innovations that fall under the rules and pose elevated risks.

Regarding the requirements and prohibitions presented in the act, it is important to mention that when regulating business practices relating to children, the consensus around child safety and its overwhelming social importance gives regulators unique freedom to act with less regard to business implications.⁸⁸ Examining the Cal-AADC suggests legislators acted on this freedom, adopting a regulatory framework that departs from extant regulation regarding adults.

Most importantly, the Act explicitly disables businesses' ability to profile children based on some types of data, such as previous browsing history and assumptions or inferences, regardless of consent. When using allowed data, the Act prohibits any profiling of children that does not meet this set criteria, even as an opt-in mechanism, and disallows practices such as personalized recommendations. This approach is aimed to broadly ensure the privacy of children. However, while opt-in approaches for data collection from children have been adopted in some jurisdictions, including in Article 8 of the GDPR,⁸⁹ they have not yet been implemented in rules pertaining to adults.

Businesses raise concerns that these rules would lead to extensive revenue losses for companies who rely on targeted-advertising, and would disable their ability to provide their users with personalized services.⁹⁰ However, since such an approach has not been implemented before, it is difficult to assess the validity of these concerns. Applying Cal-AADC's rules to the profiling of adults would expand consumers' privacy rights, but regulators would need to prepare for attacks

⁸⁷ Robertson, A. (2022) "California passes sweeping online safety rules for kids", *The Verge*. <https://www.theverge.com/2022/8/30/23326822/california-ab-2273-passes-senate-children-social-media-bill-gavin-newsom> [last accessed: 03.10.23].

⁸⁸ Macenaite, M. (2017). From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New Media & Society*, 19(5), 765–779. <https://doi.org/10.1177/1461444816686327>

⁸⁹ EU General Data Protection Regulation, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680>.

⁹⁰ See, for example, public comments submitted as part of CPPA's rulemaking process by the Computer and Communications Industry Association (https://cppa.ca.gov/regulations/pdf/comments_1_25.pdf#page=101) and the California Retailers association (https://cppa.ca.gov/regulations/pdf/comments_1_25.pdf#page=228).

by businesses, who will argue the rules do not strike the right balance between user safety, business needs and innovation.

Overall, the Cal-AADC is intended to promote a narrow set of goals (children’s information privacy and wellbeing online) that, due to their significant social importance and the vulnerability of minors, justifies an expanded regulatory toolkit. The Act’s complete ban on certain types of data profiling is effective in protecting children, but it may be seen by business advocates as an overreach when governing the use of profiling for adults. Additionally, the lack of specific classification criteria for profiling may limit the ability to govern a broader and continuously expanding list of practices based on this Act’s definition of profiling.

5.2.2.1 Summary

Examining the two rules enacted or proposed in the state of California, we find that both, each for their own reason, offer a definition of ADM or profiling, but lack specific criteria for identifying practices that pose an elevated risk of harm. The requirements and prohibitions introduced by the California Civil Rights Council emphasize ADM explainability and employer accountability, but lack rules on data collection and privacy protection. In contrast, the California Age-Appropriate Design Code Act offers a comprehensive approach of regulating all aspects of an ADM system, but the Act’s focus on child safety led to the adoption of prohibitions that might be challenged by industry leaders if applied to adult consumers.

5.3 Other U.S. States

5.3.1 Introduction

Aside from California, four states have enacted legislation focused on privacy and/or data protection since 2021:

- **Colorado** — Colorado Privacy Act (2021).
- **Connecticut** — Connecticut Data Privacy Act (2022).
- **Utah** — Utah Consumer Privacy Act (2022).
- **Virginia** — Virginia Consumer Data Protection Act (2021).

In this section, we will refer to these statutes as the “state privacy statutes”. The state privacy statutes share some substantive similarities with each other. In particular:

- Each statute confers on consumers the right to access their own personal data, to receive a portable copy of their data, and to request for it to be deleted from the data controller’s

possession.⁹¹ Colorado, Virginia, and Connecticut additionally confer the right to correct inaccuracies in their personal data.⁹²

- Each statute confers the right to opt out of targeted advertising and the sale of personal data.⁹³ Colorado, Virginia, and Connecticut additionally confer the right to opt out of profiling when that profiling has legal or similarly significant effects.⁹⁴
- Colorado, Virginia, and Connecticut require data impact assessments with regard to processing of personal data that has a “heightened risk of harm to a consumer.”⁹⁵ Colorado and Connecticut offer definitions of a “heightened risk of harm.”⁹⁶
- Each state privacy statute reserves enforcement to the state attorney general and/or district attorneys. No state has established a private right of action for violations of its privacy statute.⁹⁷
- Each statute applies only to businesses that have met certain thresholds (e.g., number of customers) for use of personal information in the applicable state.⁹⁸

5.3.2 Rulemaking and enforcement

The Utah, Virginia, and Connecticut statutes do not confer authority on any state agency for rulemaking to implement a state privacy statute. However, the Colorado Privacy Act provides that the Colorado Attorney General “may promulgate rules for the purpose of carrying out [the Colorado Privacy Act]”.⁹⁹ Colorado is the only state which has conferred rulemaking authority on a state agency for the enforcement of a state privacy statute, as of the time of writing (March 2023), Colorado is actively engaged in the rulemaking process. Accordingly, Colorado is the only U.S. state we will review in detail here.

⁹¹ Colo. Rev. Stat. §§ 6-1-1306(1)(b), (1)(d), (1)(e). Connecticut Public Act 22-15, §§ 4(a)(1), 4(a)(3), 4(a)(4). Utah Code §§ 13-61-201(1), 13-61-201(2), 13-61-201(3). Code of Virginia §§ 59.1-577(1), 59.1-577(2), 59.1-577(4).

⁹² Colo. Rev. Stat. § 6-1-1306(c). Connecticut Public Act 22-15, § 4(a)(2). Code of Virginia § 59.1-577(2).

⁹³ Colo. Rev. Stat. §§ 6-1-1306(1)(a)(A), 6-1-1306(1)(a)(B). Connecticut Public Act 22-15, §§ 4(a)(5)(A), 4(a)(5)(B). Utah Code § 13-61-201(4). Code of Virginia §§ 59.1-577(5)(i), 59.1-577(5)(ii).

⁹⁴ Colo. Rev. Stat. § 6-1-1306(1)(a)(C). Connecticut Public Act 22-15, § 4(a)(5)(C). Code of Virginia §§ 59.1-577(5)(iii).

⁹⁵ Colo. Rev. Stat. § 6-1-1309(1). Connecticut Public Act 22-15, § 8(a). Code of Virginia § 59.1-580(A).

⁹⁶ Colo. Rev. Stat. § 6-1-1309(2). Connecticut Public Act 22-15, § 8(a). Note that while Virginia lacks a specific definition of “heightened risk of harm”, Virginia’s data protection assessment requirement specifically applies to substantially the same processing activities as are covered in Colorado and Connecticut’s respective definitions. *See* Code of Virginia § 59.1-580(A)(1)-(A)(4).

⁹⁷ Colo. Rev. Stat. § 6-1-1311(1)(a). Connecticut Public Act 22-15, § 11(a). Utah Code § 13-61-402. Code of Virginia § 59.1-584.

⁹⁸ Colo. Rev. Stat. § 6-1-1304(1). Connecticut Public Act 22-15, § 2. Utah Code § 13-61-102(1). Code of Virginia §§ 59.1-576(A).

⁹⁹ Colo. Rev. Stat. § 6-1-1313(1).

5.3.3 Colorado

Consistent with its statutory mandate, the Colorado Department of Law (CDL) initiated rulemaking proceedings following the 2021 passage of the Colorado Privacy Act. On March 15, 2023, the CDL adopted its 44-page draft rules and filed them with the Colorado Secretary of State.¹⁰⁰ In this section, we refer to these rules as the “March 2023 adopted rules”.

While the rules have been adopted by the CDL, the rules have not yet been published by the Colorado Secretary of State, and the state has not published the administrative record underlying the rules. We present our analysis subject to those constraints.

Although the March 2023 adopted rules include requirements for data protection assessments, those requirements are not directly comparable with the California and federal regulatory and legislative acts discussed above. We therefore discuss Colorado’s data protection assessment regulations in section 8 of this report, “Appendix B: Colorado Data Protection Assessments”, below.

5.3.3.1 Definitions of Automated Processing

Over the course of Colorado’s rulemaking process, the CDL proposed — but did not adopt — a definition of “Automated Processing”. In its September 2022 draft rules, the CDL proposed a definition for “Automated Processing”, a similar but not identical term to “automated decisionmaking”, as follows:

“Automated Processing” as referred to in CRS §6-1-1303(20) means the Processing of Personal Data that is automated through the use of computers, computer programs or software, or other digital technology.”¹⁰¹

This definition was subsequently removed from the proposed rules and was omitted from the March 2023 adopted rules. The March 2023 adopted rules nonetheless included definitions of “Human Involved Automated Processing”, “Human Reviewed Automated Processing”, and “Human Reviewed Automated Processing” — different types of processing that in some cases are subject to different regulatory requirements, as we will discuss in the upcoming section on “Profiling Opt-Out Rights — Human-Involved Processing.”

Analysis

The CDL’s removal of the proposed definition suggests that the CDL viewed its inclusion as unnecessary for the state’s regulatory framework. Colorado’s statute uses the term “automated

¹⁰⁰ Code of Colorado Regulations eDocket. Available at <https://www.coloradosos.gov/CCR/eDocketDetails.do?trackingNum=2022-00603>.

¹⁰¹ Draft Colorado Privacy Act Rules, Colorado Department of Law, September 2022. Available at https://coag.gov/app/uploads/2022/10/CPA_Final-Draft-Rules-9.29.22.pdf.

processing” only in defining “profiling” (which the Colorado statute defines as “any form of **automated processing** of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual’s economic situation, health, personal preferences interests, reliability, behavior, location, or movements” (emphasis added)).¹⁰² In this context, the definition of automated processing is not particularly ambiguous in context — especially considering that the term “processing” is also defined in the Colorado statute.¹⁰³

Nonetheless, the term “automated processing” is nonetheless used in the Colorado statute as well as in the definitions of “Human Involved Automated Processing”, “Human Reviewed Automated Processing”, and “Human Reviewed Automated Processing”. The CDL’s choice not to define “automated processing” leaves ambiguous what level of automation is required for processing to become “automated processing”.

Compared with a restrictive definition of “automated processing”, adopting no definition preserves the CDL’s flexibility and ability to take action in future cases, including where emergent technology could fall outside the scope of a definition of automated processing adopted now. However, the ambiguity may create regulatory uncertainty. The CDL received comments noting that its previous proposed definition of “automated processing” had the potential to include “calculators, spreadsheets, emails, calendar software, etc.”¹⁰⁴ By not adopting any definition, the CDL does not explicitly exclude those forms of processing from the scope of its regulations concerning automated processing, and does not provide clear guidance on whether it will take a narrow or broad view of automated processing.

5.3.3.2 Profiling Opt-Out Rights — Human-Involved Processing

The Colorado Privacy Act confers on consumers the right to opt out of “targeted advertising”, “the sale of personal data”, and “profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.”¹⁰⁵

In its implementing regulations under this section, the CDL applied different requirements to different kinds of profiling. In the March 2023 adopted rules, the CDL distinguished between “Human Involved Automated Processing”, “Human Reviewed Automated Processing”, and “Solely Automated Processing”:

¹⁰² Colo. Rev. Stat. 6-1-1303(20).

¹⁰³ Colo. Rev. Stat. 6-1-1303(18).

¹⁰⁴ Comments of the Denver Metro Chamber of Commerce, submitted to the Colorado Department of Law in Colorado Regulations eDocket Tracking Number 2022-00603; <https://coag.my.salesforce.com/sfc/p/#t00000004XX8/a/t0000001ZNGe/iETKetOAHsUDCukXtM6zex2WhwFXa1F9JRKp0mB.lww>.

¹⁰⁵ Colo. Rev. Stat. 6-1-1306(1)(a).

- **Human Involved Automated Processing** is defined as “automated processing of Personal Data where a human (1) engages in a meaningful consideration of available data used in the Processing or any output of the Processing and (2) has the authority to change or influence the outcome of the Processing”.
- **Human Reviewed Automated Processing** is defined as “the automated processing of Personal Data where a human reviews the automated processing, but the level of human engagement does not rise to the level required for Human Involved Automated Processing”. The regulations also provide that: “Reviewing the output of the automated processing with no meaningful consideration does not rise to the level of Human Involved Automated Processing.”
- **Solely Automated Processing** is defined as “the automated processing of Personal Data with no human review, oversight, involvement, or intervention”.¹⁰⁶

In particular, the CDL created an exception to the opt-out right for profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer if the profiling is based on “Human Involved Automated Processing”, as long as the consumer receives seven specified categories of information about the profiling decision (as we will discuss in the “Notice Rights” section below).¹⁰⁷

Analysis

This approach is similar to the European Union’s requirements under the GDPR, which in Article 22 provides that data subjects have a “right not to be subject to a decision **based solely on automated processing**, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her” (emphasis added).¹⁰⁸ The GDPR’s Article 22 rights apply to all automated processing, not just profiling. However, the Colorado opt-out right may be broader than the GDPR’s Article 22 right in two ways:

- Article 22 of the GDPR applies only to decisions “based *solely* on automated processing”.¹⁰⁹ Under the March 2023 adopted rules, the Colorado opt-out right applies

¹⁰⁶ March 2023 adopted rules; Rule 2.02.

¹⁰⁷ March 2023 adopted rules; Rule 9.04(C).

¹⁰⁸ Article 22 GDPR. See: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680>

¹⁰⁹ However, the GDPR does not further define the exact scope of “based solely on automated processing”. The EU’s Article 29 Data Protection Working Party, which was an official advisory body, issued guidance on interpreting the term “based solely on automated processing”. In its October 2017 guidance, the Working Party advised that a decision is not “based solely on automated processing” if a human “reviews and takes account of other factors in making the final decision”. However, human oversight cannot be a “token gesture”; it must be “carried out by someone who has the authority and competence to change the decision”, who must “consider all the available input and output data”. See <https://ec.europa.eu/newsroom/article29/items/612053> - “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)”. Accordingly, there are some interpretations of the phrase which would not be considerably narrower than the combination of “Solely Automated Processing” and “Human Reviewed Automated Processing” as defined in Colorado.

both to “Solely Automated Processing” and to “Human Reviewed Automated Processing”, with only “Human *Involved* Automated Processing” exempted from the right.

- While the March 2023 adopted rules exempt “Human Involved Automated Processing” from the scope of the opt-out right, the Colorado rules still impose significant disclosure requirements on the data controller.

Colorado’s March 2023 adopted rules present significant ambiguity. The terms “meaningful consideration” and “change or influence” are not further defined by the Colorado regulations and, in addition to creating uncertainty about the scope of the opt-out exception, may not ensure that the exemption covers only cases in which a human exercises sufficient independent judgment to warrant immunity from the exercise of an opt-out right. Because automated decisionmaking systems scale much more economically than the work of human reviewers, companies face incentives to minimize the amount of consideration that human reviewers take on.¹¹⁰ And as the complexity of automated decisionmaking systems advances further beyond the understanding of even the engineers who designed them, such as in the case of machine learning systems, it may grow increasingly difficult for human reviewers to exercise substantive review of those systems.¹¹¹ The incentives for businesses to avoid consumer opt-outs appear to reward companies that maintain a form of human-involved processing, but it is unclear under what circumstances companies can maintain such systems.¹¹²

Finally, unlike the European Union, Colorado’s March 2023 adopted rules do not present a legally binding method for resolving these ambiguities.

5.3.3.3 Notice and Opt-Out Rights

The March 2023 adopted rules impose requirements for businesses to make disclosures when engaged in “Profiling in furtherance of Decisions that Produce Legal or Other Similarly Significant Effects Concerning a Consumer” in three different circumstances, in Rule 9.03(A), Rule 9.04(C), and Rule 9.05(C).

Rule 9.03(A) requires the disclosure of seven categories of information whenever a company engages in “Profiling in furtherance of Decisions that Produce Legal or Other Similarly Significant Effects Concerning a Consumer”.

¹¹⁰ Austin Clyde. “Human-in-the-Loop Systems Are No Panacea for AI Accountability.” Tech Policy Press, 1 Dec. 2021, <https://techpolicy.press/human-in-the-loop-systems-are-no-panacea-for-ai-accountability/>.

¹¹¹ Knight, Will. “The Dark Secret at the Heart of Ai.” MIT Technology Review, MIT Technology Review, 2 Apr. 2020, <https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/>.

¹¹² See also the comments of Consumer Reports in Colorado’s rulemaking process, available at https://coag.my.salesforce.com/sfc/p/#t00000004XX8/a/t0000001SOYM/EO7ZGzcIJdJgVmX0sNyBI_6NeC1hrnkUUzD85y.3xFl.

Rule 9.04 addresses the opt-out exception for Human Involved Automated Processing discussed above. Rule 9.04(C) requires the disclosure of seven categories of information when a company declines to honor an opt-out request pursuant to that exception.

Rule 9.05 addresses two circumstances under which a controller may request consent to engage in profiling: (1) when a consumer has previously opted out of profiling with legal or similarly significant effects and the controller seeks consent to once again engage in that profiling, and (2) when a controller seeks consent to engage in profiling with legal or similarly significant effects because that profiling is “is not reasonably necessary to or compatible with the original specified purposes for which the Personal Data was Processed”. Rule 9.05(C) requires the disclosure of seven categories of information when requesting such consent.

We compare the contents of the disclosure requirements below. In the following table, the list of disclosure requirements under each rule is provided in one column. Requirements that appear in the same row are similar to one another.

Rule 9.03(A) (General Notice Rights)	Rule 9.04(C) (Exception for Human Involved Processing Opt Out Right)	Rule 9.05(C) (Requests for Consent)
1. What decision(s) is (are) subject to Profiling	1. The decision subject to the Profiling	1. The decision subject to the Profiling
2. The categories of Personal Data that were or will be Processed as part of the Profiling in Furtherance of Decisions that Produce Legal or Other Similarly Significant Effects	2. The categories of Personal Data that were or will be used as part of the Profiling used in Furtherance of Decisions that Produce Legal or Other Similarly Significant Effects;	2. The categories of Personal Data used in the Profiling
3. A non-technical, plain language explanation of the logic used in the Profiling process;	3. A non-technical, plain language explanation of the logic used in the Profiling process	3. A non-technical, plain language explanation of the logic used in the Profiling, or a link to such information if it is included in the Controller’s privacy notice
4. A non-technical, plain language explanation of how Profiling is used in the decisionmaking process, including the role of human involvement, if any	4. A non-technical, plain language explanation of the role of meaningful human involvement in Profiling and the decision-making process	4. How Profiling is used in the decision-making process, including the role of human involvement, if any
5. If the system has been	N/A	N/A

Rule 9.03(A) (General Notice Rights)	Rule 9.04(C) (Exception for Human Involved Processing Opt Out Right)	Rule 9.05(C) (Requests for Consent)
evaluated for accuracy, fairness, or bias, including the impact of the use of Sensitive Data, and the outcome of any such evaluation		
N/A	5. How Profiling is used in the decision-making process	N/A
N/A	N/A	5. Why the Profiling is relevant to the decision-making process
6. The benefits and potential consequences of the decision based on the Profiling	6. The benefits and potential consequences of the decision based on the Profiling	6. Potential benefits and consequences of the decision based on the Profiling
7. Information about how a Consumer may exercise the right to opt out of the Processing of Personal Data concerning the Consumer for Profiling in Furtherance of Decisions that Produce Legal or Other Similarly Significant Effects	7. An explanation of how Consumers can correct or delete the Personal Data used in the Profiling used in the decision-making process	7. Any applicable links to where Consumers can find any additional information about the Profiling and decision-making process and their associated rights

Analysis

The disclosures required under the three rules are broadly similar. The most substantial difference appears in item 5 of each rule:

- Rule 9.03(A)(5) requires disclosure of: “If the system has been evaluated for accuracy, fairness, or bias, including the impact of the use of Sensitive Data, and the outcome of any such evaluation”.
- Rule 9.04(C)(5) requires disclosure of: “How Profiling is used in the decision-making process”.
- Rule 9.05(C)(5) requires disclosure of: “Why the Profiling is relevant to the decision-making process”.

We did not identify a clear reason for the differences between the requirements in item 5 of each rule.

Item 4 of each of the three rules requires disclosure of a “non-technical, plain language explanation of the logic used in the Profiling”. This requirement lacks detail on what the “explanation of the logic” must include. Without such detail, it is unclear how specific and precise this disclosure must be. For example, this requirement does not distinguish between a high-level description of the purposes underlying a profiling system and a comprehensive explanation of which factors contributed to the outcome and in what ways.

Additionally, this requirement does not specifically address circumstances under which even the data controller does not have an understanding of the “logic used in the Profiling”. Profiling systems increasingly take the form of “black box” systems that are opaque even to their creators.¹¹³ This “explainability” challenge characterizes many of the most significant recent advancements in artificial intelligence.¹¹⁴

Demands for ADM explainability are not unique to Colorado; the GDPR¹¹⁵ as well as the U.S. federal agencies we discussed earlier place explainability demands on ADM systems to explain outcomes. However, demands for explainability of machine learning systems in particular may be on a collision course with the present capabilities of the technology.

As currently worded, this requirement may push data controllers for machine learning based systems in particular to one of two extremes: (1) intentionally read the requirement very narrowly, to require such an insubstantial disclosure as to not provide value to a consumer, or (2) discontinue their service for inability to comply with a requirement that is unclear about its substantive provisions, or impossible to comply with given the nature of machine learning. It is an open question whether specifying the data used to train machine learning systems will provide enough insight to help answer the explainability question.

¹¹³ Xiang, Chloe. “Scientists Increasingly Can’t Explain How AI Works.” Vice, June 29, 2020. <https://www.vice.com/en/article/y3pezm/scientists-increasingly-cant-explain-how-ai-works>.

¹¹⁴ Xiang, Chloe. “Black Box AI.” Big Think. Accessed March 24, 2023. <https://bigthink.com/the-future/black-box-ai/>. Knight, Will. “The Dark Secret at the Heart of AI.” MIT Technology Review. April 11, 2017. <https://www.technologyreview.com/2017/04/11/51113/the-dark-secret-at-the-heart-of-ai/>.

¹¹⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, Recital 38.

6. Summary of Findings

Based on our analysis of the regulations governing the use of ADM systems introduced by federal agencies and state agencies, namely in California and Colorado, a variety of commonalities and differences emerge. These commonalities suggest the inception of new, cross-jurisdictional norms in regulating ADM systems, while the differences mark areas where regulators in different jurisdictions have either been unable to agree on approaches, or adopted unique regulatory mechanisms to achieve specific policy objectives.

First, it is clear that all regulations, regardless of jurisdiction, attempt to reduce ambiguity by enumerating and detailing the types of ADM harms that require governmental intervention. However, the rules diverge in their level of specificity, as well as the specification method. Some rules, such as the California Age Appropriate Act, specify in-scope harms by detailing examples of such harms, while others, such as in Colorado, provide a definition which is used to identify harmful uses. In that sense, no one definition of ADM has emerged that is adopted widely by academics, industry, and a wide range of regulators, even though the various definitions are rather similar.

The definitions adopted by each regulator also diverge as a result of the different policy goals pursued. Most non-state privacy regulators that govern the use of ADM systems do so in relation to specific sectors, e.g., employment, or to a specific subset of consumers, e.g., underage consumers. These different focuses result in multiple approaches to defining ADM, as each regulator tailors their definition on the aspects that relate to their policy goal. To date, the FTC is the only federal agency that takes a broad, sector agnostic or all-consumer approach to commercial ADM oversight.

