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.
[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 stands 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-theprivacy-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 Impat 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