As for the requirements and prohibitions introduced by the regulations we examined, it is clear that all consist of a similar pool of regulatory levers which includes opt-out/in rights, data collection prohibitions, transparency requirements and protections against discrimination. Each regulator deploys these levers differently, in line with its policy goals and legislative mandate. For example, most regulators adopt an opt-out approach to sufficiently provide consumers with the ability to control the ADM systems that use their data. However, the Cal-AADC adopts a broader opt-in mechanism, since it specifically focuses on a consumer category, children, who would not equally benefit from opt-out mechanisms as adults would.

In closing, we note that the ADM regulatory landscape as it exists today is deeply complex, with different (often overlapping) standards and requirements applying to different ADM systems depending on geographic location, sector, and activity. While it is obvious that the European Union exhibits some influence over this landscape, particularly through the GDPR, and may strengthen this influence after it passes the European AI Act, some of the uncertainty within the U.S. is also

due to the multiplicity of approaches to regulating consumer privacy between jurisdictions within the United States. Even setting aside the question of defining ADM, the regulatory landscape for privacy in the U.S. is diverse and lacks agreement regarding both the privacy harms consumers experience as well as the set of regulatory provisions needed to address them. This complexity imposes significant compliance costs and uncertainty on businesses, regulators, and the public. Each regulatory act we examined struck a different set of tradeoffs than the others, as is to be expected in a fractured and emergent regulatory landscape. While we have no reason to conclude that any particular tradeoff was improperly struck, we note that each regulatory act results in large part from the specific circumstances of the authority involved, including factors like the purpose underlying the actor's exercise of regulatory authority and the statutory and other authority available to the regulatory actor. Therefore, while we believe that this landscape analysis can help inform the exercise of regulatory authority in the future, the context in which any future regulatory processes take place must freshly inform the ways in which regulatory authority is exercised.

7. Appendix A: Overview of Regulatory Acts

Legislative or Regulatory Document	Jurisdiction	Underlying statute	Type	Focus	Rule	Definitions
<i>For reference:</i> California Consumer Privacy Act, as amended	California	n/a	Statute (parts enacted by ballot proposition)	Consumer privacy	<p>Authority is conferred upon CPPA to, <i>inter alia</i>:</p> <p>Access and opt out. (1) issue “regulations governing access and opt-out rights with respect to businesses’ use of automated decisionmaking technology, including profiling and requiring businesses’ response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer.”</p> <p>Risk assessments. (2) issue regulations requiring “cybersecurity audit[s]” and “risk assessment[s]” for “businesses whose processing of consumers’ personal information presents significant risk to consumers’ privacy or security”.</p>	<p>Profiling: “Profiling” means any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185, to evaluate certain personal aspects relating to a natural person and 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.</p> <p>Personal information</p>
California Age-Appropriate Design Code Act	California	n/a	Statute	Consumer privacy for children	<p>Companies that “provide[] an online service, product, or feature likely to be accessed by children must, <i>inter alia</i>:</p> <p>(1) complete a data privacy impact assessment;</p> <p>(2) use personal information only for the purposes for which it was collected unless otherwise in “best interests of children”;</p> <p>(3) engage in “profiling” absent “appropriate safeguards” and either (i) profiling is “necessary to provide the online service, product, or feature requested” or (ii) there is a “compelling reason that profiling is in the best interests of children”;</p> <p>(4) refrain from using “dark patterns to lead or</p>	<p>Profiling: “Profiling” means any form of automated processing of personal information that uses personal information to evaluate certain aspects relating to a natural person, including analyzing or predicting aspects concerning a natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.</p>

					encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature to forego privacy protections”.	
California Civil Rights Council (CCRC): Draft Modifications to Employment Regulations Regarding Automated-Decision Systems	California	Fair Employment and Housing Act	Proposed regulation	Discrimination in housing and employment	<p>“It is unlawful for an employer or a covered entity to use [...] automated decision systems [...] that screen out or tend to screen out an applicant or employee or a class of applicants or employees on the basis of a characteristic protected by this Act, unless the [automated decision systems], as used by the covered entity, are shown to be job-related for the position in question and are consistent with business necessity.”</p> <p>“It is unlawful for an employer or a covered entity to use [...] automated-decision systems [...] that screen out or tend to screen out an applicant or employee or a class of applicants or employees on the basis of their [</p> <ul style="list-style-type: none"> • accent • English proficiency • immigration status • holding an “undocumented” driver’s license • Citizenship • Height or weight • National origin and disparate impact by national origin • Sex, sex stereotypes, being of childbearing age • Having done volunteer (as opposed to paid) work • Pregnancy or perceived pregnancy • religion <p>], unless the [automated-decision systems], as used by the covered entity, are shown to be job-related for the position in question and are consistent with business necessity.”</p>	<p>Algorithm: “Algorithm.” A process or set of rules or instructions, typically used by a computer, to make a calculation, solve a problem, or render a decision.</p> <p>Automated-Decision System: “Automated-Decision System.” A computational process, including one derived from machine-learning, statistics, or other data processing or artificial intelligence techniques, that screens, evaluates, categorizes, recommends, or otherwise makes a decision or facilitates human decision making that impacts employees or applicants.</p> <p>An “Automated-Decision System” includes, but is not limited to, the following: (1) Algorithms that screen resumes for particular terms or patterns; (2) Algorithms that employ face and/or voice recognition to analyze facial expressions, word choices, and voices; Attachment B Version: 3/15/2022 (version for public workshop) (3) Algorithms that employ gamified testing that include questions, puzzles, or other challenges used to make predictive assessments about an employee or applicant, or to measure characteristics including but not limited to dexterity, reaction-time, or other physical or mental abilities or characteristics; (4) Algorithms that employ online tests meant to measure personality traits, aptitudes, cognitive abilities, and/or cultural fit.</p>
Federal Trade Commission	Federal	Federal Trade	Staff guidance	Consumer protection	<p>Companies must:</p> <ul style="list-style-type: none"> • Refrain from deception about 	None

(FTC): “Using Artificial Intelligence and Algorithms”		Commission Act	document	; fairness for protected classes	automated tools; <ul style="list-style-type: none"> • “Be transparent when collecting data”; • Explain decisions to consumers • Explain factors affecting risk scores; • Refrain from discrimination (as measured in both inputs and outputs); • Allow consumers “access and an opportunity to correct information”; • Validate algorithms for effectiveness and compliance. 	
Consumer Financial Protection Bureau (CFPB): Circular 2022-03, “Adverse action notification requirements in connection with credit decisions based on complex algorithms”	Federal	Equal Credit Opportunity Act	Policy statement (circular)	Discrimination in financial transactions	“When creditors make credit decisions based on complex algorithms that prevent creditors from accurately identifying the specific reasons for denying credit or taking other adverse actions”, they must “comply with the Equal Credit Opportunity Act’s requirement to provide a statement of specific reasons to applicants against whom adverse action is taken”.	None
Department of Housing and Urban Development (HUD): Statement of	Federal	Fair Housing Act	Litigation statement of interest	Discrimination in housing	The position of the United States is that: <ul style="list-style-type: none"> • A company that provides “tenant screening” services is subject to the Fair Housing Act despite not directly providing housing. • “To establish an FHA disparate impact claim, plaintiffs must show “the occurrence of certain outwardly neutral practices” and “a significantly adverse 	None

interest filed by the Department of Justice					or disproportionate impact on persons of a particular type produced by the defendant’s facially neutral acts or practices.’” This same standard applies to automated decision-making systems.	
Equal Employment Opportunity Commission (EEOC): “The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees”	Federal	Title VII of the Civil Rights Act of 1964 and others	Guidance document	Discrimination in employment	<p>The EEOC describes the following practices as illegal:</p> <ul style="list-style-type: none"> • The employer does not provide a “reasonable accommodation” that is necessary for a job applicant or employee to be rated fairly and accurately by the algorithm. • The employer relies on an algorithmic decision-making tool that intentionally or unintentionally “screens out” an individual with a disability, even though that individual is able to do the job with a reasonable accommodation. “Screen out” occurs when a disability prevents a job applicant or employee from meeting—or lowers their performance on—a selection criterion, and the applicant or employee loses a job opportunity as a result. A disability could have this effect by, for example, reducing the accuracy of the assessment, creating special circumstances that have not been taken into account, or preventing the individual from participating in the assessment altogether. • The employer adopts an algorithmic decision-making tool for use with its job applicants or employees that violates the ADA’s restrictions on disability-related inquiries and medical examinations. (See Question 13 below.) 	<p>Algorithm: Algorithms: Generally, an “algorithm” is a set of instructions that can be followed by a computer to accomplish some end. Human resources software and applications use algorithms to allow employers to process data to evaluate, rate, and make other decisions about job applicants and employees. Software or applications that include algorithmic decision-making tools may be used at various stages of employment, including hiring, performance evaluation, promotion, and termination.</p> <p>Artificial intelligence: Artificial Intelligence (“AI”): Some employers and software vendors use AI when developing algorithms that help employers evaluate, rate, and make other decisions about job applicants and employees. In the National Artificial Intelligence Initiative Act of 2020 at section 5002(3), Congress defined “AI” to mean a “machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments.” In the employment context, using AI has typically meant that the developer relies partly on the computer’s own analysis of data to determine which criteria to use when making employment decisions. AI may include machine learning, computer vision, natural language processing and understanding, intelligent decision support systems, and autonomous systems. For a general discussion of AI, which includes machine learning, see National Institute of Standards and Technology Special Publication 1270, Towards a Standard for Identifying and Managing Bias in Artificial Intelligence.</p>

Utah Consumer Privacy Act	Utah	n/a	Statute	Consumer privacy	<p>Access and deletion right. “(1) A consumer has the right to: (a) confirm whether a controller is processing the consumer's personal data; and (b) access the consumer's personal data. (2) A consumer has the right to delete the consumer's personal data that the consumer provided to the controller.”</p> <p>Format of copy. “(3) A consumer has the right to obtain a copy of the consumer's personal data, that the consumer previously provided to the controller, in a format that: (a) to the extent technically feasible, is portable; (b) to the extent practicable, is readily usable; and (c) allows the consumer to transmit the data to another controller without impediment, where the processing is carried out by automated means.”</p> <p>Opt out right. “(4) A consumer has the right to opt out of the processing of the consumer's personal data for purposes of: (a) targeted advertising; or (b) the sale of personal data.”</p> <p>Enforcement. By the Attorney General.</p>	<p>Targeted advertising: "Targeted advertising" means displaying an advertisement to a consumer where the advertisement is selected based on personal data obtained from the consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests. <i>With exceptions.</i></p>
Colorado Privacy Act	Colorado	n/a	Statute	Consumer privacy	<p>Opt out right. (a) Right to opt out. (I) A consumer has the right to opt out of the processing of personal data concerning the consumer for purposes of: (A) Targeted advertising; (B) The sale of personal data; or (C) Profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.</p> <p>Access. (b) Right of access. A consumer has the right to confirm whether a controller is processing personal data concerning the consumer and to access the consumer's personal data.</p> <p>Correction. (c) Right to correction. A consumer has the right to correct inaccuracies in the</p>	<p>(9) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.</p> <p>(20) "Profiling" means any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.</p> <p>(25) "Targeted advertising" [...] Means displaying to a consumer an advertisement that is selected based on personal data obtained or inferred over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict consumer preferences</p>

					<p>consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.</p> <p>Deletion. (d) Right to deletion. A consumer has the right to delete personal data concerning the consumer.</p> <p>Portability. (e) Right to data portability. When exercising the right to access personal data pursuant to subsection (1)(b) of this section, a consumer has the right to obtain the personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance. A consumer may exercise this right no more than two times per calendar year. Nothing in this subsection (1)(e) requires a controller to provide the data to the consumer in a manner that would disclose the controller's trade secrets.</p> <p>Data protection assessments. A controller shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment of each of its processing activities that involve personal data acquired on or after July 1, 2023, that present a heightened risk of harm to a consumer.</p>	<p>or interests [...]. <i>With exceptions.</i></p> <p>Heightened risk of harm. (2) For purposes of this section, "processing that presents a heightened risk of harm to a consumer" includes the following: (a) Processing personal data for purposes of targeted advertising or for profiling if the profiling presents a reasonably foreseeable risk of: (I) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (II) Financial or physical injury to consumers; (III) A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or (IV) Other substantial injury to consumers; (b) Selling personal data; and (c) Processing sensitive data.</p>
Virginia Consumer Data Protection Act	Virginia	n/a	Statute	Consumer data protection	<p>Rights. A controller shall comply with an authenticated consumer request to exercise the right:</p> <p>[Access.] 1. To confirm whether or not a controller is processing the consumer's personal data and to access such personal data;</p> <p>[Correction.] 2. To correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;</p>	<p>Profiling. "Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.</p> <p>Targeted advertising. "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's</p>

					<p>[Deletion.] 3. To delete personal data provided by or obtained about the consumer;</p> <p>[Portability.] 4. To obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means; and</p> <p>[Opt out.] 5. To opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.</p> <p>Data protection assessments. A. A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:</p> <ol style="list-style-type: none"> 1. The processing of personal data for purposes of targeted advertising; 2. The sale of personal data; 3. The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers; 4. The processing of sensitive data; and 	<p>activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests. <i>With exceptions.</i></p>
--	--	--	--	--	--	---

					5. Any processing activities involving personal data that present a heightened risk of harm to consumers.	
Connecticut Data Privacy Act	Connecticut	n/a	Statute	Consumer privacy	<p>Rights. A consumer shall have the right to:</p> <p>[Access.] (1) Confirm whether or not a controller is processing the consumer's personal data and access such personal data, unless such confirmation or access would require the controller to reveal a trade secret;</p> <p>[Correction.] (2) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;</p> <p>[Deletion.] (3) delete personal data provided by, or obtained about, the consumer;</p> <p>[Portability.] (4) obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means, provided such controller shall not be required to reveal any trade secret; and</p> <p>[Opt out.] (5) opt out of the processing of the personal data for purposes of (A) targeted advertising, (B) the sale of personal data, except as provided in subsection (b) of section 6 of this act, or (C) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.</p> <p>Data protection assessments. A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm</p>	<p>Dark pattern. (11) "Dark pattern" (A) means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and (B) includes, but is not limited to, any practice the Federal Trade Commission refers to as a "dark pattern".</p> <p>Profiling. (22) "Profiling" means any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.</p> <p>Targeted advertising. (28) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer's preferences or interests. <i>With exceptions.</i></p> <p>Heightened risk of harm. processing that presents a heightened risk of harm to a consumer includes: (1) The processing of personal data for the purposes of targeted advertising; (2) the sale of personal data; (3) the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of (A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers, (B) financial, physical or reputational injury to consumers, (C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a</p>

					to a consumer.	reasonable person, or (D) other substantial injury to consumers; and (4) the processing of sensitive data.
--	--	--	--	--	----------------	--

8. Appendix B: Colorado Data Protection Assessments

8.1 Background

The Colorado Privacy Act requires that any data controller engaged in “processing that presents a heightened risk of harm to a consumer [...] conduct[] and document[] a data protection assessment of each of its processing activities that involve personal data”.¹¹⁶ The statute further defines “processing that presents a heightened risk of harm to a consumer” as follows:

For purposes of this section, "processing that presents a heightened risk of harm to a consumer" includes the following:

- (a) Processing personal data for purposes of targeted advertising or for profiling if the profiling presents a reasonably foreseeable risk of:
 - (I) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
 - (II) Financial or physical injury to consumers;
 - (III) A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or
 - (IV) Other substantial injury to consumers;
- (b) Selling personal data; and
- (c) Processing sensitive data.¹¹⁷

The CDL’s rules cover data protection assessments in Rule 8 (covering all data protection assessments) and in Rule 9.06 (covering data protection assessments for profiling only).

Rule 8.04 requires that data protection assessments include 13 specified categories of information, including “[a] short summary of the Processing activity” (Rule 8.04(A)(1)), “[t]he categories of Personal Data to be Processed and whether they include Sensitive Data” (Rule 8.04(A)(2)), and “[t]he nature and operational elements of the Processing activity” (Rule 8.04(A)(4)).

Two provisions of the rules address which harms must be assessed in a data protection assessment for profiling: Rule 8.04(A)(6) and Rule 9.06(F).

Rule 8.04(A)(6) applies to all data protection assessments (both profiling and non-profiling). It requires that data protection assessments include the “sources and nature of risks to the rights of Consumers associated with the Processing activity posed by the Processing activity”. Rule

¹¹⁶ Colo. Rev. Stat. § 6-1-1309(1).

¹¹⁷ Colo. Rev. Stat. § 6-1-1309(2).

8.04(A)(6) notes that “[t]he source and nature of the risks may differ based on the processing activity and type of Personal Data processed”, and then lists the following 11 nonexhaustive “example[s]” of “[r]isks to the rights of Consumers that a Controller may consider in a data protection assessment”:

- a. Constitutional harms, such as speech harms or associational harms;
- b. Intellectual privacy harms, such as the creation of negative inferences about an individual based on what an individual reads, learns, or debates;
- c. Data security harms, such as unauthorized access or adversarial use;
- d. Discrimination harms, such as a violation of federal antidiscrimination laws or antidiscrimination laws of any state or political subdivision thereof, or unlawful disparate impact;
- e. Unfair, unconscionable, or deceptive treatment;
- f. A negative outcome or decision with respect to an individual’s eligibility for a right, privilege, or benefit related to financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services;
- g. Financial injury or economic harm;
- h. Physical injury, harassment, or threat to an individual or property;
- i. Privacy harms, such as physical or other intrusion upon the solitude or seclusion or the private affairs or concerns of Consumers, stigmatization or reputational injury;
- j. Psychological harm, including anxiety, embarrassment, fear, and other mental trauma; or
- k. Other detrimental or negative consequences that affect an individual’s private life, private affairs, private family matters or similar concerns, including actions and communications within an individual’s home or similar physical, online, or digital location, where an individual has a reasonable expectation that Personal Data or other data will not be collected, observed, or used.¹¹⁸

Rule 9.06(F) applies only to profiling presenting a “reasonably foreseeable risk” as discussed above. It requires that data protection assessments [for profiling] include additional analysis for each “assessed reasonably foreseeable risk”. Rule 9.06(F) requires that the analysis for each such risk include 12 enumerated categories of information “as applicable to the assessed reasonably foreseeable risk”, including “[a] plain language explanation of why the Profiling directly and reasonably relates to the Controller’s goods and services” (Rule 9.06(F)(4)), “[a]n explanation of the training data and logic used to create the Profiling system” (Rule 9.06(F)(5)), and “[s]afeguards used to reduce the risk of harms identified” (Rule 9.06(F)(11)).

Rule 9.06(E) further defines the term “[o]ther substantial injury to consumers”, which is one of the categories of risk that, if “reasonably foreseeable”, trigger the data protection assessment

¹¹⁸ 4 CCR 904-3, Rule 8.04.

requirement. Rule 9.06(E) provides that “Controllers should consider both the type and degree of potential harm to Consumers when determining if Profiling presents a reasonably foreseeable risk of “other substantial injury” to Consumers [...]. For example, a small harm to a large number of Consumers[] may constitute “other substantial injury”.”¹¹⁹

8.2 Analysis

8.2.1 Differences in Substantive Standards

Rule 8.04(A)(6) and Rule 9.06(F) present different substantive standards for determining which risks must be discussed under each rule. Under Rule 8.04(A)(6), a risk must be included if it is a “risk[] to the rights of Consumers associated with the Processing activity posed by the Processing activity”. Under Rule 9.06(F), a risk must be included if it is an “assessed reasonably foreseeable risk”. While “reasonably foreseeable” is not further defined in the Colorado Privacy Act, the statutory section imposing data protection assessment requirements uses the term as a qualifier for “[u]nfair or deceptive treatment of, or unlawful disparate impact on, consumers”, “[f]inancial or physical injury to consumers”, “[a] physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person”, and “[o]ther substantial injury to consumers” (Colo. Rev. Stat. § 6-1-1309).

The difference in substantive standards — between risks “associated with the Processing activity” and “reasonably foreseeable risk[s]” — likely stems from the statute, which uses the term “reasonably foreseeable” only in the context of profiling (and not for other types of processing that are subject to the data protection assessment). Independent of the design of the statute, however, there is no discernable regulatory justification for the differences in standards. The use of two separate standards raises questions as to whether the substantive standards are intended to be different and, if so, which standard includes more or less risks.

8.2.2 Foreseeability

Colo. Rev. Stat. § 6-1-1309(2)(a) and Rule 9.06(F) both use the “reasonably foreseeable risk” standard. Foreseeability is a well-known standard of legal analysis and the subject of active debate. Zipursky (2009) notes that “[t]he adjective ‘foreseeable’ occurs twice in section 3 of the *Restatement (Third)* on ‘Negligence’”, which reads as follows:

“A person acts negligently if the person does not exercise reasonable care under all [of] the circumstances. Primary factors to consider in ascertaining whether the person's conduct lacks reasonable care are the foreseeable likelihood that the person's conduct will result in

¹¹⁹ 4 CCR 904-3, Rule 9.06(E).

harm, the foreseeable severity of any harm that may ensue, and the burden of precautions to eliminate or reduce the risk of harm.”¹²⁰

While there is no single clear, unambiguous, and objective definition of foreseeability, the term and standard are often used in legal writing and by courts, which gives data controllers guidance on how the term is likely to be interpreted in the context of the Colorado Privacy Act and the CDL’s rules.

The wording of the Rule 9.06(F) standard is broader than the equivalent GDPR standard. Article 35 of the GDPR requires a risk assessment if the processing is “likely to result in a high risk to the rights and freedoms of natural persons”.¹²¹ Although the definition of foreseeability is subject to some disagreement, it is clear that foreseeability is a lower standard than “likely to result”. That is, any risk that is “likely to result” from processing is also foreseeable, but the opposite is not true.

The reasoning underlying negligence torts is similar to the reasoning for data protection assessments. Both the common-law definitions of negligence torts and Colorado’s data protection assessment requirements seek to ensure that relevant actors exercise reasonable care in assessing and reducing risks of harm (c.f. Rule 9.06(F)(11), requiring data protection assessments to identify “[s]afeguards used to reduce the risk of harms”). One benefit of the foreseeability standard is that it is consistent with legal standards used in broader contexts.

Compared with the GDPR “likely to result” standard, Colorado’s foreseeability standard benefits consumers by requiring analysis of a broader set of risks to consumers. However, relative to the “likely to result” standard, the foreseeability standard imposes greater requirements on businesses by requiring them to expend resources analyzing risks that are not necessarily “likely to result” from their profiling activities.

8.2.3 Risks Associated with the Processing Activity Posed by the Processing Activity

Unlike Rule 9.06(F), Rule 8.04(A)(6) — which requires discussion of “risks to the rights of Consumers associated with the Processing activity posed by the Processing activity” — does not adopt a standard that is regularly used in other contexts. Under this standard, a risk must be discussed if it is “associated with the Processing activity” and “posed by the Processing activity”. These terms are not further defined in the CDL’s rules, creating uncertainty about what set of risks are typically “associated with” and “posed by” a particular activity.

¹²⁰ Benjamin C. Zipursky, “Foreseeability in Breach, Duty, and Proximate Cause,” *Wake Forest Law Review* 44, no. 5 (2009): 1247-1276.

¹²¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, Article 27.

8.2.4 List of Harms

Despite having a less clear standard, Rule 8.04(A)(6) does provide a list of harms that data controllers “may consider”, as discussed above. As of this writing, the CDL has not released the materials on which it drew in arriving at this list of risks. However, many of these risks correlate with the risks defined in the Colorado Privacy Act. Additionally, many of these risks are consistent with the theoretical framework enumerated in Citron and Solove (2022), which we discuss earlier in our literature review section. We list the closest parallel harms identified in the Colorado statute and/or other relevant authority, as well as in Citron and Solove (2022), in the following table:

Harm Enumerated in March 2023 Adopted Rules (4 CCR 904-3, Rule 8.04(A)(6))	Parallel Statutory Provision (Or, If None, Relevant Authority)	Parallel Harm in “Privacy Harms” by Citron & Solove (2022)¹²²
“Constitutional harms, such as speech harms or associational harms” (Rule 8.04(A)(6)(a)).	None apparent. However, in Colo. Rev. Stat. § 6-1-1302, the Colorado General Assembly as part of its legislative findings in adopting the Colorado Privacy Act found that “Colorado’s Constitution explicitly provides the right to privacy under section 7 of article II, and fundamental privacy rights have long been, and continue to be, integral to protecting Coloradans and to safeguarding our democratic republic”.	Section V.E.6, “Chilling Effects”, a subsection of “Autonomy Harms”, defined as follows: “Chilling effects involve harm caused by inhibiting people from engaging in certain civil liberties, such as free speech, political participation, religious activity, free association, freedom of belief, and freedom to explore ideas.”
“Intellectual privacy harms, such as the creation of negative inferences about an individual based on what an individual reads, learns, or debates” (Rule 8.04(A)(6)(b)).	None apparent. The term “intellectual privacy” likely originates from Neil Richards’s “Intellectual Privacy: Rethinking Civil Liberties in the Digital Age” (2015).	Section V.E.6, “Chilling Effects”, a subsection of “Autonomy Harms”. Citron & Solove (2022) cite Richards when writing: “Chilling effects involve harm caused by inhibiting people from engaging in certain civil liberties, such as free speech, political participation, religious activity, free association, freedom of belief, and freedom to explore ideas.”

¹²² Citron, Danielle Keats and Solove, Daniel J., Privacy Harms (February 9, 2021). GWU Legal Studies Research Paper No. 2021-11, GWU Law School Public Law Research Paper No. 2021-11, 102 Boston University Law Review 793 (2022), Available at SSRN: <https://ssrn.com/abstract=3782222> or <http://dx.doi.org/10.2139/ssrn.3782222>

Harm Enumerated in March 2023 Adopted Rules (4 CCR 904-3, Rule 8.04(A)(6))	Parallel Statutory Provision (Or, If None, Relevant Authority)	Parallel Harm in “Privacy Harms” by Citron & Solove (2022) ¹²²
“Data security harms, such as unauthorized access or adversarial use” (Rule 8.04(A)(6)(c)).	Several statutory provisions, including Colo. Rev. Stat. § 6-1-1308(5), which imposes a duty of care on data controllers to “secure personal data during both storage and use from unauthorized acquisition”.	None apparent.
“Discrimination harms, such as a violation of federal antidiscrimination laws or antidiscrimination laws of any state or political subdivision thereof, or unlawful disparate impact” (Rule 8.04(A)(6)(d)).	Colo. Rev. Stat. § 6-1-1309(2)(a)(I), which defines “processing that presents a heightened risk of harm to a consumer” to include “unfair or deceptive treatment of, or unlawful disparate impact on, consumers”.	Section V.F, “Discrimination Harms”, defined as follows: “Discrimination harms involve entrenching inequality and disadvantaging people based on gender, race, national origin, sexual orientation, age, group membership, or other characteristics or affiliations”.
“Unfair, unconscionable, or deceptive treatment” (Rule 8.04(A)(6)(e)).	Colo. Rev. Stat. § 6-1-1309(2)(a)(I), which defines “processing that presents a heightened risk of harm to a consumer” to include “unfair or deceptive treatment of, or unlawful disparate impact on, consumers”.	Section V.E.4, “Thwarted Expectations”, defined as follows: “The harm caused by thwarted expectations involves the undermining of people’s choices, such as breaking promises made about the collection, use, and disclosure of personal data.”
“A negative outcome or decision with respect to an individual’s eligibility for a right, privilege, or benefit related to financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services” (Rule 8.04(A)(6)(f)).	Colo. Rev. Stat. § 6-1-1303(10), which defines “decisions that produce legal or similarly significant effects concerning a consumer” to mean “a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services”.	None apparent. However, this relates to Section V.B, “Economic Harms”, defined as follows: “Economic harms involve monetary losses or a loss in the value of something. Privacy violations can result in financial losses that the law has long understood as cognizable harm.”
“Financial injury or economic harm” (Rule 8.04(A)(6)(g)).	Colo. Rev. Stat. § 6-1-1309(2)(a)(II), which defines	Section V.B, “Economic Harms”, defined as follows:

Harm Enumerated in March 2023 Adopted Rules (4 CCR 904-3, Rule 8.04(A)(6))	Parallel Statutory Provision (Or, If None, Relevant Authority)	Parallel Harm in “Privacy Harms” by Citron & Solove (2022) ¹²²
	“processing that presents a heightened risk of harm to a consumer” to include “financial or physical injury to consumers”.	“Economic harms involve monetary losses or a loss in the value of something. Privacy violations can result in financial losses that the law has long understood as cognizable harm.”
“Physical injury, harassment, or threat to an individual or property” (Rule 8.04(A)(6)(h)).	Colo. Rev. Stat. § 6-1-1309(2)(a)(II), which defines “processing that presents a heightened risk of harm to a consumer” to include “financial or physical injury to consumers”.	Section V.A, “Physical Harms”, defined as follows: “Privacy violations can lead to physical harms, which are harms that result in bodily injury or death.”
“Privacy harms, such as physical or other intrusion upon the solitude or seclusion or the private affairs or concerns of Consumers, stigmatization or reputational injury” (Rule 8.04(A)(6)(i)).	Colo. Rev. Stat. § 6-1-1309(2)(a)(III), which defines “processing that presents a heightened risk of harm to a consumer” to include “a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person”.	Several: Section V.C, “Reputational Harms”, defined as follows: “Reputational harms involve injuries to an individual’s reputation and standing in the community.” Section V.D.2, “Disturbance”, defined as follows: “Disturbance involves unwanted intrusions that disturb tranquility, interrupt activities, sap time, and otherwise serve as a nuisance.”
“Psychological harm, including anxiety, embarrassment, fear, and other mental trauma” (Rule 8.04(A)(6)(j)).	None apparent.	Section V.D, “Psychological Harms”, and subsection 2 thereof, titled “Emotional Distress”: “Psychological harms involve a range of negative mental responses, such as anxiety, anguish, concern, irritation, disruption, or aggravation.”
“Other detrimental or negative	No directly comparable	None apparent.

Harm Enumerated in March 2023 Adopted Rules (4 CCR 904-3, Rule 8.04(A)(6))	Parallel Statutory Provision (Or, If None, Relevant Authority)	Parallel Harm in “Privacy Harms” by Citron & Solove (2022)¹²²
consequences that affect an individual’s private life, private affairs, private family matters or similar concerns, including actions and communications within an individual’s home or similar physical, online, or digital location, where an individual has a reasonable expectation that Personal Data or other data will not be collected, observed, or used” (Rule 8.04(A)(6)(k)).	provision apparent. However, Colo. Rev. Stat. § 6-1-1309(3) requires that, when conducting a data protection assessment, a controller “shall factor into” the assessment of the risks and benefits of the processing of data “the reasonable expectations of consumers”.	

The inclusion of a specific example list of risks that processing may pose to the rights of a consumer is a strength of CDL’s March 2023 adopted rules. The list is both non-exhaustive and nonbinding: the rule provides that controllers “may consider” the risks on the list, and the phrases “for example” and “include” indicate that the listed risks are not the only risks to consider. Nonetheless, the inclusion of the list of risks in the regulation (rather than, for example, a subsequent nonbinding guidance document) clearly indicates the wide scope of risks that companies are expected to consider.

A significant benefit of the nonbinding nature of the list of risks is the increased flexibility for data controllers (companies) whose processing clearly does not pose one or more of the enumerated risks. With a nonbinding list of risks, those processors would not be required to conduct an analysis of risks that are wholly inapplicable to their processing activity.

However, a significant corresponding regulatory gap is that the rule provides little guidance for a data controller to determine which risks it is required to discuss. As we discussed above, Rule 8.04(A)(6)’s substantive standard for inclusion of a risk (“risks to the rights of Consumers associated with the Processing activity posed by the Processing activity”) lacks detail and is unclear about the threshold at which a particular risk must be discussed. The inclusion of a nonbinding list of risks that controllers “may consider” does not address this concern: controllers may still erroneously assess that an enumerated class of risks is inapplicable to their processing activity and therefore fail to include analysis of that class of risks in their data protection assessment. Without a detailed specification of the circumstances under which each enumerated harm should be analyzed, inclusion of the list of harms fails to prevent controllers from narrowly assessing the risks of harm arising from their processing and thereby failing to consider those risks of harm in their data protection assessments. This regulatory gap could be partly, but not entirely,

addressed with greater interpretive guidance from the CDL; however, unlike in the European Union, such guidance would lack legal effect.

8.2.5 Large and Small Risks

Rule 9.06(E) requires data controllers to “consider both the type and degree of potential harm to Consumers” when determining what harms trigger the data protection assessment requirement. In particular, Rule 9.06(E) provides that “a small harm to a large number of Consumers[] may constitute ‘other substantial injury’”, which would then trigger a data protection assessment.

This approach is consistent with Citron and Solove (2022)’s observation that “many privacy harms [...] are small but numerous”. In particular, Citron and Solove (2022) note that “[p]rivacy harms often involve the aggregation of many small harms to each individual, which is compounded by the aggregation of all these harms to many individuals”, and argue that this phenomenon, “Aggregation of Small Harms”, is the first of three “challenges that make [the] recognition [of privacy harms] difficult”.¹²³

Rule 9.06(E) addresses Citron and Solove (2022)’s observation by requiring data controllers to give additional consideration to harms that could affect many individuals. However, the rules do not further define “large number of Consumers” or otherwise impose specific requirements on the harms that must be discussed, which may limit the practical application of this section.

¹²³ Citron, Danielle Keats and Solove, Daniel J., Privacy Harms (February 9, 2021). GWU Legal Studies Research Paper No. 2021-11, GWU Law School Public Law Research Paper No. 2021-11, 102 Boston University Law Review 793 (2022), Available at SSRN: <https://ssrn.com/abstract=3782222> or <http://dx.doi.org/10.2139/ssrn.3782222>

From: Rachel Michelin [REDACTED]
Sent: Monday, March 27, 2023 4:51 PM
To: Regulations
Subject: PR 02-2023 - comments on regulations
Attachments: CRA CCPA Reg comments April 2023.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Thank you for the opportunity to provide comments on the regulatory process. Please do not hesitate to reach out if you have any questions or need additional information.

Rachel Michelin

Rachel Michelin

President & CEO
1121 L Street, #607
Sacramento, CA 95814

P: [REDACTED]





April 27, 2023

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

VIA Email: regulations@coppa.ca.gov.

Dear Members of the Committee:

Thank you for the opportunity to provide comments. Below, please find general comments followed by more specific comments on various sections within the regulations.

RISK ASSESSMENTS

On behalf of the California Retailers Association (CRA), we are encouraged to see the California Privacy Protection Agency (CPPA) is asking about existing regimes and considering whether the risk assessments under the General Data Protection Regulation (GDPR) or Colorado Privacy Act would be sufficient to satisfy the California Privacy Rights Act (CPRA) requirements. CRA is in favor of consistent standards across jurisdictions as many retailers operate globally. CRA encourages the CPPA to specifically allow companies to meet the requirements under these provisions by conducting audits, assessments, and opt-out as allowed under existing laws.

For risk assessments, CPPA should clearly and carefully define what activities may present a significant risk of harm to trigger a risk assessment. Looking to the standards under GDPR and other existing state laws is a good point of reference. CRA would like to note that risk assessments are generally not required to be proactively filed with the government, as the rulemaking provision contemplates. That adds a layer of process that will be burdensome for businesses (as far as timing and process, and in preparing a separate summary of the assessments, as contemplated by the rulemaking directive) and could potentially become overwhelming to the agency as they will be inundated with filings. CRA respectfully suggests that the agency reserve the right to request risk assessments from the business as relevant to an enforcement action or inquiry to avoid the burden on both sides. These should be kept confidential when provided.

CYBER SECURITY

CRA is not aware of any current United States laws that require cybersecurity audits to be performed. While it is appropriate to hold companies accountable for reasonable cybersecurity practices that consider the size and scope of personal information, the process in defining their cybersecurity program and required audits should be narrowly tailored to prevent overburdening companies with documentation and processes that don't improve their cybersecurity posture. Any proactive auditing requirement should be limited to systems that process large volumes of data whose breach could result in harm to the consumer (harm such as identity

theft). CRA encourages the CPPA to make any auditing requirement narrower than systems that process sensitive data, since that definition includes categories of data that would not lead to such a harm (such as geolocation data).

AUTO DECISION MAKING

The statute is narrow on what the CPPA should consider rulemaking on – the scope of access and opt-out rights related to this type of process. We encourage the CPPA to not expand beyond this scope to consider issues such as “the prevalence of algorithmic discrimination” as mentioned in the request for comment. We contend this could potentially go beyond the CPPA mandate and could potentially be outside the scope of the CPPA.

State laws applicable to automated decision-making opt-outs are generally limited to profiling for targeted advertising purposes; and CPRA should be likewise limited since there is no definition of automated decision-making, but the definition of profiling seems to contemplate advertising uses of the data. This would allow California to be consistent with existing state laws. If the opt-out right were broader than advertising-related uses of automated decision making, opt-out rights should be limited to decisions made using “solely automated” processes. Processing that is ultimately human-driven does not present the risks to individuals which the ability to opt-out of solely automated processing is designed to address.

Below are California Retailers Association comments on specific sections:

CYBERSECURITY AUDITS

CCPA comment request section 1.3: Reliance on Existing Audits: *What would the benefits and drawbacks be for businesses and consumers if the Agency accepted cybersecurity audits that the business completed to comply with the laws identified in question 1, or if the Agency accepted any of the other cybersecurity audits, assessments, or evaluations identified in question 2? How would businesses demonstrate to the Agency that such cybersecurity audits, assessments, or evaluations comply with CCPA’s cybersecurity audit requirements?*

CRA Comment: Some existing laws allow businesses to submit an annual self-certification that the required audit has occurred (e.g., as under New York State Department of Financial Services - NYDFS). The Agency should adopt a similar regulation and allow annual self-certification to the Agency. Further, if the processing that creates a significant risk (as eventually defined by the regulation) is already the subject of another audit (e.g., PCI or SOX), then the existing audit should suffice for the purposes of the CPRA regulations.

Businesses should also be given the option (as an alternative, not as the sole requirement) to submit proof of a certification such as PCI, NIST, or ISO that demonstrates their compliance with this requirement.

Businesses may already perform certain industry standard audits and reports. For example, storage of payment cards on file is regulated in the industry by the PCI-DSS standards and merchants are required to re-certify every year. In those circumstances, businesses should be able to re-use such audits/certifications rather than duplicate their efforts, which would unduly add to the cost and burden of compliance.

Businesses should be permitted to use certifications and audits related to cybersecurity from service providers to help meet their requirements to conduct cybersecurity audits and provide risk assessments.

CPPA comment request section 1.4: Monitoring: *With respect to the laws, cybersecurity audits, assessments, or evaluations identified in response to questions 1 and/or 2, what processes help to ensure that these audits, assessments, or evaluations are thorough and independent? What else should the Agency consider to ensure that cybersecurity audits will be thorough and independent?*

CRA Comment: The Agency should allow companies to rely on reasonable industry standards. To ensure that audits are independent, companies should also be permitted to rely on internal bodies that have safeguards to ensure that they are independent.

CPPA Comment request section 1.5: Other Considerations: *What else should the Agency consider to define the scope of cybersecurity audits?*

CRA Comment: The Agency should clearly define what type of processing creates a significant risk, preferably by limiting the types of personal information to which the audit requirement applies. Other sector-specific laws that require similar audit are limited to specific types of personal information such as payments data (as in the NYDFS Cybersecurity Regulation). For large businesses, conducting such an audit for lower risk personal information that does not require such audits under other laws would create significant expense with little benefit to consumers.

Many businesses already have self-audit mechanisms and other internal standards and protocols based on appropriate industry standards. And larger businesses have internal teams that exist solely to conduct audits and that are separate from the first-line teams that are implementing security controls. Such an audit can be conducted by auditors internal or external to the covered entity and its affiliates. These teams are designed to be thorough and independent. Businesses should be able to leverage those existing processes to meet CPRA requirements.

Businesses should not be required to use third party auditors as the burden and expense would be wildly disproportionate to any downstream consumer benefit, and the result would likely be increased consumer costs. Paradoxically, third-party audits may also present a security risk, as they may expose a business's confidential security practices and (depending on the nature of the audit) potentially also underlying data to one or more third parties.

CPPA Comment request section 2.3: Risky Processing Activities: *To determine what processing of personal information presents significant risk to consumers' privacy or security under Civ. 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? b. What other models or factors should the Agency consider? c. Should the models or factors be different, or assessed differently, for determining when processing requires a risk assessment versus a cybersecurity audit? If so, how? d. What processing, if any, does not present significant risk to consumers' privacy or security? Why?*

CRA Comment: section (d): From a privacy risk perspective, risk assessments should be limited to processing that has a legal or similarly significant effect on an individual, i.e., where it materially affects a decision that will impact housing, education, employment, and other areas protected from discrimination under the law. This should exclude incidental processing of personal data that is not a primary factor in the decision that has the legal or similarly significant effect.

From a security risk perspective, risk assessments should be limited to processing data that, if compromised, is likely to result in real, concrete harm to individuals. Examples may include identity theft/fraud, extortion, or physical injury from disclosure of intimate or other objectively sensitive personal details (e.g., sexual orientation).

Processing of personal information in any context for fraud prevention, anti-money laundering processes, screening, or to otherwise comply with legal obligations should be exempted from the scope of this definition/regulation. These activities protect consumers' privacy and security and we keep such activities confidential to prevent bad actors from gaining insight into our internal systems.

Additional data protection measures, such as pseudonymizing or encrypting the relevant data, can meaningfully reduce the risk of processing.

CCPA Comment request section 2.4: *DPIA Content: What minimum content should be required in businesses' risk assessments? a. What would the benefits and drawbacks be if the Agency considered the data protection impact assessment content requirements under GDPR and the Colorado Privacy Act? b. What, if any, additional content should be included in risk assessments for processing that involves automated decision-making, including profiling?*

CRA Comment: section (a): The DPIA should be detailed enough for the business and the regulator to appreciate the risk. However, it should not be overly prescriptive or specific. This will allow businesses to retain flexibility and scale existing processes, where a wide variety of factors may apply.

The Agency should consider a similar approach as the EU's Article 29 Data Protection Working Group Report (2017): *"The GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA to allow for this to fit with existing working practices. There are several different established processes within the EU and worldwide which take account of the components described in recital 90. However, whatever its form, a DPIA must be a genuine assessment of risks, allowing controllers to take measures to address them."*

The DPIA should be viewed as a documentation requirement, and not a substantive requirement that the company must mitigate or fix any identified risk. The DPIA should also be limited to the actual processing of data—it should not be used as a proxy to require a risk assessment of the feature itself as distinct from any processing of data that occurs as part of that feature. Finally, the Agency should permit a single risk assessment to cover multiple related types of data processing activities.

CCPA Comment request section 2.5: Reliance on Other DPIAs: *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?*

CRA Comment: The regulations should recognize that risk assessments are an increasingly common requirement under U.S. and international privacy and data protection laws. To promote interoperability and minimize burdens to covered businesses, the regulations should specify that the Agency will accept risk assessments that were originally conducted pursuant to a comparable legal requirement. Privacy obligations and risk balancing should be consistent across jurisdictions relating to the same requirements. As such, we suggest aligning with any data impact or risk assessments required under other similar laws, such as the CPA and VCDPA. However, the Agency should be wary of adopting in full any future regulatory guidance under other laws, including the GDPR. EU case law is evolving in unpredictable ways, and California should develop guardrails that would ensure that the any future obligations on California businesses are appropriately balanced against any potential burden.

A consistent standard across jurisdictions would allow businesses to continue to build robust systems to protect consumers information. These systems will benefit from clear guidelines that allow businesses to innovate and develop their data protection assessments and properly assess their cybersecurity risks.

CCPA Comment request section 2.6: DPIA Submission: *How should businesses submit risk assessments to the Agency?*

- 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?*
- 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)?*

CRA Comment: (a): As a threshold matter, the Agency should clarify that its function under the statute to provide "a public report summarizing the risk assessments filed with the agency" refers to the risk assessments identified in 1798.185(15)(b). The statute appears to mistakenly refer to 1798.185(15)(a), which concerns cybersecurity audits.

With respect to (a)(i), risk assessments should highlight the most significant privacy risks associated with the processing activity in question and the steps being taken to address and mitigate that risk. They should not require the company to divulge commercially sensitive information or sensitive security information, such as details about technical safeguards that would allow a bad actor to compromise the company's security practices.

With respect to (a)(ii), the Agency should not overly prescribe the format in which the business must submit the risk assessment. Businesses may prepare and record assessments in different ways and in response to different jurisdictions, and so they should retain flexibility to submit the assessment without needing to alter the format or content to match California-specific requirements. An example of an overly-prescriptive format would be if the Agency mandated that a business submit the required information via a webform with answer bubbles that needed to be manually populated.

With respect to (a)(iii), the regulations should not require organizations to repeatedly conduct or submit risk assessments for processing activities that have not materially changed and that pose no new or heightened risks. Such a requirement would be operationally burdensome, particularly for small and medium sized businesses, and could incentivize businesses to treat risk assessments as a mere ‘*check-the-box*’ compliance exercise. Therefore, the Agency’s regulations should specify that businesses are only required to “*regularly submit*” assessments for new or materially changed processing practices that present a significant risk. If the Agency requires periodic updates absent any change, then such updates should not occur more frequently than once every three years.

CCPA Comment request section 2.8: Other Considerations: *What else should the Agency consider in drafting its regulations for risk assessments?*

CRA Comments: In providing guidance for conducting risk assessments and weighing the benefits of processing against potential risks, the regulations should provide that the factors relevant to this balancing may include:

- Technical and organizational measures and safeguards implemented by the business to mitigate privacy and security risks.
 - The reasonable expectations of consumers
 - The context of the processing with respect to the relationship between the business and consumers
 - The regulations should also include protections to ensure that businesses have the necessary confidence to use risk assessments to fully document and assess processing practices and are not incentivized to treat their assessments as a defensive measure against potential future litigation.
- Therefore, in addition to the important carve out for trade secrets, the regulations should clarify that risk assessments conducted pursuant to the CPRA are confidential and exempt from public inspection and copying under the California Public Records Act and that submitting an assessment to the agency does not constitute a waiver of any attorney-client privilege or work-product protection. The Agency should also not be permitted to use the submitted assessment as evidence of wrongdoing or used to penalize the business for weighing the risks in a way with which the Agency disagrees.

Automated Decision-making

CCPA Comment request section 3.1: Existing Legal Mechanisms: *What laws requiring access and/or opt-out rights in the context of automated decision-making currently apply to businesses or organizations (individually or as members of specific sectors)?*

CRA Comment: The Agency should keep in mind the following context: automation is a subset of decision-making—and so existing laws (such as anti-discrimination frameworks) that govern how a company makes decisions generally would also apply to ADM.

With respect to laws targeted solely to automated decision-making, companies in the US are subject to several existing (or enacted but not yet effective) privacy laws that already impose substantial obligations with respect to the consumer right to opt out of automated decision-making. This includes the Colorado, Connecticut, and Virginia state privacy laws. Critically, each of these laws is limited to high-risk decisions, described as those which have “*legal or similarly significant effects*,” and in the case of Connecticut, target “*solely*” automated decisions.

To ensure interoperability with those laws and to strike the right balance between protecting consumers while enabling access to important technology, the Agency should likewise confirm through rulemaking that the profiling opt out (i) applies only to decisions with “*legal or similarly significant effect*”, (ii) is limited to solely or fully automated decisions, and (iii) applies only after an automated decision is made.

Significant and High-Risk Decisions: On (i), the Agency should not regulate the use of low risk automated decision-making technology, such as spell check, GPS systems, databases, spreadsheets, or transcription services. Requiring businesses to provide opt outs for such low risk technology could slow down their activities substantially, while not providing a meaningful benefit to consumers, who should expect that business activities are performed using well-accepted, widely used technology. Regulators should focus on high-risk use cases, such as using technology to make final decisions regarding access to housing, medical benefits, or other critical services without appropriate human involvement. For example, under the Virginia privacy law, the consumer’s right to opt out of profiling is restricted to “*decisions that produce legal or similarly significant effects concerning a consumer.*” This is defined as “*a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.*”

Fully Automated Decisions: On (ii), this limitation avoids creating an unreasonable obligation on businesses, without impacting the right of a consumer to have their decisions assessed by a human.

Final Decisions: On (iii), companies make numerous decisions every day, and automation is one of the ways companies provide faster and more predictable products/services, allowing better customer experience and cheaper prices.

- **Costs and Delays:** Forcing companies to have the option of human involvement even before any decision is made creates a huge burden on companies, which might not be able to support the same number of requests without incurring unreasonable expenses. For example, individuals receive faster access to services if businesses can quickly identify low fraud risks. This is only possible at scale using either simple algorithms – e.g., approve transaction with no prior fraud flags – or more complex algorithms including ones using machine learning. Then, for the smaller set of fraud risk cases, businesses can use manual review to make final decisions, for example through an appeals process. In these situations, if non-final decisions – e.g., cases flagged only by algorithms for further human review

- are regulated, then consumers will receive slower access to services, and will incur higher costs from increased, and unnecessary, manual review.
- **Minimal customer benefit:** While such a pre-decisional requirement will result in higher costs and slower service times, it would not provide consumers with any benefits beyond those that a post-decisional opt-out would provide. For example: If individuals apply for a loan and have a positive outcome on the first automated decision, which might take just a few seconds to be issued, they likely will not want or need to opt-out and request review (but they would still have the right to). Even if they have a negative outcome (again, which they might know in just a few seconds), they will still be able to exercise the right to contest that decision and have a human issuing a new decision. If laws force companies to have the opt-out even before a decision is made, the experience could take several days and without any actual gain for customers, because the decision will be issued by the same person, they already had access in the first example.

CCPA Comment request section 3.2: *Existing Practices: What other requirements, frameworks, and/or best practices that address access and/or opt-out rights in the context of automated decision-making are being implemented or used by businesses or organizations (individually or as members of specific sectors)?*

CRA Comment: Practically speaking, companies do not typically have requirements, frameworks, or best practices that address access/opt outs related to low risk, everyday technology, even those that arguably make automated decisions (for example, spellcheck correcting a typo in the user's name). Access or opt out rights for this type of automated decisions would slow down business substantially with no benefit to consumers. For example, businesses do not typically give consumers the right to opt out of using optical character recognition on PDF documents containing that consumer's personal information. Or, they do not give consumers the right to opt out of having their information stored in an internal database that automatically sorts information alphabetically, and instead demand handwritten records be stored and sorted manually. Regulations should not dictate how businesses use (or don't use) everyday, low-risk technology.

CCPA Comment request section 3.3: *Reliance on Existing Mechanisms: With respect to the laws and other requirements, frameworks, and/or best practices identified in response to questions 1 and 2:*

- a) ***How is "automated decision-making technology" defined? Should the Agency adopt any of these definitions? Why, or why not?***
- b) ***To what degree are these laws, other requirements, frameworks, or best practices aligned with the processes and goals articulated in Civ. Code § 1798.185(a)(16)?***
- c) ***What processes have businesses or organizations implemented to comply with these laws, other requirements, frameworks, and/or best practices that could also assist with compliance with CCPA's automated decision-making technology requirements?***
- 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?***
- e) ***What gaps or weaknesses exist in businesses or organizations' compliance processes with 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?*

CRA Comment: (a): To avoid a sweeping definition that captures all technology or software, policymakers should focus on automated decision-making systems that use machine learning (ML) to automate decisions that produce legal or similarly significant effects. ML is the type of technology that generally implicates transparency, bias, and explainability considerations. Accordingly, automated decision-making should be defined as “*final decisions that are made solely/fully with AI/ML technology with legal or similarly significant effects,*” and AI/ML technology should be defined as: “*the use of machine learning and related technologies that use data to train algorithms and predictive models for the purpose of enabling computer systems to perform tasks normally associated with human intelligence or perception, such as computer vision, natural language processing, and speech recognition.*”

(c): To comply with GDPR, companies already allow EU customers to request review of certain fully automated decisions. Companies can extend that process to US customers as appropriate.

CCPA Comment request section 3.4: Business ADM Practices: *How have businesses or organizations been using automated decision-making 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.*

CRA Comment: Businesses in every industry sector use automatic decision making (ADM) to improve their competitiveness and enhance their product and service offerings, including routine and low-risk applications such as spellcheck and tabulations. For instance, algorithms may be used to recommend a book or song or allow a small business to market its products to the right consumers at affordable prices.

With respect to AI/ML, it is important to note that the adoption of AI across industries is now so widespread that a 2021 McKinsey and Company study found that 56% of business leaders across the globe now report using AI in at least one business function. The McKinsey report highlights that the most common AI uses cases are low risk, involving service-operations optimization, AI-based enhancement of products, and contact-center automation.

CCPA Comment request section 3.5: Consumer Use of ADM: *What experiences have consumers had with automated decision-making technology, including algorithms? What concerns do consumers have about their use of businesses’ automated decision-making technology? Please provide specific examples, studies, cases, data, or other evidence of such experiences or uses when responding to this question, if possible.*

CRA Comment: Automated technology has significant benefits to both businesses and consumers, including enhanced accuracy and consistency, safer and more innovative products, scalability, cost savings, and increased efficiency. Accordingly, regulators should be very mindful about providing consumers with any right to opt out of automated activities, as it could severely hamper businesses’ and other consumers’ ability to realize those advantages.

Guardrails rather than opt out: If high risk business offerings are essential or critical, and it is not reasonable for consumers to consider other options, businesses should have the ability to demonstrate the existence of operational guardrails instead of providing for an opt out. Depending on the specifics of the use case, appropriate guardrails could include things like:

- Significant, rigorous testing
- Corroboration of results
- System monitoring
- Appeals/complaint processes.

Automation as the offered service or product: Automation may be core to certain high-risk service offerings, making opt-outs infeasible. For example, an in-car safety system that automatically senses a crash and immediately connects a driver with assistance shouldn't be required to provide a consumer with some sort of manual process that conducts the same task – that would defeat the purpose of the automated service. In these instances, businesses should have the ability to demonstrate the existence of operational guardrails that protect California consumers' interests instead of providing for an opt out.

Automation may also be essential to products that involve less significant effects, but which nonetheless provide high value with minimal risk to consumers. For example, calendars that provide you with updated travel times based on traffic patterns from your current location. Businesses shouldn't have to design objectively worse (and potentially even dangerous) versions of their products and services merely to give customers a right to opt out of ADM. To avoid unnecessary interruption to consumer enjoyment of these products and services, the Agency should follow the approach of other US state privacy laws and limit the profiling opt out to automation that has legal or similarly significant effects.

Opt-out option may create significant risks: The regulations should recognize that some uses of automated decision-making that produce legal or similarly significant effects may be highly beneficial to consumers—and if turned off, creates the risk of potential harm. The statute did not intend for consumers to be able to opt out of these uses. For example:

- a health-care system that uses an individual's address to select the closest ambulance dispatch location;
- a bank that uses income or account balance to assess available credit; or
- fraud detection and related activities in making financial or insurance decisions.

To protect California consumers' interests without burdening beneficial uses, the regulations should tailor the scope of "*legal or similarly significant effects*" to the harms regulators seek to protect against (e.g., discrimination against protected classes in access to housing or credit). And as noted above, the regulations should permit operational guardrails rather than requiring an opt out.

CCPA Comment request section 3.7: *Opt-out Right to Address Bias: How can access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling, address algorithmic discrimination?*

CRA Comment: Businesses should be allowed to use race/ethnicity and other demographic data with the user's consent for the narrow purpose of evaluating and preventing bias. Regulators should consider a safe harbor for businesses that are trying to prevent bias. It's not possible to prevent bias without measuring the algorithm's impact on different user groups, including minority groups.

CCPA Comment request section 3.8: Industry/Tech Use Cases: *Should access and opt-out rights with respect to businesses' use of automated decision-making 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?*

CRA Comment: Employee and B2B Data: The profiling opt out should exclude automation involving individual data in the employment or and commercial contexts. With respect to the employment context: First, there are developing state and local laws that already specifically target the use of these technologies in the workplace, so California should let that regulatory activity run its course. Second, those laws are being tailored to the nuances of an employment context and, recognizing the potential unreasonableness of requiring specific opt-outs for every instance of automated decision-making, are mainly focused on transparency and human review. Third, basically any decision in the employment context arguably could have a "legal or similarly significant effect," including innocuous ADM like task allocation that is intended to enable efficiency and scale.

CCPA Comment request section 3.9: Access Requests: *What pieces and/or types of information should be included in responses to access requests that provide meaningful information about the logic involved in automated decision-making processes and the description of the likely outcome of the process with respect to the consumer?*

- *What mechanisms or frameworks should the Agency use or require to ensure that truly meaningful information is disclosed?*
- *How can such disclosure requirements be crafted and implemented so as not to reveal a business or organization's trade secrets?*

CRA Comment: Businesses should be able to fulfill consumer access requests by providing a general explanation of technology functionality, rather than information on specific decisions made. Businesses should be able to provide this information via a publicly available disclosure on their webpage. To provide "meaningful" information about the logic involved in a decision, businesses should be permitted to provide a description of the general criteria or categories of inputs used in reaching a decision. For example, if a rental company considers certain personal information when evaluating a housing application, those categories of information could be described.

A more detailed description of any complex algorithms involved in automated decision-making will not provide the average consumer with "meaningful" information on the logic involved in the processing. In

addition, providing a detailed explanation of the algorithms involved runs the risk of imposing obligations that conflict with the intellectual property, trade secret, and other legal rights of the business in question. With respect to fraud or security decision-making, disclosures could instruct fraudsters or bad actors to circumvent the system.

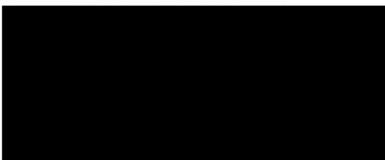
Any regulation should also ensure that businesses are protected from disclosing proprietary information, such as that which is subject to intellectual property or trade secret protection, in response to consumer access requests.

CPPA Comment request section 3.10: *Process: To the extent not addressed in your responses to the questions above, what processes should be required for access and opt-out rights? Why?*

CRA Comment: Any regulations around automated decision-making needs necessary exceptions to access/opt out to avoid abuse (as is already the case in Colorado, Connecticut and Virginia). For example:

- Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report, or prosecute those responsible for any such action.
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena or summons by authorities.
- Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may be illegal.
- Provide a product or service a consumer requested or perform a contract with the consumer.
- Take immediate steps to protect an interest that is essential for the life of the consumer or another natural person, if the processing cannot be manifestly based on another legal basis.
- Process personal data for reasons of public interest in the area of public health, subject to certain conditions.
- Conduct internal research.
- Fix technical errors.
- Perform internal operations that are consistent with the consumer's expectations.

Thank you for your consideration of our concerns. If you have any questions or would like additional input, please do not hesitate to reach out to me directly.



Rachel Michelin
President & CEO
California Retailers Association

From: Tonsager, Lindsey [REDACTED]
Sent: Monday, March 27, 2023 4:55 PM
To: Regulations
Cc: Ponder, Jayne; Fenton, Hensey
Subject: PR 02-2023 Comments of CalChamber
Attachments: Comments of CalChamber.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Attached please find the comments of CalChamber responding to the CPPA's Invitation for Preliminary Comments on Proposed Rulemaking on the following topics: Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking (PR 02-2023).

Best,
Lindsey Tonsager
Jayne Ponder
Hensey Fenton
Counsel for CalChamber

Lindsey Tonsager
Pronouns: She/Her/Hers

Covington & Burling LLP
Salesforce Tower, 415 Mission Street, Suite 5400
San Francisco, CA 94105-2533
T + [REDACTED] [REDACTED]
www.cov.com

COVINGTON

This message is from a law firm and may contain information that is confidential or legally privileged. If you are not the intended recipient, please immediately advise the sender by reply e-mail that this message has been inadvertently transmitted to you and delete this e-mail from your system. Thank you for your cooperation.

COVINGTON

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

Lindsey Tonsager

Covington & Burling LLP
Salesforce Tower
415 Mission Street, Suite 5400
San Francisco, CA 94105-2533

T [REDACTED]
[REDACTED]

By Electronic Mail

March 27, 2023

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

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

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

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

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

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

- For **cybersecurity audits**, the regulations should (A) promote interoperability and align with the processes and goals set forth in existing legal frameworks or recognized standards and (B) afford a business the flexibility to use a risk-based approach, including by tailoring cybersecurity audits to the size and complexity of the business and the nature of the data and processing activity, and to conduct thorough audits internally (“Section I”);
- Regarding **privacy risk assessments** (“privacy assessments”), regulations should (A) prioritize compatibility with existing privacy statutes and (B) align with requirements in the statutory text and related requirements in the CCPA (“Section II”); and
- With respect to **automated decisionmaking** rights, regulations should: (A) define automated decisionmaking to promote coherence across legal frameworks, (B) clarify that certain automated decisionmaking is not subject to opt-out and access rights, and (C) permit a business to provide meaningful information about automated decisionmaking through its privacy policy or similar disclosures, without revealing trade secrets (“Section III”).

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

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

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

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

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

⁴ Cal. Civ. Code § 1798.185(15).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A. The CCPA Should Prioritize Compatibility With Existing Privacy Statutes

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

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

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

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

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

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

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

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

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

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

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

²² VCDPA § 59.1-580(E).

²³ Cal. Civ. Code § 1798.185(15).

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

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

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

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

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

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

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

²⁶ VCDPA § 59.1-580(D).

²⁷ Cal. Civ. Code § 1798.185(15)(B).

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

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

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

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

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

CalChamber appreciates the opportunity to provide input on the scope of access and opt-out rights for automated decisionmaking. Automated decisionmaking technologies offer tremendous opportunities to improve lives and tackle a diverse array of societal challenges, from disaster recovery and resilience³¹ to reducing climate impact.³² At the same time, CalChamber appreciates that businesses should act as trustworthy stewards of automated decisionmaking

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

⁴¹ See California Consumer Privacy Act Regulations, § 7011.

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

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

COVINGTON

March 27, 2023
Page 12

*

*

*

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

Sincerely,

/s/

Lindsey Tonsager
Jayne Ponder
Hensey Fenton
Counsel for CalChamber

From: Jennifer King PhD [REDACTED]
Sent: Monday, March 27, 2023 4:56 PM
To: Regulations
Subject: Stanford submission for PR 02-2023 (part 2)
Attachments: Stanford_ADM_Recommendations.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Greetings -- Attached please find the second of two submissions by Stanford University for PR 02-2023. This submission is a set of public comments in response to the Agency's rulemaking on cybersecurity audits, risk assessments, and automated processing by a team of graduate students in the Program in Public Policy.

Thanks

Jen King

--

Jennifer King, Ph.D (she/her)
Privacy and Data Policy Fellow
Stanford Institute for Human-Centered Artificial Intelligence
hai.stanford.edu

<https://hai.stanford.edu/people/jennifer-king>

www.jenking.net/publications

Google Scholar profile: <https://scholar.google.com/citations?user=O5jENBMAAAAJ&hl=en>



Stanford University
Human-Centered
Artificial Intelligence

Via email: regulations@cppa.ca.gov

27 March 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd
Sacramento, CA 95834

RE: Submission of Preliminary Comments (PR 02-2023)

Dear California Privacy Protection Agency,

On behalf of the graduate students under my direction in the 2022-2023 Stanford University Program in Public Policy graduate practicum, I am pleased to submit these recommendations to the California Privacy Protection Agency (CPPA)'s Preliminary Rulemaking Activities on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking. We appreciate the opportunity to address the CPPA's Invitation for Preliminary Comments on Proposed Rulemaking.

This submission contains a set of policy recommendations made by the student team after the completion of a landscape analysis of the state of automated decisionmaking definitions currently adopted in the U.S.

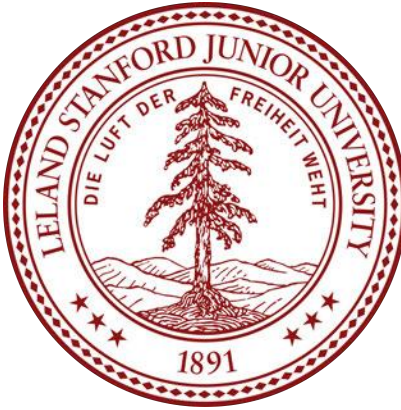
Thank you for your consideration.

Sincerely,

Dr. Jennifer King
Privacy and Data Policy Fellow
Stanford Institute for Human-Centered Artificial Intelligence

Keertan Kini
MPP/MBA Candidate

Kevin Li
MA Candidate, Public Policy



Policy Recommendations

Comments to the California Privacy Protection Agency on Cybersecurity Audits, Risk Assessments, and Automated Processing

Graduate Practicum, Program in Public Policy

Advisor: Dr. Jennifer King,
Stanford University

March 2023

1. Table of Contents

1. Table of Contents	3
2. Introduction	4
3. Recommendation 1: Adopt an Input-Processing-Output Framework for ADM	5
4. Recommendation 2: Shared-Use Data	7
5. Recommendation 3: Adopt A Taxonomy of Harms	9
6. Recommendation 4: Impact Assessments & Trade Secrets	13

2. Introduction

Over the course of the past six months, our team has conducted a report on the landscape of automated decisionmaking (ADM) regulations within the jurisdictions of the State of California, the Federal Government, and other US States. The purpose of this landscape report was to provide insight into how other agencies and jurisdictions defined and pursued regulation of ADM within their appropriate jurisdictions, informing the tradeoffs of various approaches.

The recommendations we offer are independent of the report, but they are informed by the insights that we gained in reviewing the various definitions, requirements, and prohibitions that have been promulgated by either legislation or agencies at each level. The recommendations are similarly based on the gaps and tradeoffs identified as well as the mandate and position of the California Privacy Protection Agency (CPPA) within the regulatory context as the first dedicated privacy regulator within the US and with unique influence over many significant actors within the tech industry.

We do not recommend a specific definition of ADM for adoption by the CPPA. Adoption of a specific definition of ADM may unnecessarily and prematurely curtail the CPPA's regulatory authority if emerging technologies do not clearly fall within that definition. Unlike other states' privacy statutes, the CCPA, as amended, does not impose directly-effective requirements on automated decisionmaking or profiling. Instead, under Cal. Civil Code § 1798.185(a)(16), the authority and responsibility for adopting "regulations governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology" rests with the CPPA.

Accordingly, the CPPA may define subsets of "automated decisionmaking" and specify applicable access and opt-out rights without imposing a regulatory definition of "automated decisionmaking" in full. The CPPA is not mandated to subject all ADM systems to the same regulatory requirements. As we discuss in the following sections, the enumeration of specific harms and risks on which the CPPA can impose more rigorous regulatory requirements may take more salience than adoption of a specific ADM definition.

3. Recommendation 1: Adopt an Input-Processing-Output Framework for ADM

3.1 Recommendation

*The effectiveness of the access and opt-out rights conferred by regulations issued by CPPA under Cal. Civil Code § 1798.185(a)(16) relies on the effectiveness of **substantive consumer privacy rights at each applicable point in the IPO model**: inputs, processing, and outputs.*

3.2 Background

Regulation of automated decisionmaking (ADM) systems by policymakers, including those utilizing forms of artificial intelligence (AI) such as machine learning, predominantly focuses on the outputs of those systems. Outputs include decisional outcomes as well as consumer profiling, and raise issues regarding the fairness of those outputs, potential biases in how they are rendered, as well as impacts on individuals' information privacy. The Input-Process-Output (IPO) framework is a useful concept for understanding and analyzing the various stages of an ADM system's operation. It largely aligns with the NIST AI Risk Framework's three primary components: Data & Input, AI Model, and Task Output.¹ Inputs represent the data fed into an ADM system, which is then processed through complex algorithms to generate outputs or decisions. Similarly, the OECD's classification of AI systems emphasizes the importance of these components in understanding the functionality and risks associated with AI applications.² Recognizing the distinct stages in the IPO model is critical in identifying the appropriate privacy rights and protections for individuals interacting with AI systems.

3.3 Example

Opt-out rights at each stage of the IPO model can significantly affect the efficacy of ADM systems while safeguarding consumer privacy. For instance, at the input stage, consumers may opt-out of data collection, limiting the personal information used by the AI system overall and for any later usage. This action may result in decreased personalization but increased privacy. Furthermore, requiring companies building ADM-based systems to be more transparent about the data used to construct their models, such as by documenting their datasets in depth, may also aid in reducing civil rights and privacy violations as well as potentially enabling explainability of outcomes.

In the processing stage, individuals can exercise their right to object to certain types of data processing, such as general profiling, which can affect the ADM system's ability to generate accurate predictions or more specific use cases such as credit-worthiness. By doing so, however, the data may still be collected for non-profiling uses or for less personally impactful use-cases than

¹ Tabassi, Elham. "Artificial Intelligence Risk Management Framework (AI RMF 1.0)." *NIST*, Elham Tabassi, 26 Jan. 2023, <https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10>.

² OECD (2022), OECD Framework for the Classification of AI systems , *OECD Digital Economy Papers*, No. 323, OECD Publishing, Paris, <https://doi.org/10.1787/cb6d9eca-en>.

credit-worthiness. Nevertheless, this opt-out right is clearly more nuanced and permissive than a prohibition against use of the data itself.

Finally, at the output stage, consumers may choose to opt-out of receiving personalized recommendations, thereby reducing the potential impact of biased or intrusive decision-making. In this circumstance, the data may still be used to train more general models. This case in particular may have implications with respect to medical or health information where information of an individual can improve the lives of others through models while still retaining an individuals' right to avoid the outcomes of the model. These examples highlight the importance of providing consumers with opt-out rights at each stage of the IPO model to protect their privacy while considering the potential consequences on AI system performance.

3.4 Conclusion

As discussed in our landscape analysis, many regulatory agencies such as the CFPB, EEOC, and HUD largely focus on the outputs of a system—especially with respect to discriminatory harms. In addition, while many such bodies do consider some inputs of importance, particularly with respect to prohibitions on protected characteristics, processing as a stage is largely overlooked. Opt-out and access rights are not presented holistically as to where in the data processing pipeline they may have the most impact for consumers and why certain rights are enforced at specific stages. That said, regulatory action is increasingly encompassing all stages. The FTC's recent enforcement actions against Ever and WW required not only the deletion of data collected without consent but the models as well.³

The effectiveness of the CPPA's regulations to protect consumer privacy as technology evolves will rely on the Agency's ability to identify the applicable points (such as prior to collection, prior to a given processing pipeline, or prior to delivery of outcome) within the lifecycle for a given ADM-driven decision-making system. By carefully considering the risks associated with each ADM system, the CPPA can develop and enforce robust privacy protections that are tailored to the specific needs of California consumers, striking a balance between privacy rights and the benefits of AI technologies.

³ See generally: Staff, the Premerger Notification Office, and Stephanie T. Nguyen. "FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology." *Federal Trade Commission*, 18 Sept. 2021, <https://www.ftc.gov/news-events/news/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse-facial-recognition-technology>; <https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers-illegally-collecting-kids-sensitive>.

4. Recommendation 2: Shared-Use Data

4.1 Recommendation

We recommend the CPPA explicitly consider adopting regulations regarding shared-use data (as initially considered in the CCPA regarding 'households') which has largely been omitted from other rules and regulations. When doing so, CPPA should address inputs as opposed to solely focusing on outputs of ADM systems.

4.2 Background

Shared-use data is information that is being collected by a device that may belong to one individual, about another individual. This poses a significant challenge since the individual that is not the owner of the device, or does not have an account on that device, may not have consented to the information being gathered on them or may not even know about the information that is being collected about them. In initial regulatory drafts by the CCPA, this issue was addressed under the topic of 'household' information. According to the California Consumer Privacy Act, a "'household' means a group, however identified, of consumers who cohabitate with one another at the same residential address and share use of common devices or services."⁴ Further, the CCPA defines "aggregate consumer information" as "information that relates to a group or a category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device."⁵ In the CPPA's original proposed regulations a 'household' is defined as "a person or group of people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier."⁶ The definitions and discussion of 'households' and 'household information' are relevant to the discourse regarding regulation to protect consumers' access and opt-out rights, specifically when it comes to shared-use data. One example of such a regulation would be the inclusion of a section explicitly reaffirming the access and opt-out rights of consumers with regard to decisions about themselves, even when the data was originally collected from someone else.

4.3 Examples

A few examples that illustrate the importance of protecting the access and opt-out rights for consumers and their shared-use data are:

- Location data from one party or individual could be used to pinpoint others' location without their consent.

⁴ California Legislative Information. Civil Code section 1798.140(q). November 2020.
https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

⁵ California Legislative Information. Civil Code section 1798.140(b). November 2020.
https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

⁶ California Privacy Protection Agency. Title 11. Law. Division 6. California Privacy Protection Agency. Chapter 1. California Consumer Privacy Act Regulations. Text of Proposed Regulations. 2022
https://cppa.ca.gov/meetings/materials/20220608_item3.pdf

- Voice assistants collecting voice data from non-primary users. Some examples may include smart home devices, smart TVs, and mobile phones.
- Smart home devices that collect music preferences of individuals residing in the same household of the individual that is the owner of the smart home device.
- Smart doorbells with cameras collecting generalized surveillance data from public spaces.
- Augmented reality glasses that belong to one individual recording public spaces and individuals without their consent (unlike virtual reality headsets that do not record the outside world).

4.4 Conclusion

We consider this authority provided via the CPPA's power to issue "regulations governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology."⁷ In particular, we note that in the CCPA, 'households' are explicitly mentioned based on the principle that one person's data can impact another person's privacy. Rather than a narrow focus on households, we recognize this gap as one that the CPPA is in a particularly important position to fill given the recognition of this principle by the People of California and lack of recognition by other jurisdictions and regulations. This issue of shared-use data is specifically related to the issue of inferences in ADM and AI. The CCPA should consider prohibiting the use of ADM systems from being able to make inferences about anyone other than an individual based on their own data. Without such specificity, at the current state, this may present a loophole for those who work to protect their individual exposure. The CPPA should consider restricting the ability of ADM to make inferences that can be made about an individual based on 'shared-use' data is critical in protecting consumers' privacy.

⁷ California Legislative Information. Civil Code section 1798.185(a)(16). November 2020.
https://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum=1798.185

5. Recommendation 3: Adopt A Taxonomy of Harms

5.1 Recommendation

We recommend that the Agency adopt a list of enumerated information privacy harms and require all companies subject to the risk assessment requirement to assess each of those harms with respect to their processing. We also recommend that the Agency adopt a list of exceptions under which companies are not required to consider a particular enumerated harm under specific circumstances.

We additionally recommend that the Agency adopt a set of standards or principles by which newly emerging harms can be assessed for inclusion on this enumerated list in the future.

5.2 Background

California Civil Code section 1798.185(a)(15) confers upon the Agency responsibility for:

“Issuing regulations requiring businesses whose processing of consumers’ personal information presents significant risk to consumers’ privacy or security, to [...] [s]ubmit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public”.

This statutory mandate leaves to the Agency significant questions about the scope of the risk assessment requirement. The questions left to be resolved through the Agency’s rulemaking process include:

- The scope of the term “significant risk to consumers’ privacy or security”, which is not further defined in the CCPA, as amended;
- The contents of the risk assessment; and
- Whether businesses that experience different kinds of risks should be subject to different requirements.

5.3 Discussion

The Agency Should Consider and Build Upon the Approaches Taken by Colorado, Connecticut, and Virginia

As we discuss in our Landscape Analysis, three other states have adopted requirements for data impact assessments in their respective state privacy statutes: Colorado, Connecticut, and Virginia. Each of those states requires that businesses conduct a data impact assessment when processing

personal data with a “heightened risk of harm to a consumer”.⁸ In particular, each of those states requires a data protection assessment in the following circumstances, and Colorado and Connecticut explicitly define “heightened risk of harm to a consumer” to include the following:

- The sale of personal data;
- The processing of “sensitive data”, as that term is defined in each statute;
- Targeted advertising;⁹
- Profiling, if that profiling involves a “reasonably foreseeable” risk of “(i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers”.

At a minimum, the CPPA should adopt this general framework of defining “significant risk to consumers’ privacy or security” for the purposes of section 1798.185(a)(15) by specifying specific cases that *per se* trigger data protection assessments (sale of personal data, processing of sensitive data, and targeted advertising¹⁰) and then further by imposing a requirement that businesses address other reasonably foreseeable risks in the context of profiling. This approach would bring California’s minimum requirements into alignment with the unanimous consensus of states that have imposed data protection assessment requirements to date.

The Agency Should Adopt a List of Risks That Must be Considered in Risk Assessments

Colorado has gone further than Connecticut and Virginia by writing into its regulations a list of 11 classes of injury that businesses must consider when conducting data protection assessments. As we discuss in our Landscape Analysis, these enumerated harms find significant support in the literature as well as in Colorado’s legal and regulatory context, and provide useful guidance for businesses seeking to comply with the data protection assessment requirement. However, as we note in the Landscape Analysis, Colorado’s list of enumerated harms is optional for businesses to consider, which significantly limits its effectiveness.

⁸ Colo. Rev. Stat. § 6-1-1309(1). Connecticut Public Act 22-15, § 8(a). Code of Virginia § 59.1-580(A).

⁹ Colorado requires targeted advertising to undergo a data protection assessment only if it presents a reasonably foreseeable risk of the listed injuries, just like for profiling.

¹⁰ With regard to targeted advertising, we note that harms associated with targeted advertising have been broadly recognized. For example, the European Union’s European Data Protection Board has issued specific guidance on “targeting of social media users” noting that such targeting “may involve uses of personal data that go against or beyond individuals’ reasonable expectations”, “may involve criteria that, directly or indirectly, have discriminatory effects”, is open to “potential possible manipulation of users”, can be “used to unduly influence individuals when it comes to political discourse and democratic electoral processes”, “may adversely affect the likelihood of access to diversified sources of information in relation to a particular subject matter”, and overall “may a chilling effect on freedom of expression, including access to information”. See Guidelines 8/2020 on the targeting of social media users, European Data Protection Board, September 2, 2020. Available at https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf.

By contrast, the enumerated harms and the factors governing whether a data protection assessment is required under the EU's GDPR are much more detailed and are binding. Under Article 35(4) of the GDPR, the national supervisory authorities have authority to adopt a *binding* "list of the kind of processing operations which are subject to the requirement for a data protection impact assessment".¹¹ As an example of the exercise of this authority, the Ireland Data Protection Commission has adopted a list of 10 specific circumstances under which a data protection impact assessment is required, including:

- "Profiling vulnerable persons including children to target marketing or online services at such persons";
- "Systematically monitoring, tracking or observing individuals' location or behaviour"; and
- "Profiling individuals on a large-scale".¹²

Unlike Colorado's regulatory list, this list is not a suggestion but instead has the force of law under Article 35(4) of the GDPR. The Ireland Data Protection Commission further lists other factors that businesses should consider when "determining if there is a high risk", including:

- "Uses of new or novel technologies";
- "Data processing at a large scale"; and
- "Processing of combined data sets that goes beyond the expectations of an individual, such as when combined from two or more sources where processing was carried out for different purposes or by different data controllers".

We recommend adopting a combination of the approaches taken by Colorado and the European Union. Specifically, we urge that the CPPA adopt a list of harms that businesses must take into account in the course of their risk assessments. We believe the list of harms found in Colorado's rules presents a strong foundation for the CPPA's use.

However, unlike Colorado but like the GDPR's approach, we recommend mandating discussion of the risks enumerated in the CPPA's regulations (i.e. making the list legally binding) to ensure that the required risk assessments cover the appropriate range of risks. If the Agency identifies that a risk should be enumerated on its list of harms, but that risk is clearly inapplicable to a particular type of processing activity, we recommend that the Agency adopt an exception allowing risk assessments for those processing activities to omit discussion of that particular enumerated risk.

¹¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, Article 35(4).

¹² Ireland Data Protection Commission (2018). "List of Types of Data Processing Operations which require a Data Protection Impact Assessment." Available at <https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Data-Protection-Impact-Assessment.pdf>

Unlike in Colorado, data protection assessments conducted pursuant to the CCPA, as amended, are required to be “[s]ubmit[ted] to the California Privacy Protection Agency on a regular basis”¹³, giving the Agency a regular opportunity to reassess which harms are suitable for mandatory inclusion with the benefit of understanding how its regulations will be applied.

Finally, while this recommendation specifically addresses enumerating harms in the context of algorithmic impact assessments, we also urge the Agency to adopt, for internal use, a list of risks that arise from the processing of personal data more broadly. Formulating such a list may be of use when the Agency considers the exercise of its other regulatory functions.

The Agency Should Adopt Clear Principles by Which Additional Harms May Be Enumerated

We recognize the fast-developing nature of information privacy risks and specifically of the AI systems powering forms of automated decisionmaking that have the potential to generate novel risks in the future. We urge the CPPA to regularly update the regulatory list of enumerated harms into the future. However, to avoid the future perception of these updates as ad-hoc regulatory measures, we recommend that the Agency provide as much forward guidance as possible in the form of a set of coherent principles that will guide which harms will be added to the list of enumerated harms in the future.

¹³ California Civil Code section 1798.185(a)(15).

6. Recommendation 4: Impact Assessments & Trade Secrets

6.1 Recommendation

*We recommend that with respect to impact assessments all companies subject to the CPPA's jurisdiction be required to conduct appropriate risk impact assessments **regardless of whether they are submitted to the CPPA.***

6.2 Background

Under Cal. Civil Code § 1798.185(a)(15)(b), the CPPA may: “[i]ssu[e] regulations requiring businesses whose processing of consumers’ personal information presents significant risk to consumers’ privacy or security” to submit to the CPPA regular risk and impact assessments related to that processing and the consumer privacy risks thereof. However, the title also notes that “[n]othing in this section shall require a business to divulge trade secrets.”

In such a rapidly evolving space where technological and academic advancement provide critical edges to businesses’ functions, we are concerned that this trade secret provision will introduce ambiguity. In the event of an enforcement action against a company requiring review of completed impact assessments, their effectiveness may well be reduced due to a lack of disclosure if important information relates to the internals of such systems which may be judged as trade secrets.

This tension between disclosure for auditing and maintenance of trade secrets is not new. In the recent Algorithmic Accountability Act of 2022, introduced by Sen. Ron Wyden (D-OR), this issue is addressed by ensuring that summary reports are always required.¹⁴ However the bill also ensures that the only information made public is “to establish a repository of information where consumers and advocates can review which critical decisions have been automated by companies along with information such as data sources, high level metrics and how to contest decisions, where applicable.”¹⁵

While the bill did not pass in the last Congressional session, it addressed the issue by mandating disclosure to the FTC with heavier restrictions on what information may be disclosed more broadly.

¹⁴ “Wyden, Booker and Clarke Introduce Algorithmic Accountability Act of 2022 to Require New Transparency and Accountability for Automated Decision Systems.” *U.S. Senator Ron Wyden of Oregon*, 3 Feb. 2022, <https://www.wyden.senate.gov/news/press-releases/wyden-booker-and-clarke-introduce-algorithmic-accountability-act-of-2022-to-require-new-transparency-and-accountability-for-automated-decision-systems?peek=BH793HGzEX7gimi20t7HiHEg8n9b3vET476N7MsTy%2BcOuyHe>.

¹⁵ “The New 5-Step Approach to Model Governance for the Modern Enterprise.” *AI Infrastructure Alliance*, 27 May 2022, <https://ai-infrastructure.org/the-new-5-step-approach-to-model-governance-for-the-modern-enterprise/>.

In contrast, the Cal. Civil Code provision prevents some information from being collected by the CPPA in the first place.

6.3 Example

Consider the scenario where due to a new form of ADM technology, disclosure about a given impact assessment would require disclosure of a fundamentally new technology. In this scenario—where a trade secret would be disclosed—the Cal. Civil Code is not instructive with respect to what information is necessary then to disclose.

The CPPA could well craft impact assessments that avoid such information entirely, but by doing so, it is also possible that the full picture of risk is not being disclosed to the agency given the novelty of the technology. To quote a recent study discussing the usefulness of third-party audits, “The mere insistence for audits is not enough – in particular, specific interventions will be necessary to allow for the effective participation of third parties, who play a critical role yet continue to face serious and often debilitating challenges when engaged in their work.”¹⁶ Yet specific interventions necessary to make useful the audits may require knowledge about the specifics which may overlap with trade secrets.

In such a circumstance, rather than watering down the impact assessment requirements, we believe that the appropriate action is to mandate completion and archiving of the desired impact assessments even if at a given time it may not be mandated to be disclosed to the CPPA. That way, there is an auditable trail in the event that a new or unforeseen harm is discovered as a result of the novel technology. Once a harm is discovered or a given ADM system is perceived to have a significant risk, then the CPPA may investigate, and the history of impact assessments in such a situation would be valuable.

6.4 Conclusion

In the event of new harms, we believe that it is prescient of the CPPA to mandate completion of impact assessments even if for reasons such as trade secret protection, the outputs of those assessments may not immediately be disclosed. Doing so creates a fall-back for investigation and remediation in the event of new and unforeseen harms without contradicting the provisions of the Cal. Civil Code.

¹⁶ Inioluwa Deborah Raji, Peggy Xu, Colleen Honigsberg, and Daniel Ho. Outsider oversight: Designing a third party audit ecosystem for ai governance. In Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society, AIES '22, page 557–571, New York, NY, USA, 2022. Association for Computing Machinery. ISBN 9781450392471. doi: 10.1145/3514094.3534181. URL <https://doi.org/10.1145/3514094.3534181>

From: Richards, Michael [REDACTED]
Sent: Monday, March 27, 2023 4:59 PM
To: Regulations
Cc: Crenshaw, Jordan; Eggers, Matthew J
Subject: PR 02-2023
Attachments: PR 02_2023_Chamber.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender [REDACTED]

To whom it may concern –

Please see the following comments from the U.S. Chamber of Commerce regarding the Preliminary Rulemaking Activities on Cybersecurity Audits, Risk Assessments, and Automated Decision-making.

Please let me know if you have any questions regarding anything attached.

V/r

Michael Richards

Policy Director
Chamber Technology Engagement Center
U.S. Chamber of Commerce
Cell: [REDACTED]



www.americaninnovators.com
[REDACTED]

March 27, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

To Whom It May Concern:

Re: Notice of Proposed Rulemaking, California Privacy Protection Agency (March 27th, 2023)

The U.S. Chamber of Commerce's Technology Engagement Center ("Chamber" or "C_TEC") appreciates the opportunity to provide public comment on its Proposed Rulemaking to amend California's privacy regulations to implement the California Privacy Rights Act ("CPRA"). Consumers deserve strong privacy protections and innovative products and services. Businesses need certainty, uniformity, and protection. It is, for this reason C_TEC supports national privacy legislation that does all these things. The California Privacy Protection Agency's ("CPPA" or "Agency") proposed rules will impact businesses beyond the borders of the Golden State, which is why we believe it is essential that the agency looks for every opportunity to harmonize with already implemented policies, such as GDPR and the provisions of other state privacy laws. Therefore, we offer the following comments promoting consumer protection and business clarity that fall within the limits of CPRA.

I. Cybersecurity Audits

Among other things, the proposed rulemaking calls on CCPA to issue regulations requiring businesses "whose processing of consumers' personal information presents significant risk to consumers' privacy or security" to perform annual cybersecurity audits, "including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent."

A large number of businesses conduct cybersecurity audits either because of a legal obligation or as a best practice. Any new regulation in this area should have sufficient flexibility to allow businesses to align their existing auditing programs and processes with requirements that the agency develops. In addition, CPPA should expressly allow businesses to leverage industry-led, widely accepted cybersecurity best practices, frameworks, and standards as a basis for regulatory and legal liability safeguards.¹

¹ The U.S. Chamber of Commerce's January 2023 comment letter to the New York Department of Financial Services on the department's second amendment to its cybersecurity requirements for financial services companies. This letter is available upon request.

Trigger. CPPA should ensure that the trigger for a cybersecurity audit is distinct from businesses' assessments relating to consumer privacy risks. The trigger for a cybersecurity audit should be based on a significant cybersecurity incident consistent with the definition of a covered cyber incident under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (P.L. 117-113).² CPPA should avoid overly broad interpretations of what constitutes a significant risk. The statutory text supports this. Section 1798.185(a)(15) of the CPRA directs CPPA to develop regulations relating to cybersecurity audits and risk assessments for the “processing of personal information [that] presents significant risk to consumers’ ... security.” Without a finely tuned definition or definitions, businesses could be forced into considerable auditing activity—in essence, pulling business resources away from managing the cybersecurity of both their enterprises and the consumers they serve.

CPPA should also distinguish between security risks and privacy risks, and limit the trigger for auditing requirements to the former. As noted at the outset, many businesses already perform cybersecurity audits. Standards and best practices for cybersecurity audits focus on security risks, which are different from privacy risks. Different frameworks and processes for identifying, classifying, and remediating cybersecurity and privacy risks exist for this very reason.³

It is important to spotlight that the statutory text reflects the same approach. Indeed, section 1798.185(a)(15) directs the agency to develop standards relating to processing that presents “significant risks” to “privacy or security” and contemplates separate vehicles for doing this—(1) a cybersecurity audit that includes “the factors to be considered in determining when processing may result in significant risk to the security of personal information”; and (2) a risk assessment, which includes the processing of sensitive information and sets forth a high-level framework similar to data protection requirements under other state, as well as global, data privacy frameworks.

Scope. The statute calls for an annual cybersecurity audit. Regulations should be reasonable in scope, covering the security program for the relevant segment of an organization that processes consumers' personal information. This is a common approach of widely recognized standards, such as NIST special publications.

² <https://www.congress.gov/bill/117th-congress/house-bill/2471>

³ National Institute of Standards and Technology (NIST) has developed frameworks for managing cybersecurity and privacy risks.

The regulations should not mandate audits for low-impact or insignificant cyber activity. Such a mandate would place businesses in a perpetual state of unproductive auditing that would likely conflict with related examinations and/or requirements. Requiring multiple audits would generate substantial activity and costs but yield little to no return on security and resilience. In short, CPPA should prioritize harmonizing its regulation regarding cybersecurity audits with existing laws and requirements that businesses already follow.

CPPA asks stakeholders whether they recommend that officials consider the cybersecurity audit models created by other laws as the regulations are written. Existing laws and regulations typically apply to specific sectors. The Chamber recommends that CPPA officials develop regulations that permit the entities that are required to abide by sector-specific auditing requirements and existing federal guidelines to leverage these for their compliance with any CPPA requirement. Existing regulations include nuanced considerations and enforcement mechanisms that are specific to each sector and are neither easy nor prudent to generalize across industry. California policymakers should maintain, and not duplicate, these existing regulations for entities that are covered under their provisions to prevent regulatory overlap.

One company told the Chamber that the Health Insurance Portability and Accountability Act of 1996 (HIPAA) tasks the Department of Health and Human Services (HHS) with creating regulations to protect the privacy and security of certain health information, including Personal Health Information (PHI) and now e-PHI. HIPAA includes the Privacy Rule and the Security Rule, which set standards for HIPAA-regulated entities (e.g., health care payers) to follow. HIPAA-regulated entities follow detailed privacy and security provisions to protect data, including the use of the minimum necessary data standard and specific data protection steps. HIPAA-regulated entities also adhere to breach notification and data use requirements.

HIPPA is unlikely to apply to entities outside the health care sector. Yet HIPPA illustrates how CPPA officials can align their cybersecurity auditing regulation with existing laws and rules. Worth noting, too, is that such thinking lines up well with the Biden administration's recent *National Cybersecurity Strategy*, which calls for harmonizing new and existing regulations as a means of strengthening U.S. cybersecurity. The White House stresses that effective regulation minimizes the costs and burdens of compliance, "enabling organizations to invest resources in building resilience and defending their systems and assets."⁴

⁴ <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>

California Civil Code § 1798.185(a)(15)⁵

(15) Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to:

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

(B) **Submit to the California Privacy Protection Agency on a regular basis a risk assessment** with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public. Nothing in this section shall require a business to divulge trade secrets [emphasis added].

Process. An auditing process needs to be workable. The regulations should grant businesses the flexibility to use either internal cybersecurity auditing processes or retain independent third-party auditors as opposed to mandating one over the other. With respect to internal audits, this concept is not new to California. The state's insurance code permits internal audits that are organizationally independent.⁶

In response to Civil Code § 1798.185(a)(15)(A), private organizations that are already performing annual or semiannual cybersecurity audits (e.g., based on HITRUST or the Payment Card Industry Data Security Standard) will likely want to leverage work they are already doing and any subsequent certifications.

Also, CPPA's notice asks to what degree do other legally required cybersecurity audits, assessments, evaluations, or best practices align with the processes and goals articulated in California Civil Code § 1798.185(a)(15)(A). A firm stressed to the

⁵ https://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum=1798.185

⁶ CA Ins Code § 900.3 (2019)
<https://law.justia.com/codes/california/2019/code-ins/division-1/part-2/chapter-1/article-10/section-900-3>

Chamber that CCPA should make reciprocity a feature of its cybersecurity audits regulation vis-à-vis cloud certification programs, such as the Federal Risk and Authorization Management Program (FedRAMP) and the State Risk and Authorization Management Program (StateRAMP). Each program is sufficient to meet the requirements of the CCPA. FedRAMP is the federal government's approach to the risk-based adoption and use of cloud services. An organization that earns a FedRAMP authorization typically completes a readiness assessment and pre-authorization prior to undergoing a full security assessment and authorization.

StateRAMP is a multi-state organization in which California is a member.⁷ StateRAMP establishes common security criteria to standardize cloud security verification, which is especially helpful to state and local governments purchasing services. Reciprocity between FedRAMP and StateRAMP provides vendors with the ability to leverage their federally approved security assessments for the StateRAMP Fast Track.⁸ Such steps are more than sufficient to provide California and its citizens assurance that an organization is undertaking the types of cybersecurity practices designed to manage cybersecurity risks identified in the CCPA.

Businesses Need Flexibility Regarding Compliance, Including Cybersecurity Audits

Missing from CCPA's proposed requirements are safeguards for businesses that demonstrate their use of existing cybersecurity programs to meet the requirements of the CCPA. Businesses with cybersecurity programs that reasonably align with these and other laws and regulations that contain cybersecurity requirements should be entitled to liability protections. CCPA should balance regulatory compliance with greater flexibility in meeting industry-recognized standards, as well as positive incentives to increase the economic security of regulated parties and California.

While far from a comprehensive listing, CCPA should deem that the following cybersecurity best practices, frameworks, standards, and programs satisfy any cybersecurity auditing requirements under the CCPA:

- The Cybersecurity Framework developed by NIST
- NIST special publication 800-171
- NIST special publications 800-53 and 800-53a

⁷ <https://stateramp.org/participating-governments>

⁸ <https://stateramp.org/blog/stateramp-fast-track>

- NIST special publication 800-218
- NIST profile of the Internet of Things Core Baseline for Consumer IoT Products (NIST Internal Report 8425)
- Cybersecurity Maturity Model Certification
- The Federal Information Security Modernization Act of 2014
- Title V of the Gramm-Leach-Bliley Act of 1999, as amended
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- The Security Assessment Framework for FedRAMP
- The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 family, information security management systems
- The ISO/IEC 30111 and 29147, coordinated vulnerability handling and disclosure
- Critical Security Controls for Effective Cyber Defense developed by the Center for Internet Security
- The Profile developed by the Cyber Risk Institute
- The Payment Card Industry Data Security Standard, as administered by the Payment Card Industry Security Standards Council

In sum, the Chamber strongly urges CPPA officials to align its regulation related to cybersecurity audits with existing ones as well as to leading industry best practices. CPPA should also collaborate closely with businesses to determine the most effective and efficient cadence for cybersecurity auditing and reporting.

II. Risk assessments

1. What laws or other requirements that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require risk assessments?

C_TEC would like to highlight that many organizations and companies are already complying with various laws that require privacy risk assessments. The regulations should leverage existing best practices (such as the NIST Privacy Framework) and existing regulatory standards, including the EU General Data Protection Regulation (effective May 2018) and other state privacy laws, such as those enacted in Virginia, Connecticut, and Colorado.

a. To what degree are these risk-assessment requirements aligned with the processes and goals articulated in Civil Code § 1798.185(a)(15)(B)?

The CPRA sets out the rulemaking goals for risk assessments to include assessing “whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing . . . against the potential risks to the rights of the consumer associated with that processing.” These goals align with the data protection assessment requirements in the privacy laws enacted in Virginia, Connecticut, and Colorado. Taking the Virginia CDPA as an example: this standard requires that businesses (i.e. controllers) conduct and document a data protection assessment of...processing activities involving personal data, and more specifically, the processing of sensitive data and any processing activities involving personal data that present a heightened risk of harm to consumers. The provisions further require that assessments also identify and weigh the benefits [to the controllers] against the potential risks to the rights of the consumers, as mitigated by safeguards that can be employed to reduce such risks. The Connecticut and Colorado standards are identical. This clearly advances the goals of the CPRA.

Moreover, this standard supports a risk-based approach, which is the most meaningful way to advance consumer protections and ensure that a risk assessment doesn’t become a “check the box” exercise.. Notably, we are not aware of any existing mandates that call for risk assessments for every processing activity. The GDPR, for instance, mandates data protection assessments when processing “is likely to result in a high risk to the rights and freedoms of a natural person.” See Art. 35(1). Such high-risk processing activities include profiling for consequential decisions, the large-scale processing of sensitive data, and the systemic and large-scale monitoring of publicly accessible areas. Art. 35(3).

The CPRA regulations can meaningfully advance consumer privacy standards by aligning the risk assessment requirement with these standards and the NIST Privacy Framework. This will incentivize meaningful assessments of the most impactful processing activities while simultaneously harmonizing.

e. Would you recommend the Agency consider the risk assessment models created through these laws, requirements, or best practices when drafting its regulations? Why, or why not? If so, how?

We support impact assessments for high-risk processing activities and align such risk assessment models to enable efficient and consistent compliance by organizations and consistent protections for consumers.

We note that existing laws currently apply to specific industries and recommend that policymakers refer to sector-specific regulation and existing federal guidelines and enforcement as being compliant with the CPRA’s risk assessment requirements.

Existing regulations include considerations and enforcement specific to those industries, and policymakers should maintain and enable the continuation of these regulations for entities that fall under their provisions and avoid regulatory overlap.

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?

As noted above, we fully support a harmonized approach to privacy risk assessments. Accepting risk assessments completed in compliance with other laws such as the EU GDPR or Colorado Privacy Act will provide the following:

- Efficiency as businesses will not need to navigate a patchwork of requirements, allowing them to implement more consistent policies and processes.
- Reflection of the global context in which data is processed -- that data processing is rarely limited to individuals located in one state or geographic area; and
- Alignment with current regulatory trends to accept risk assessments conducted in compliance with comparable laws of other jurisdictions.

Benefits to consumers include:

- More efficient response time by companies to consumer rights requests.
- Consistent protections for consumers, regardless of where a consumer resides.
- More consistent risk evaluation and mitigation.

This harmonized approach is something that both Virginia, Colorado and Connecticut have recognized the benefits of, as they have included stipulations which allow them to accept privacy risk assessments completed in compliance with the laws of other jurisdictions:

Sec. 59.1-580, E, of the Virginia CDPA, allows that data protection assessments conducted for the purpose of compliance with other laws or regulations be sufficient to comply with Virginia's privacy risk assessment requirement, provided the assessments have a reasonably comparable scope and effect."

Section 6-1-1309(5) of the Colorado Privacy Act provides that "a single data protection assessment may address a comparable set of processing operations that include similar activities."

6. In what format should businesses submit risk assessments to the Agency? In particular: (a) if a business 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, and (iii) How often should they be submitted?

At the outset, we appreciate that the Agency is considering permitting summaries of risk assessments to fulfill the submission requirement rather than requiring the submission of each risk assessment conducted. This is an appropriate balance of resources, both for the Agency as it reviews the submission and for businesses conducting them. On the latter point, we note that risk assessments are most impactful when they present an opportunity for a full discussion and consideration of the processing activities and ways to mitigate any identified risks of harm. An overbroad requirement to submit each risk assessment would chill the free and open discussion necessary to make this process meaningful. Moreover, risk assessments need to involve various internal stakeholders, including legal counsel. Thus, a mandate to turn over the assessment could chill the ability of legal counsel to advise in the process due to concerns that any privilege could be vitiated from the compelled submission.

In terms of format and procedures for summary submissions, the Agency should consider requirements that recognize that the summaries may be of a signal assessment that addresses comparable sets of processing for similar activities.

III. Automated Decisionmaking

1. What laws requiring access and/or opt-out rights in the context of automated decisionmaking currently apply to businesses or organizations (individually or as members of specific sectors)?

At the outset, we note that the CPRA itself does not confer an opt-out right related to automated decision-making. The statutory text is clear on the opt-outs authorized, which is for sales and sharing of personal data. While the CPRA does state that the Agency is authorized to engage in rulemaking with respect to an “opt-out right” for automated decision-making, this provision raises constitutional questions worth noting regarding the broad nature of the delegation of authority⁹.

If the Agency does move forward despite these issues and creates an opt-out right through regulations, it should be guided by two complementary goals: ensuring the opt-out right is meaningful to consumers without disrupting beneficial and low-risk uses of automated decision making and that it is interoperable with other states that

^{9 9} *Gerawan Farming, Inc., v. Agricultural Labor Relations Bd.*, 405 P.3d 1087, 1100 (CA. Sup. Ct. 2017) (citing *Carson Mobilehome Park Owners’ Assn. v. City of Carson*, 672 P.2d 1297, 1300 (Ca. Sup. Ct. 1983)).

have enacted opt-outs. The Agency can achieve both goals by following the approaches in the Virginia, Colorado, and Connecticut privacy laws, which have all incorporated automated decision-making opt-outs limited to automated decision-making used for profiling in furtherance of “decisions that produce legal or similarly significant effects,” California’s approach should be informed by and consistent with this emerging norm in these three state laws. This balances the opt-out right to empower consumers to exercise their choice for legal decisions or otherwise similarly consequential profiling through the use of automated decision-making, while preserving clearly benign and routine uses of automated decision-making that enhance the customer experience without implicating consequential decisions. It would also avoid imposing duplicative requirements, which would add unnecessary burden onto businesses without promoting consumer privacy.

2.What other requirements, frameworks, and/or best practices that address access and/or opt- out rights in the context of automated decisionmaking are being implemented or used by businesses or organizations (individually or as members of specific sectors)?

We believe it is important to clarify that companies, for the most part, don’t have requirements, frameworks, or best practices that specifically address access/opt-out requirements when it comes to the use of low-risk automated decision-making. These types of tools which we interact with every day, such as spellcheck, have little to no risk associated with their use, and requiring access or opt-out rights for such tools would be burdensome for users.

C_TEC would like to highlight that there continues to be a significant number of efforts in developing Artificial Intelligence / Machine Learning standards and frameworks, which look to address the development and use of high-risk automated decision-making. These efforts include the recently released National Institutes of Standards and Technology (NIST) AI Risk Management framework created through a collaborative and multi-stakeholder process. Since the framework was published (January 2023), many organizations have sought to utilize NIST’s framework. We strongly suggest that the CPPA look at NIST’s efforts. It is also important to highlight that NIST’s previous work developing Cybersecurity and Privacy Frameworks has become the gold standard in guiding industry practice.

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

- a. *How is “automated decisionmaking technology” defined? Should the Agency adopt any of these definitions? Why, or why not?*

To succeed in creating a regulatory framework for the use of Automated Deployment Technology, it is imperative that there be a clear legal definition that provides precise legal certainty and harmonizes with others. This is why we believe it is important for alignment with federal agency guidance and standards development groups that continue to advance work, including definitions, in this space. This includes ongoing AI initiatives around best practices, including the NIST work groups developing voluntary AI Risk Management guidance and standards to define and measure types of bias in AI. We also stress that it is essential for definitions to be precise and align with terms and standards developed by established consensus-based entities.

4. How have businesses or organizations 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.

C_TEC would like to highlight that the use of Automated Decisionmaking Technologies (ADT) continues to become more prevalent within businesses and organizations as they provide essential efficiencies, especially to small businesses. C_TEC released a report last year which indicated that 27%¹⁰ of small businesses currently plan to utilize artificial intelligence in their practices. Using ADT and data analytics is essential in allowing small businesses to compete by streamlining important tasks like hiring and tailoring services.

5. What experiences have consumers had with automated decision-making technology, including algorithms? What particular concerns do consumers have about their use of businesses' automated decisionmaking technology? Please provide specific examples, studies, cases, data, or other evidence of such experiences or uses when responding to this question, if possible.

C_TEC would like to highlight that consumers interact with automated decision-making technologies every day, which provide a constant benefit to them. From navigation software that provides consumers with the most time-efficient directions to their destination, to digital calendars, which update consumers on when they should leave their current location to meet their following obligation

¹⁰ <https://americaninnovators.com/wp-content/uploads/2022/08/Empowering-Small-Business-The-Impact-of-Technology-on-U.S.-Small-Business.pdf>

based on current traffic patterns. At the Cleveland Clinic AI is being used to “identify and triage the sickest COVID-19 patients, allowing its physicians and nurses to allocate resources effectively and provide more personalized care.”¹¹ The use of technology is providing enormous benefits to society, and its utilization assists consumers by providing them with enhanced accuracy, cost savings, and overall efficiencies in their daily lives.

7. How can access and opt-out rights with respect to businesses’ use of automated decisionmaking technology, including profiling, address algorithmic discrimination?

Having excellent and robust data is the foundation for addressing algorithmic discrimination within ADT. For this reason, we would like to highlight the importance of the use of data such as race/ethnicity for the purpose of preventing bias. Regulators should also look at other ways to provide incentives, such as safe harbors to companies and organizations proactively looking to prevent bias that may result from the use of algorithms, by looking at specific impacts on different user groups, including minority groups.

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?

We believe it is important for regulators to understand that the risks, concerns, and benefits in relation to the use of the technology vary depending on specific sectors. Therefore, it is essential for the agency to defer to those sector-specific regulating agencies when addressing potential concerns regarding the use of the technology.

We continue to stress that each sector to look for harmonization with others on critical issues in the development of technology, as a patchwork approach could create unnecessary compliance burdens. This issue is currently being seen as different CA agencies promulgating rules on automated decision systems — CA Civil Rights Council is in the process of its rulemaking to regulate automated decision systems, in addition to what the CPPA is expected to put forth. We are strongly concerned that this presents issues of overregulation, inconsistent standards for

¹¹ https://www.uschamber.com/assets/documents/CTEC_AICommission2023_Report_v5.pdf

businesses subject to varying rules, and confusion for the consumers they seek to protect.

Regarding opt-out rights with respect to business, we believe it is important to highlight that the use of automated decision-making by businesses, even in “high-risk” uses of the technology, is highly beneficial to consumers. Things such as healthcare providers who uses someone’s geolocation to determine the closest medical facility, to banks using the ADT for fraud detection. It is important to highlight that opt-out requirements of such tools could significantly harm consumers.

Conclusion:

The Chamber stands ready to work with you to ensure that the CPPA protects the laudable goals of giving consumers the right to access, correct, delete, and opt-out of sharing information, among others. At the same time, we urge the Agency to carefully follow the statutory text, which will provide the certainty needed for a thriving innovation economy.

Sincerely,



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

From: Anderson, Meghan G. (Fed) [REDACTED]
Sent: Tuesday, May 2, 2023 1:54 PM
To: Regulations
Subject: PR 02-2023 - Comments from National Institute of Standards and Technology
Attachments: NIST Privacy Engineering Program_PR 02-2023.pdf; Attachment A_PRAM.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear California Privacy Protection Agency,

Please find attached the National Institute of Standards and Technology (NIST) Privacy Engineering Program's comments in response to the Invitation for Preliminary Comments on Proposed Rulemaking. Also attached is "Attachment A_PRAM," which is referenced to in our comments.

We appreciate the opportunity to submit! Please let me know if you have any questions.

Thank you,
Meghan

--

Meghan G. Anderson

Privacy Risk Strategist | Privacy Engineering Program

U.S. Department of Commerce | National Institute of Standards and Technology

Tel: [REDACTED]

E: [REDACTED]

Catalog of Problematic Data Actions and Problems

This catalog is a *non-exhaustive, illustrative* set of problematic data actions and problems that individuals could experience as the result of data processing or their interactions with systems, products, or services.

Problematic Data Actions

Appropriation: Data is used in ways that exceed an individual's expectation or authorization (e.g., implicit or explicit). Appropriation includes scenarios in which the individual would have expected additional value for the use given more complete information or negotiating power. Privacy problems that appropriation can lead to include loss of trust, loss of autonomy, and economic loss.

Distortion: Inaccurate or misleadingly incomplete data is used or disseminated. Distortion can present users in an inaccurate, unflattering, or disparaging manner, opening the door for stigmatization, discrimination, or loss of liberty.

Induced Disclosure: Induced disclosure can occur when individuals feel compelled to provide information disproportionate to the purpose or outcome of the transaction. Induced disclosure can include leveraging access or rights to an essential (or perceived essential) service. It can lead to problems such as discrimination, loss of trust, or loss of autonomy.

Insecurity: Lapses in data security can result in various problems, including loss of trust, exposure to economic loss and other identity theft-related harms, and dignity losses.

Re-identification: De-identified data, or data otherwise disassociated from specific individuals, becomes identifiable or associated with specific individuals again. It can lead to problems such as discrimination, loss of trust, or dignity losses.

Stigmatization: Data is linked to an actual identity in such a way as to create a stigma that can cause dignity losses or discrimination. For example, transactional or behavioral data such as the accessing of certain services (e.g., food stamps or unemployment benefits) or locations (e.g., health care providers) may create inferences about individuals that can cause dignity losses or discrimination.

Surveillance: Data, devices or individuals are tracked or monitored in a manner disproportionate to the purpose. The difference between a benign action and the problematic data action of surveillance can be narrow. Tracking or monitoring may be conducted for operational purposes such as cybersecurity or to provide better services, but it can become surveillance when it leads to problems such as discrimination; loss of trust, autonomy, or liberty; or physical harm.

Unanticipated Revelation: Data reveals or exposes an individual or facets of an individual in unexpected ways. Unanticipated revelation can arise from aggregation and analysis of large and/or diverse data sets. Unanticipated revelation can give rise to dignity losses, discrimination, and loss of trust and autonomy.

Unwarranted Restriction: Unwarranted restriction includes not only blocking access to data or services, but also limiting awareness of the existence of data or its uses in ways that are disproportionate to operational purposes. Operational purposes may include fraud detection or other compliance processes. When individuals do not know what data an entity has or can make use of, they do not have the opportunity to participate in decision-making. Unwarranted restriction also diminishes accountability as to whether the data is appropriate for the entity to possess or it will be used in a fair or equitable manner. Lack of access to data or services can lead to problems in the loss of self-determination category, loss of trust, and economic harm.

Problems

Dignity Loss: Includes embarrassment and emotional distress.

Discrimination: Unfair or unethical differential treatment of individuals whether singly or as a group arising from the processing of data.

Economic Loss: Can include direct financial losses as the result of identity theft or the failure to receive fair value in a transaction.

Loss of Self Determination

- **Loss of Autonomy:** Includes losing control over determinations about information processing or interactions with systems/products/services, as well as needless changes in ordinary behavior, including self-imposed restrictions on expression or civic engagement.
- **Loss of Liberty:** Incomplete or inaccurate data can lead to improper exposure to arrest or detainment. Improper exposure or use of information can contribute to abuses of governmental power.
- **Physical Harm:** Physical harm or death.

Loss of Trust: The breach of implicit or explicit expectations or agreements about the processing of data. These breaches can diminish morale or leave individuals reluctant to engage in further transactions potentially creating larger economic or civic consequences.

Worksheet 1: Framing Organizational Objectives and Privacy Governance

This worksheet is intended to capture the organizational environment in which the system/product/service is being developed in order to support the development and implementation of appropriate privacy capabilities and increase trust in the organization's system/product/service. There is no right way to fill out the worksheet as all of the information may not exist. For example, an organization may not have an enterprise risk management strategy or the strategy may not address privacy.

Task 1: Frame Organizational Objectives

Capturing the mission/business objectives and functional capabilities for the system/product/service help in understanding its purpose in order to determine how to respond to identified privacy risks and support the selection of controls that can mitigate privacy risks while optimizing performance. Identifying how you might highlight or market any privacy protections will help to ensure that your assessment and control selection provide a basis of evidence for these claims and demonstrate the trustworthiness of your system/product/service.

1. Describe the mission/business needs that your system/product/service serves.

2. Describe the functional needs or capabilities of your system/product/service.

3. Describe any privacy-preserving goals for your system/product/service that you may plan to highlight or market to users or customers.

Task 2: Frame Organizational Privacy Governance

Understand the governance structure for your organization by identifying privacy-related legal obligations and commitments to principles or other organizational policies. This will help you to define the privacy requirements for your system/product/service and better assess the impact of data processing on your organizational priorities, risk tolerances, and values for individuals' privacy.

1. Legal Environment: Identify any privacy-related statutory, regulatory, contractual and/or other frameworks within which the organization must operate. List any specific privacy requirements.

2. Identify any privacy-related principles or other commitments to which the organization adheres (e.g., Fair Information Practice Principles, Privacy by Design principles, ethics principles).

3. Identify any privacy goals that are explicit or implicit in the organization's vision and/or mission.

4. Identify any privacy-related policies or statements within the organization, or business unit.

5. Document your organization's risk tolerance with respect to privacy from your organization's enterprise risk management strategy.

Worksheet 2: Assessing System Design

Purpose:

Determining the risks or privacy arising from data processing or individuals' interactions with systems, products, or services requires determining the likelihood that a data action will be problematic (i.e. the processing or interaction creates the potential for problems or adverse effects on individuals either singly or as a group) and its impact (to be analyzed in *Worksheet 3: Prioritizing Risk*). The purpose of this worksheet is to identify and catalog the inputs to this risk analysis. These inputs are the data processing operations or capabilities (i.e. data actions), the data being processed or individuals' interactions with the system/product/service, and relevant contextual actors.

Tasks:

1. Define the privacy capabilities of the system/product/service (*Tab 2: System Privacy Capabilities*).
2. Map data processing within the system/product/service (see *Worksheet 2: Supporting Data Map* powerpoint).
3. Catalog general contextual actors (*Tab 3: Contextual Factors*).
4. Catalog specific data actions, data being processed, unique contextual actors, and summary issues (*Tab 4: Data Action Analysis*).

Guidance:

Data Actions	Information system operations that process data. Processing includes the full data lifecycle (e.g. collection, generation/transformation, use, disclosure, retention, disposal).
Data Action Identification	To better analyze the context applicable to each data action's risk, data actions should be described at a sufficiently granular level. For example, rather than using a high-level label such as "collection" or "retention," include more descriptive details, such as "collection from users at registration via mobile device" or "storage in an internal database." Early stages of system design may preclude the ability to capture such details, but they should be added iteratively as they become known. Developing a data map (see <i>Worksheet 2: Supporting Data Map</i> powerpoint) can be helpful in identifying data actions.
Data	Identify the data being processed at granular levels. For example, instead of the generic category label of "health information," enumerate doctor name, doctor address, medical diagnosis, etc. Data that can create risk should be considered broadly, not just as biographic information, but also transactional information, as well as how the system may influence individuals' behaviors or activities. It may become apparent that specific elements of data are increasing the privacy risk of a data action, such that implementing controls that manage these elements can decrease the privacy risk while still permitting the system to conduct its operational purpose.
Context	Context means the circumstances surrounding the system's processing of data or individuals' interactions. These circumstances, along with the associated data, contribute to whether a data action is likely to be problematic. <i>Tab 3: Contextual Factors</i> provides more guidance on identifying relevant actors. The listed actors are for illustrative purposes. Assessors should consider any actor that supports the risk assessment within their specific environment. There also may be contextual actors that are specific to a particular data action that can be captured in the specific context column in <i>Tab 4: Data Action Analysis</i> . Some actors to consider regarding specific context: -the duration or frequency of the data actions being taken by the system(s) -how visible the data actions are to the individual -the relationship between data actions and the operational purpose of the system/product/service. For example, in what manner or to what degree is the data being processed contributing to the operational purpose, particularly as that operational purpose may be understood by individuals?
Summary Issues	This column may be used to capture any summary observations about the inputs (each data action, its associated data, and general and specific contextual actors) or open questions. For example, a summary observation might be that given the nature of the organization, the type of data, and the relationship of the users to the organization, it may be concluded that the users would expect to have such data collected by the organization. Or there may be questions that are not answerable at the current stage of system design, but should be captured as their eventual determination may alter the risk assessment.

Example:

An individual wishes to use ACME IDP service to augment a social credential with identity proofing and a second authentication factor to create a stronger credential. This stronger credential will be used to access state government benefits.

Data Action	Data	Specific Context	Summary Issues
Collection from the Social Media Site	<ul style="list-style-type: none"> - Self-Asserted Full Name - Validated Email - User Profile Access 	<ul style="list-style-type: none"> - One-time action (per user) between social credential and ACME IDP, but establishes an ongoing relationship between user's social media presence and ACME IDP - Social credential linking is visible to user - Linking of social credential simplifies access to government benefits system - User profile may contain information the user considers sensitive - User profile may contain information from other users not participating in the system - User profile includes information unrelated to the purpose and operation of the system - Access to data is consented to by user 	<ul style="list-style-type: none"> - Full social credential profile access is not necessary for fulfilling operational purpose - Will users understand the eventual high-assurance credential is controlled by ACME and not by their social credential provider? - How will perception of the social media organization's privacy practices impact users' willingness to consent to this data action? - Will users understand ACME will have ongoing access to information stored in their social profiles? - Will users' social media privacy settings allow this data action?

Task 1: System Privacy Capabilities

Use the table to document the privacy capabilities of the system/product/service. The capabilities should reflect the organizational privacy requirements and marketing goals from *Worksheet 1: Framing Organizational Objectives and Privacy Governance*. Consider which of the privacy engineering and security objectives are most important with respect to your organization's mission/business needs, risk tolerance, and privacy goals or your system/product/service. Not all of the objectives may be equally important or trade-offs may be necessary among them. As the assessment is intended to be iterative, the capabilities may be updated as specific privacy risks are identified through this assessment or changes in the environment occur, including design changes to the system/product/service.

Privacy Engineering and Security Objectives:

Predictability	enabling reliable assumptions by individuals, owners, and operators about P and its processing by an information system
Manageability	providing the capability of granular administration of P, including alteration, deletion, and selective disclosure
Disassociability	enabling the processing of P or events without association to individuals or devices beyond the operational requirements of the system
Confidentiality	preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
Integrity	guarding against improper information modification or destruction, and includes ensuring information non-repudiation and source authentication
Availability	ensuring timely and reliable access to and use of information or an information system

Example:

Objective	Privacy Capability
Predictability	user, RP, and IDP can assume that the RP cannot process information about the user's relationship with the IDP
	user, RP, and IDP can assume that the IDP cannot process information about the user's relationship with the RP
Manageability	only the user can choose to disclose their attribute information to an RP
	a user can see their attribute values at an IDP prior to release to an RP, and have a mechanism to dispute inaccuracies prior to release
Disassociability	the RP can accept an authentication assertion and identity attributes without associating a user
	the IDP can transmit an authentication assertion and identity attributes without associating a user
Confidentiality	3rd parties do not have plaintext access to user credentials or attributes either at rest, or in transit
	a malicious man-in-the-middle attack will not result in a breach of personal data of the authenticating user
Integrity	RP is assured that the data is provided by a valid IDP
	RP is assured that a malicious 3rd party cannot impersonate a valid user and/or reuse prior, valid information
Availability	a remediation process is in place to help restore lost access to services and/or data to valid users

Objective	Privacy Capability
Predictability	
Manageability	
Disassociability	
Confidentiality	
Integrity	
Availability	

Task 3: Assess System Design

Catalog Context: Record contextual factors that describe the circumstances surrounding the system's processing of PI. The following categories and considerations may be helpful in capturing factors that could either increase or decrease the likelihood of a data action being problematic, but they should not limit the analysis.

Organizational: Consider

the nature of the organizations engaged in the system such as public sector, private sector or regulated industry and how these factors might impact the data actions being taken by the system(s).

the public perception about participating organizations with respect to privacy.

the nature and history of individuals' relationships with the organizations participating in the system(s).

System: Consider

the degree of connections to external systems and the nature of the data actions being conducted by those external systems such as retention, disclosure, or secondary use.

any intended public exposure of data and the degree of granularity.

the nature and history of individuals' interactions with the system(s).

the degree of similarity between the operational purpose (e.g. goods or services being offered) of this system and other systems that individuals have interacted with at participating organizations.

Individuals: Consider

what is known about the privacy interests of the individuals.

the individuals' degree of information technology experience/understanding.

any demographic factors that would influence the understanding or behavior of individuals with respect to the data actions being taken by the system(s).

Example:

Contextual Factors
Organizational
<i>System includes both state benefits agency and commercial service providers</i>
<i>Multiple privacy policies governing system</i>
<i>Public perception: high expectation of privacy with state benefits agency low expectation with social credential provider</i>
<i>Relationships: No pre-existing relationship with ACME IDP regular interactions with state benefits agency regular interactions with social</i>
System
<i>Personal information is not intended to be made public</i>
<i>New system no history with affected individuals Low similarity with existing systems/uses of social identity</i>
<i>Four parties sharing personal information: one public institution three private</i>
<i>ACME will use 3rd party cloud provider</i>
Individual
<i>High sensitivity about government benefits provided by system</i>
<i>Users exhibit various levels of technical sophistication</i>
<i>Potential user confusion regarding who "owns" the various segments of each system</i>
<i>20% of users use privacy settings at social provider</i>

Task 4: Assess System Design

Please complete the below table based on your system(s).

[illegible]

Worksheet 2: Supporting Data Map

- Worksheet 2 is used to identify the inputs to the privacy risk model, including:
 - Data actions being performed by the system
 - Data being processed by the data actions
 - Relevant contextual factors

Task 2:

- In order to identify the data actions and the data being processed it is helpful to create a data map of the system(s) to be assessed.
- The following data maps illustrate common system design diagrams, but organizations can overlay the data map on any system design artifact typically used by the organization to enable easier collaboration with system designers or engineers.
- **Note** that the scenario described in the following slides and the remainder of the worksheets is purely illustrative. It does not necessarily demonstrate a feasible or desirable federated identity solution.

Example Use Case






ACME IDP service generates a high-assurance identity credential by combining:

- The individual's (social site) online identity,
- An in-person identity proofing event at a trusted third party office (such as a UPS, FedEx location etc.), and
- A One Time Password (OTP) service to be used as a second authentication factor.




The high-assurance credential will subsequently be used to verify the identity of the individual as he or she attempts to access government benefits.

Legend

High-level data action indicator

	Collection
	Retention/Logging
	Generation/Transformation
	Disclosure/Transfer
	Disposal

Color coding to depict the operator of the data action

	ACME IDP
	Commercial third-party
	Government third-party

Generation of high-assurance credential

Social Site Credential



1. ACME collects individual's PI from social site:

- Self-asserted full name
- Validated email
- List of friends
- Profile photograph



Individual

2. ACME collects PI from individual to provision OTP:

- Name
- Address
- Cellular number



3. Individual provides hard copy documentation to third party employee for proofing and data entry to ACME:

- Driver's license
- SSN card
- Cellular number

Third Party In-person Identity Proofer

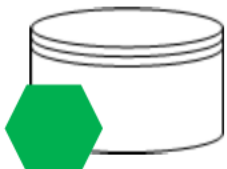


4. Third party employee enters PI into ACME's website:

- DOB
- Legal name
- Address
- SSN
- Cellular number

Third Party Cloud Hosting Service

9. ACME uses a cloud provider to store all PI and transactional information



OTP Service



5. ACME transfers PI to OTP service to create OTP account:

- Legal name
- Address
- DOB
- Cellular number

6. OTP service generates token identifier

7. OTP transfers token identifier to ACME

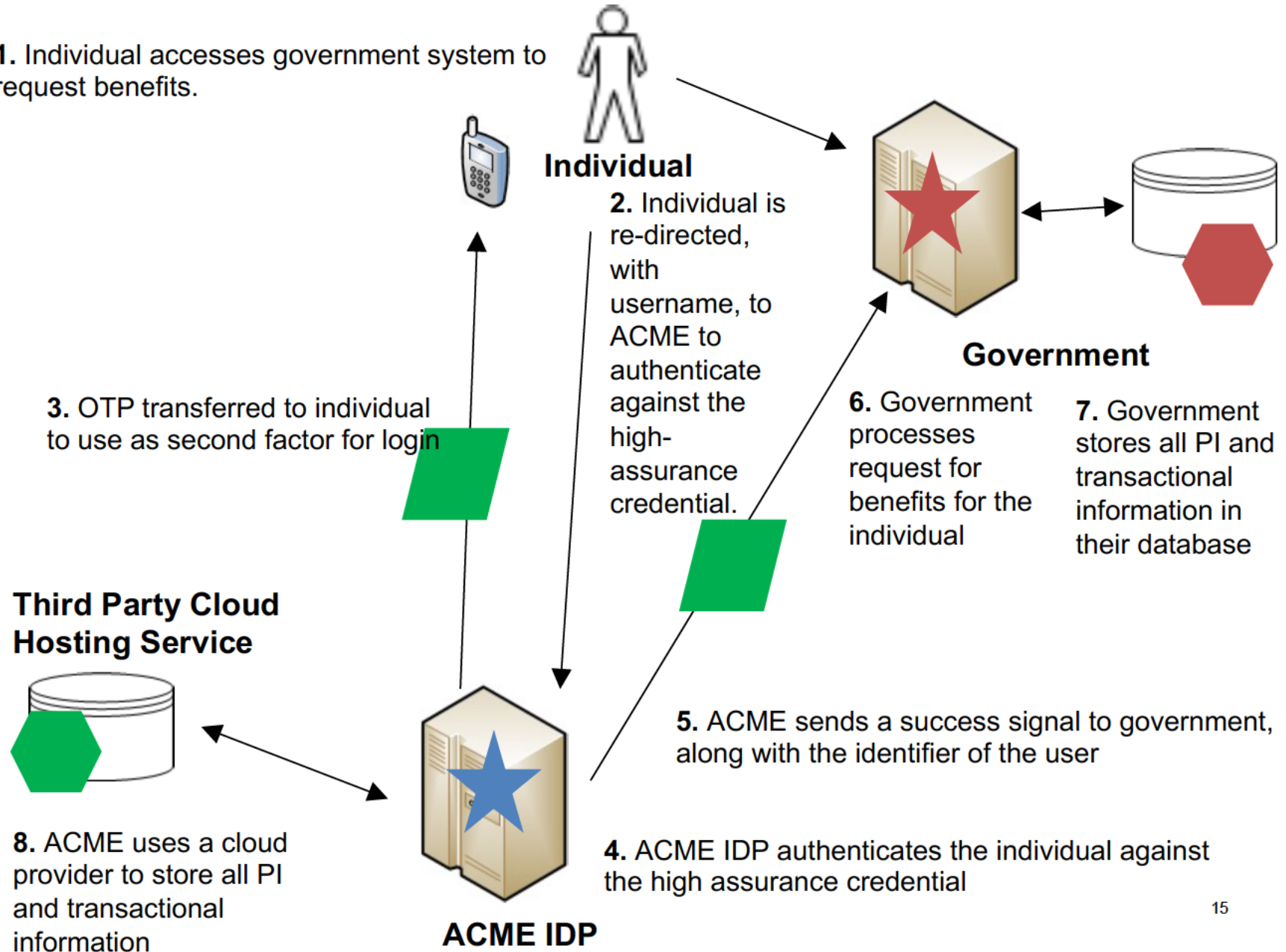
8. ACME generates high-assurance credential based on PI collected and OTP-provided token identifier

ACME IDP

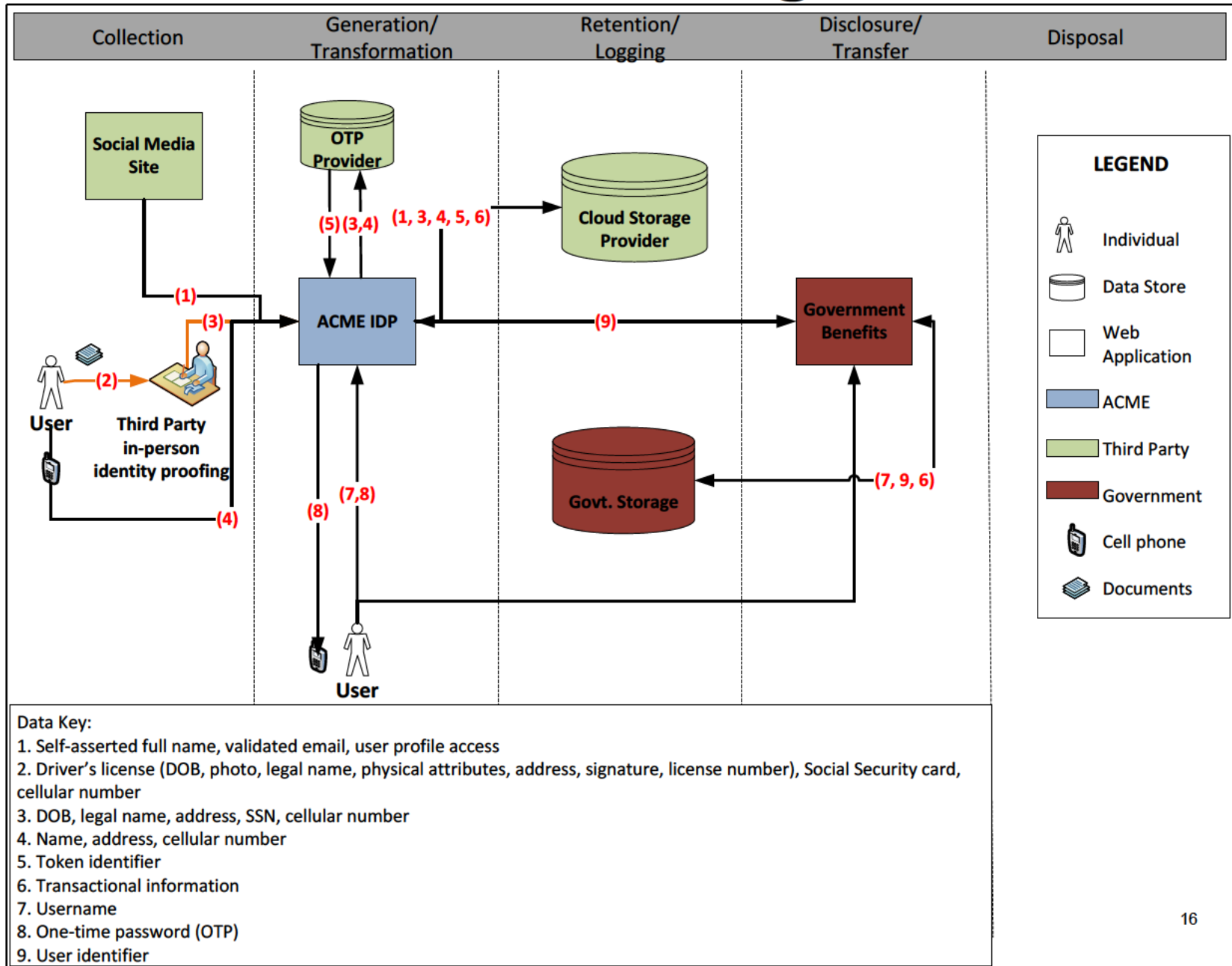


Use of credential to access benefits

1. Individual accesses government system to request benefits.



Data Flow Diagram



NIST Privacy Risk Assessment Methodology
Version: February 2019

Worksheet 3: Prioritizing Risk

Purpose:

This worksheet enables the assessment and prioritization of privacy risk in systems. It requires inputs from *Worksheet 1: Framing Organizational Objectives and Privacy Governance* and *Worksheet 2: Assessing System Design*.

Tasks:

1. Assess likelihood (*Tab 2: Likelihood*).
2. Assess impact (*Tab 3: Impact*).
3. Calculate risk (*Tab 4: Risk*).
4. Prioritize risk (*Tab 5: Risk Prioritization SAMPLE & Tab 6: Risk Prioritization INPUT*).

Task 1: Assess Likelihood**Guidance:**

Likelihood: Probability that a data action will become problematic for representative or typical individuals whose data is being processed or is interacting with the system/product/service

Assessment: Determine on a scale from 1-10 the estimated expected probability of occurrence for each potential problem for individuals with 10 being most problematic. Organizations can use any scale they prefer as long as they use the same scale throughout the process.

Prior Worksheet Inputs: Data actions and associated summary issues from Worksheet 2

Problematic Data Actions Catalog: See *Catalog of PDAP*. The catalog may be used as a way to categorize the adverse effects that could arise from the issues or questions highlighted in the summary issues column. As noted in Worksheet 2, a summary issue may alleviate rather than raise concerns about adverse effects. In that case, the summary issue should be scored as 0.

Problems for Individuals Catalog: See *Catalog of PDAP*. Problematic data actions may create the potential for more than one type of problem. However, some of the problems may have a higher likelihood of occurrence than others. If the data action ultimately is scored as risky, scoring the problems separately may help pinpoint what type of control would be most effective to mitigate the risk of the highest scored problem(s), thereby lowering the score of the data action as a whole to an acceptable level.

Example:

Data Actions	Summary Issues	Problematic Data Actions	Potential Problems for Individuals	Likelihood
Collection from the Social Media Site	Full social credential profile access (including picture and list of friends) is not necessary for fulfilling operational purpose	-Appropriation -Induced disclosure -Surveillance -Unanticipated Revelation	Dignity Loss: Information is revealed about the individual that could be embarrassing or discomfiting	7
			Loss of Autonomy: People must provide information that could be used in ways that exceed expectations	2
	Will users understand the eventual high-assurance credential is controlled by ACME and not by their social credential provider?	-This summary issue will be associated with another data action		NA
	How will perception of the social media organization's privacy practices impact users' willingness to consent to this data action?	-Induced disclosure -Surveillance	Loss of Trust: Individuals lose trust in ACME due to a breach in expectations about the handling of personal information	6

Data Actions	Summary Issues	Problematic Data Actions	Potential Problems for Individuals	Likelihood

Task 2: Assess Impact

Guidance:

Although individuals experience problems directly, it may be difficult for an organization to assess the impact of these problems. This worksheet is not intended to prevent organizations from assessing the direct impact of problems on individuals; however, should they be unable to do so, organizational impact factors as secondary costs absorbed by the organization can be used in lieu of or in addition to direct impact assessment.

Assessment Determine on a scale from 1-10 the estimated effect of each potential problem on individuals per data action on the organizational impact factors. The assigned values are added to calculate organizational impact per potential problem.

Prior Worksheet Inputs Relevant inputs from *Worksheet 1*. For example, in considering noncompliance costs, review the legal requirements or obligations identified in the legal environment box or policy statements made about privacy. In considering internal culture costs, consider the commitments to privacy principles or mission values, etc.

Organizational Impact Factors

Noncompliance Costs Regulatory fines, litigation costs, remediation costs, etc.

Direct Business Costs Revenue or performance loss from customer abandonment or avoidance, etc.

Reputational Costs Brand damage, loss of customer trust, etc.

Internal Culture Costs Impact on capability of organization/unit to achieve vision/mission. Consider impact on productivity/employee morale stemming from conflicts with internal cultural values or ethics.

Other Any other costs that an organization wants to consider.

Example:

Data Actions	Summary Issues	Problematic Data Actions	Potential Problems for Individuals	Organizational Impact Factors					Total Business Impact (per Potential Problem)
				Noncompliance Costs	Direct Business Costs	Reputational Costs	Internal Culture Costs	Other	
Collection from the Social Media Site	Full social credential profile access (including picture and list of friends) is not necessary for fulfilling operational purpose.	-Appropriation -Induced disclosure -Surveillance -Unanticipated Revelation	Dignity Loss	7	6	6	4		23
			Loss of Autonomy	7	6	8	4		25
	How will perception of the social media organization's privacy practices impact users' willingness to consent to this data action?	-Induced disclosure -Surveillance	Loss of Trust	7	6	8	7		28

Data Actions	Summary Issues	Problematic Data Actions	Potential Problems for Individuals	Organizational Impact Factors					Total Business Impact (per Potential Problem)
				Noncompliance Costs	Direct Business Costs	Reputational Costs	Internal Culture Costs	Other	
									0
									0
									0
									0

Task 3: Calculate Risk

Guidance:

Risk per Data Action Apply the risk equation to the outputs of the *Likelihood* tab and *Impact* tab to determine the estimated risk per data action. The estimated likelihood of each potential problem or individuals per data action is multiplied by its estimated impact to yield the estimated risk per potential problem. The sum of the estimated risks of each potential problem or individuals is the estimated risk per data action.

Example:

Data Actions	Potential Problems for Individuals	Likelihood	Impact	Risk per Potential Problem	Risk per Data Action
Collection from the Social Media Site	Dignity Loss	7	23	161	379
	Loss of Autonomy	2	25	50	
	Loss of Trust	6	28	168	
DA2	Economic Loss	6	32	192	317
	Loss of Autonomy	5	19	95	
	Loss of Trust	2	15	30	
DA3	Loss of Trust	6	25	150	577
	Dignity Loss	7	36	252	
	Loss of Liberty	5	35	175	
DA4	Loss of Trust	5	48	240	240
DA5	Economic Loss	6	37	222	821
	Loss of Autonomy	5	20	100	
	Discrimination	3	25	75	
	Loss of Trust	8	33	264	
	Dignity Loss	4	40	160	
DA6	Loss of Trust	5	22	110	438
	Loss of Autonomy	5	32	160	
	Dignity Loss	6	28	168	
DA7	Loss of Autonomy	8	43	344	659
	Dignity Loss	9	10	90	
	Economic Loss	7	27	189	
	Loss of Trust	4	9	36	
DA8	Loss of Autonomy	4	13	52	514
	Dignity Loss	9	32	288	
	Economic Loss	8	15	120	
	Loss of Trust	6	9	54	
DA9	Loss of Trust	3	39	117	213
	Loss of Liberty	2	48	96	
DA10	Loss of Trust	4	14	56	161
	Economic Loss	6	9	54	
	Dignity Loss	3	17	51	

Data Actions	Potential Problems for Individuals	Likelihood	Impact	Risk per Potential Problem	Risk per Data Action
					0
					0
					0
					0
					0
					0
					0
					0
					0
					0
					0

Task 4: Prioritize Risk**Guidance**

Prioritization: This tab provides some examples of prioritization methods. Organizations should choose prioritization methods that provide the best communication tool for their organization and that best support decision-making about how to respond to the identified risks.

System Risk Table: Indicates the estimated risk presented by a data action, its estimated percentage of system risk, and its estimated rank among data actions. The risk column is the total estimated risk per data action and colored to facilitate visual prioritization. The percent of system risk column is the estimated risk per data action relative to all other data actions. The rank among data actions column assigns relative values to the data actions pursuant to their estimated system risk percentage.

SAMPLE - Simple Data Action Risk Prioritization Table

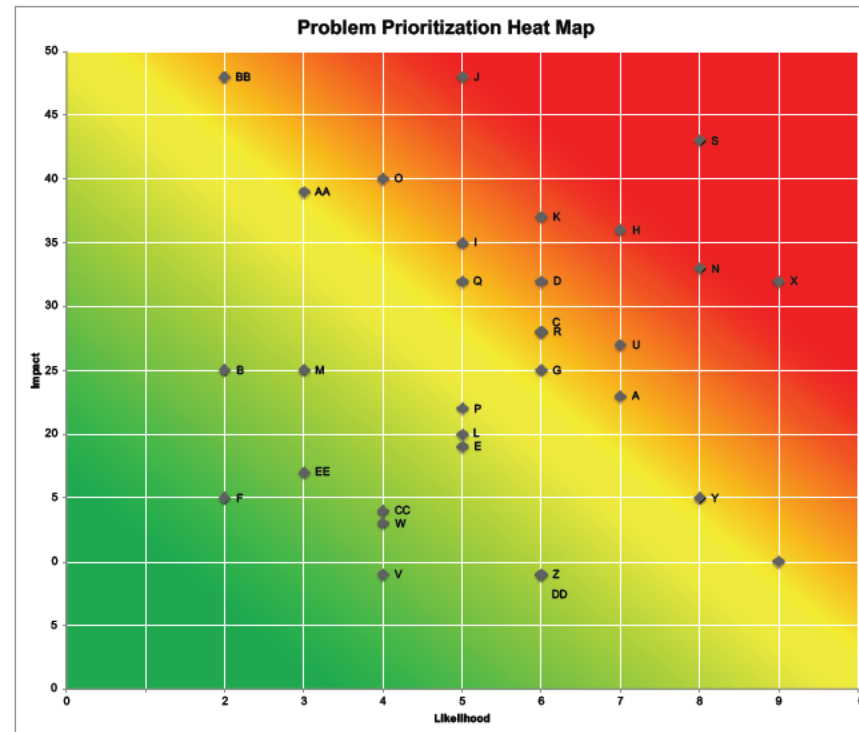
Data Actions	Risk	Percent of System Risk	Rank among data actions
Collection from social media site	379	9%	6
DA2	317	7%	7
DA3	577	13%	3
DA4	240	6%	8
DA5	821	19%	1
DA6	438	10%	5
DA7	659	15%	2
DA8	514	12%	4
DA9	213	5%	9
DA10	161	4%	10

Guidance

Top 5 Outliers Table: Red cells indicate the five (5) highest likelihood and impact results per potential problems for individuals per data action. Each potential problem for individuals is assigned a point label which is plotted on the adjacent heat map as a function of its assigned likelihood and impact values.

SAMPLE - Two Dimensional Problem Prioritization Table (including Top 5 Highest Likelihood and Impact outliers)

Data Actions	Potential Problems for Individuals	Point Label	Likelihood	Impact
Collection from the Social Media Site	Dignity Loss	A	7	23
	Loss of Autonomy	B	2	25
	Loss of Trust	C	6	28
	Economic Loss	D	6	32
	Loss of Autonomy	E	5	19
DA2	Loss of Trust	F	2	15
	Loss of Trust	G	6	25
DA3	Dignity Loss	H	7	36
	Loss of Liberty	I	5	35
DA4	Loss of Trust	J	5	48
	Economic Loss	K	6	37
DA5	Loss of Autonomy	L	5	20
	Discrimination	M	3	25
	Loss of Trust	N	8	33
	Dignity Loss	O	4	40
DA6	Loss of Trust	P	5	22
	Loss of Autonomy	Q	5	32
	Dignity Loss	R	6	28
	Loss of Autonomy	S	8	43
DA7	Dignity Loss	T	9	10
	Economic Loss	U	7	27
	Loss of Trust	V	4	9
	Loss of Autonomy	W	4	13
DA8	Dignity Loss	X	9	32
	Economic Loss	Y	8	15
	Loss of Trust	Z	6	9
	Loss of Trust	AA	3	39
DA9	Loss of Liberty	BB	2	48
	Loss of Trust	CC	4	14
DA10	Economic Loss	DD	6	9
	Dignity Loss	EE	3	17



Task 4: Prioritize Risk

Guidance

Prioritization: The *Risk Prioritization SAMPLE* tab provides some examples of prioritization methods. Organizations should choose prioritization methods that provide the best communication tool for their organization and that best support decision-making about how to respond to the identified risks.

System Risk Table: Indicates the estimated risk presented by a data action, its estimated percentage of system risk, and its estimated ranking amongst other data actions. The risk column is the total estimated risk per data action and colored to facilitate visual prioritization. The percent of system risk column is the estimated risk per data action relative to all other data actions. The rank among data actions column assigns relative values to the data actions pursuant to their estimated system risk percentage.

Simple Data Action Risk Prioritization Table

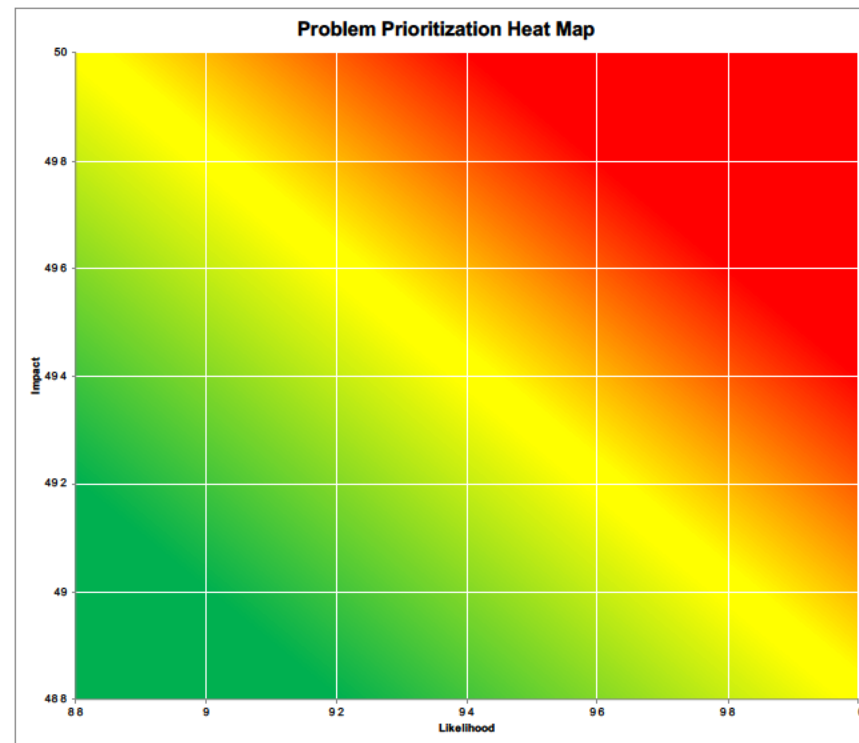
[illegible]

Guidance

Top 5 Outliers Table: Red cells indicate the five (5) highest likelihood and impact results per potential problems for individuals per data action. Each potential problem for individuals is assigned a point label which is plotted on the adjacent heat map as a function of its assigned likelihood and impact values.

SAMPLE - Two Dimensional Problem Prioritization Table
(including Top 5 highest Likelihood and Impact outliers)

Comprehensive Report on System Performance and Impact Analysis				
Data Actions	Potential Problems for Individuals	Point Label	Likelihood	Impact
		A		
		B		
		C		
		D		
		E		
		F		
		G		
		H		
		I		
		J		
		K		
		L		
		M		
		N		
		O		
		P		
		Q		
		R		
		S		
		T		
		U		
		V		
		W		
		X		
		Y		
		Z		
		AA		
		BB		
		CC		
		DD		
		EE		
		FF		



NIST Privacy Risk Assessment Methodology
Version: February 2019

Worksheet 4: Selecting Controls

Purpose:

This worksheet supports the selection of controls to mitigate privacy risks identified in *Worksheet 3*. It requires inputs from *Worksheets 2* and *3*.

Tasks:

1. Define system requirements (*Tab 2*).
2. Select controls (*Tab 3*).

Task 2: Define System Requirements

Guidance:

Using your preferred prioritization method from *Worksheet 3*, select the data actions and associated problems that are creating the privacy risks that you plan to mitigate or list data actions and their associated problems in order of highest to lowest priority. List potential system requirements that will be used to mitigate the identified risks. System requirements can be technical or policy measures or a combination of both.

In the considerations column, review the benefits or limitations of these potential system privacy requirements with respect to relevant factors such as system performance, cost, interaction with other system requirements, user experience, problem mitigation, etc. Considerations may also include how system privacy requirements help to meet the organizational privacy requirements or privacy capabilities captured in *Worksheet 1*. Considerations may also include cross-references to security risk assessments and security risks that could be mitigated by the system privacy requirements (or vice versa). The considerations should contain enough information to compare the potential system requirements and make decisions about which ones will be selected.

Example:

Data Actions	Problems for Individuals	Potential System Requirements	Considerations
Collection from the Social Media Site	Dignity Loss: Information is revealed about the individual that they would prefer not to disclose	1 Configure API to enable more granular retrieval of information, pull full name and email only; enable capability to pull profile photograph if future proofing requires it 2 Inform users of collection 3 Delete unneeded information after collection	1 Significantly reduces collection of information, possibly decreasing risk across the system. Would potentially lower risk of dignity loss, loss of autonomy, and loss of trust problems. 2 Users may be informed of specific information collected in this data action, but that may not improve risk across the system as they are unable to prevent the revelation of information. 3 Social Media site may refuse to reconfigure API. Unclear how users will understand the process. Leverages appropriate disposal controls. Decreases risk of dignity loss, but not necessarily loss of autonomy or loss of trust. Compare potential failure rate for API configuration to pull specified data correctly to potential failure rate of disposing of information after collection.
	Loss of Autonomy: People must provide extensive information, giving the acquirer an unfair advantage		
	Loss of Trust: Individuals lose trust in ACME due to a breach in expectations about the handling of personal information		

Problems	Potential Problems for Individuals	Potential System Requirements	Considerations

Task 3: Select Controls

Guidance:

1. List data actions and the r associated prob lems from *Tab 2: Define System Requirements* w th requ irements that w ll be met.
2. List pr vacy contro s se ected for mp ementat on. References for cons derat on: NIST Spec a Pub cat on 800 53, *Security and Privacy Controls for Federal Information Systems and Organizations* (ava ab e here: <https://csrc.nst.gov/pub cat ons/deta /sp/800 53/rev 4/f na>).
3. Descr be the rat ona e for se ect ng the contro s or eav ng the r sk un m t gated.
4. List the assoc ated system requ irements from *Tab 2: Define System Requirements* that are met by the se ected contro s.
5. Popu ate the res dua r sks co umn w th un m t gated summary ssues or adjusted summary ssues based on the contro s se ected.
6. Imp ement, assess and mon tor the se ected contro s for effect veness n manag ng the dent f ed pr vacy r sks. Reassess the res dua r sk acceptance determ nat on as needed. Iterate on the worksheets as changes to the system/product/serv ce occur.

Data Actions	Potential Problems for Individuals	Selected Controls	Rationale	System Requirements Met	Residual Risks

**NIST**

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-0001

May 2, 2023

Re: Invitation for Preliminary Comments on Proposed Rulemaking – Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking – PR 02-2023

Dear California Privacy Protection Agency,

Please accept the following in response to the California Privacy Protection Agency's "Invitation for Preliminary Comments on Proposed Rulemaking – Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking."

I. Introduction

The National Institute of Standards and Technology (NIST) is a non-regulatory agency within the United States Department of Commerce. Founded in 1901, NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST has conducted research and developed information security guidance for industry, government, and academia for over 50 years.

In addition to NIST, the United States Department of Commerce includes several other bureaus that work on privacy. The National Telecommunications and Information Administration (NTIA) is doing significant work on issues like privacy and civil rights, and privacy and artificial intelligence (AI), including a recent request for comment on AI accountability. The International Trade Administration (ITA) works to facilitate data flows in a way that protects consumers and facilitates global trade and economic growth through initiatives such as the European Union-United States Privacy Shield Framework (soon to be called the EU-U.S. Data Privacy Framework) and through its work in the newly formed Global Cross Border Privacy Rules (CBPR) Forum. These efforts aim to help companies, including small and medium-sized enterprises, meet privacy compliance requirements in Europe and around the world.

The NIST Privacy Engineering Program (PEP) focuses on understanding how a risk-based approach to privacy can help organizations make better privacy decisions and more effectively integrate privacy solutions into their products and services.¹ As a leader in privacy risk management, PEP has created novel and foundational constructs to foster and advance the field, such as a privacy risk model and privacy engineering objectives.² PEP has also developed privacy risk management tools and resources, including the *Privacy Risk Assessment Methodology* (PRAM) and *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*, Version 1.0 (Privacy Framework).³

These comments provide a brief summary of NIST's approach to privacy risk management as well as a high-level overview of PEP's privacy risk management resources, which any organization can use to create innovative products and services while protecting the privacy of individuals and communities.

¹ See NIST Privacy Engineering Program, available at <https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering>.

² See NIST IR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, available at <https://doi.org/10.6028/NIST.IR.8062>.

³ NIST *Privacy Risk Assessment Methodology* (PRAM), available at <https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources>; NIST *Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*, Version 1.0, available at <https://doi.org/10.6028/NIST.CSWP.01162020>. See Attachment A.

NIST

II. NIST's Approach to Privacy Risk Management

The Internet and associated information technologies provide benefits that are fueled by data about individuals that flow through a complex ecosystem. As a result, individuals may be unable to understand the potential consequences for their privacy as they interact with systems, products, and services. At the same time, organizations may not realize the full extent of these consequences for individuals, for society, or for their enterprises, which can affect their brands, their bottom lines, and their future prospects for growth. As discussed in the Privacy Framework, privacy is a condition that safeguards important human values of autonomy and dignity. But its broad and shifting nature makes clear communication about privacy risks within and between organizations and with individuals difficult. Privacy is ill-suited to one-size-fits-all solutions and privacy risks must be evaluated within the context of an organization's unique data processing activities. Privacy risk management is a key process that enables organizations to achieve mission goals while minimizing adverse outcomes. By providing a common language to address privacy risks, privacy risk management is especially helpful in communicating both inside the organization (e.g., across management levels and operating units), as well as outside the organization.

As illustrated in Figure 1, managing cybersecurity risk contributes to managing privacy risk, but is insufficient, as privacy risks can also arise by means unrelated to cybersecurity incidents. Having a general understanding of the different origins of cybersecurity and privacy risks is important for determining the most effective solutions to address the risks. The NIST approach to privacy risk is to consider privacy events as potential problems (i.e., harms) individuals could experience arising from system, product, or service operations with data, whether in digital or non-digital form, through the complete data lifecycle. The problems individuals can experience as a result of data processing can be expressed in various ways, but NIST describes them as ranging from dignity-type effects such as embarrassment or stigmas, to more tangible harms such as discrimination, economic loss, or physical harm.

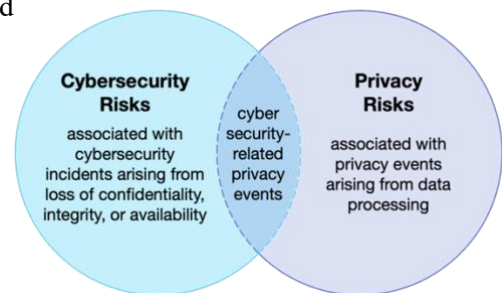


Figure 1: Relationship between Cybersecurity and Privacy Risks (NIST Privacy Framework)

NIST developed a privacy risk model to help organizations answer the fundamental question of how to distinguish between data actions (i.e., operations with data) that are beneficial or benign and data actions that can create harms to individuals. The NIST risk model equips organizations to calculate privacy risk as the likelihood that individuals will experience problems resulting from data processing multiplied by the impact should such problems occur. This impact assessment is where privacy risk and organizational risk intersect. Individuals and groups (including at the societal level) experience the direct impact of harms. As a result of these harms, an organization may experience impacts such as non-compliance costs, lost revenue, customer abandonment, and harm to its brand, reputation, or internal culture. By connecting harms that individuals experience to these well-understood organizational impacts, organizations can bring privacy risk into parity with other risks in their portfolio and drive more informed decision-making about resource allocation to strengthen privacy programs.

III. NIST Privacy Risk Management Resources

A. Privacy Risk Assessment Methodology (PRAM)

The NIST *Privacy Risk Assessment Methodology* (PRAM) was created to help organizations identify, assess, and prioritize privacy risks to determine how to respond and select appropriate solutions for

potential problematic data actions.⁴ Organizations may choose to prioritize and respond to privacy risk in different ways, depending on their policies and established privacy values, risk tolerance levels, and regulatory environment. Response approaches typically fall into four categories:⁵

- Mitigating the risk (e.g., organizations may be able to apply technical and/or policy measures to the systems, products, or services that minimize the risk to an acceptable degree);
- Transferring or sharing the risk (e.g., contracts are a means of sharing or transferring risk to other organizations, privacy notices and consent mechanisms are a means of sharing risk with individuals);
- Avoiding the risk (e.g., organizations may determine that the risks outweigh the benefits, and forego or terminate the data processing); or
- Accepting the risk (e.g., organizations may determine that problems for individuals are minimal or unlikely to occur, therefore the benefits outweigh the risks, and it is not necessary to invest resources in mitigation).

Privacy risk assessments are particularly important because privacy safeguards multiple values. The methods for safeguarding these values may differ and could be in tension with one another. Identifying if data processing creates problems for individuals, even when an organization may be fully compliant with applicable laws or regulations, can help with ethical decision-making in system, product, and service design or deployment. This facilitates optimizing beneficial uses of data while minimizing adverse consequences for individuals' privacy and society as a whole, as well as avoiding losses of trust that damage organizations' reputations, slow adoption, or cause abandonment of products and services.

Used as a customizable, internal way for organizations to determine how to prioritize risk, the PRAM's semi-quantitative approach, based on a scale of 1-10, helps organizations estimate expected probabilities for potential privacy problems occurring.⁶ However, we emphasize that PRAM risk assessment scores are *not* a generalizable score that can be extrapolated to all organizations. To the contrary, each risk assessment score is calculated based on the unique context in which an organization's data processing activities are taking place, and then used to communicate with decision-makers about the appropriate response.

The PRAM consists of four worksheets to guide organizations through their risk assessment in a clear and systematic way.

- **Worksheet 1: Framing Organizational Objectives and Privacy Governance** helps organizations capture the organizational environment (i.e., the mission/business objectives and legal privacy responsibilities) in which systems/products/services are deployed to support the development and implementation of appropriate privacy capabilities.
- **Worksheet 2: Assessing System Design** helps organizations identify and document inputs for the risk analysis. These inputs are:
 - The data actions performed by the system,
 - The data elements being processed or individuals' interactions with the system/product/service, and
 - Relevant contextual factors.

Worksheet 2 encourages the development of a visual data map for identifying data actions within the system.

⁴ See the NIST *Privacy Risk Assessment Methodology* (PRAM) at [3].

⁵ See NIST Special Publication (SP) 800-39, *Mapping Information Security Risk Organization, Mission, and Information System View* at <https://doi.org/10.6028/NIST.SP.800-39>.

⁶ Semi-quantitative assessments, as described in SP 800-30, employ a set of methods, principles, or rules for assessing risk that can use scales (e.g., 1-10) to translate a score into qualitative terms that can support risk communications for decision makers, p. 14. See NIST SP 800-30, Rev. 1, available at [13].

- **Worksheet 3: Prioritizing Risk** provides structure for the assessment and prioritization of privacy risk in systems. Determining the privacy risk of a particular data action requires assessing the likelihood that a data action will be problematic for individuals and the impact should such a problem occur.⁷ Organizations can consult the PRAM's non-exhaustive, illustrative Catalog of Problematic Data Actions and Problems to assist in this analysis.⁸ Worksheet 3 also provides examples of prioritization methods (e.g., ordered tables, heat map) that organizations can use to support decision-making about how to respond to the identified risks.
- **Worksheet 4: Selecting Controls** helps organizations that have determined which risks to mitigate to further define their privacy requirements and select and implement controls (i.e., technical, physical, and/or policy safeguards) to meet the requirements.⁹ Organizations can use Worksheet 4 to document potential controls and considerations and then finalize their selection and rationale. This provides a basis for the organization to monitor and assess implemented controls for effectiveness in managing the identified privacy risks. As needed, an organization can reassess the residual risk acceptance determination moving forward.

The PRAM helps drive cross-organization discussions and collaboration to identify, prioritize, and respond to privacy risks with effective solutions tailored to organizations' unique contexts. Its activities and outputs enable organizations to tell a clear story about the privacy risks they may experience to encourage decision-making and generate positive change.

B. NIST Privacy Framework

Whereas the PRAM is a tool for assessing privacy risks at the system-level, the NIST Privacy Framework: *A Tool for Improving Privacy through Enterprise Risk Management*, Version 1 (Privacy Framework) is a voluntary, law, technology, and sector neutral tool designed to help organizations bring privacy risk management into their overall enterprise risk management portfolio.¹⁰ The Privacy Framework follows the structure of the *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) to facilitate using both frameworks together, allowing for increased collaboration between privacy and security programs.¹¹

Following a transparent, consensus-based process including both private and public stakeholders, NIST published the Privacy Framework to enable better privacy risk management practices that support privacy by design concepts and help organizations protect individuals' privacy. The Privacy Framework can help organizations in building customers' trust by supporting ethical decision-making in product and service design or deployment that optimizes beneficial uses of data while minimizing adverse consequences for individuals' privacy and society as a whole. It also can help organizations demonstrate the measures they are taking to fulfill current compliance obligations, as well as help them future-proof products and services to meet these obligations in a changing technological and policy environment. Finally, it is a

⁷ Referencing back to Figure 1, the middle of the Venn diagram focuses on the security risk assessment. However, organizations can use the PRAM to do both security risk assessments and data processing risk assessments. By doing both, organizations can make distinctions and understand what the source of the risk is, so they can implement appropriate controls.

⁸ In the Catalog, descriptions are provided for the problematic data actions: Appropriation; Distortion; Induced Disclosure; Insecurity; Re-Identification; Stigmatization; Surveillance; Unanticipated Revelation; and Unwarranted Restriction and the problems: Dignity Loss; Discrimination; Economic Loss; Loss of Self Determination (including Loss of Autonomy, Loss of Liberty, Physical Harm); and Loss of Trust.

⁹ For assistance with this process, see NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, available at <https://doi.org/10.6028/NIST.SP.800-53r5>

¹⁰ See the NIST Privacy Framework: *A Tool for Improving Privacy through Enterprise Risk Management*, Version 1.0 at [4]. The Privacy Framework Resource Repository available at <https://www.nist.gov/privacy-framework/resource-repository> provides resources such as crosswalks to laws, regulations, and standards, and guidance and tools for implementation support.

¹¹ See the *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), available at <https://doi.org/10.6028/NIST.CSWP.04162018>

powerful tool for facilitating communication about privacy practices with individuals, business partners, assessors, and potentially even regulators.

The Privacy Framework is composed of three parts:

- The **Core** provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk.¹²
- **Profiles** are a selection of specific Functions, Categories, and Subcategories from the Core that an organization has prioritized to help it manage privacy risk.
- **Implementation Tiers** help an organization communicate about whether it has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile.

To account for the unique needs of an organization, use of the Privacy Framework is flexible, although it is designed to complement existing business and system development operations. The Privacy Framework sets up organizations to establish privacy values and determine their risk appetite, which then enables them to better understand which outcomes and activities from the Privacy Framework Core to prioritize. Designed to be jurisdiction- and sector-agnostic, the Privacy Framework provides the building blocks for executing on legal obligations without using terms specific to a given law or jurisdiction so that any organization can more easily use it. Avoiding definitional issues promotes a focus on what is happening with data, whether the processing is giving rise to privacy risks, and how best to respond effectively.

IV. Conclusion

NIST's resources are designed to help drive communication within organizations around privacy risk management practices to more effectively build trust in products or services. We hope that creating awareness around these resources can open the door to more organizations taking privacy into consideration.

Thank you again for the opportunity to respond to the "Invitation for Preliminary Comments on Proposed Rulemaking – Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking." We are pleased to provide this feedback and would welcome any questions or further discussion about our resources.

Sincerely,
Meghan Anderson
Privacy Risk Strategist
Privacy Engineering Program
National Institute of Standards and Technology (NIST)

¹² The Privacy Framework's Core Functions are:

- Identify-P: Develop the organizational understanding to manage privacy risk for individuals arising from data processing.
- Govern-P: Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.
- Control-P: Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.
- Communicate-P: Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding about how data are processed and associated privacy risks.
- Protect-P: Develop and implement appropriate data processing safeguards.

Please see **Attachment A** for the Privacy Risk Assessment Methodology (PRAM).