1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 | fpf.org

July 18, 2024

Via Electronic Submission

Civil Rights Department
c/o Rachael Langston
Assistant Chief Counsel
555 12th Street, Suite 2050
Oakland, CA 94607

To Whom It May Concern,

The Future of Privacy Forum (FPF) is pleased to submit comments to the California Civil Rights Council regarding their Proposed Modifications to the Employment Regulations Regarding Automated-Decision Systems.[1] FPF is a global non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices. In alignment with the aims of the California Civil Rights Council, FPF has extensive experience identifying risks associated with artificial intelligence (AI) and developing guidelines and best practices to support the ethical deployment of emerging technologies, including the publication of FPF's *Best Practices for AI and Workplace Assessment Technologies* ("Best Practices").[2]

By modernizing the state's current employment regulations, the California Civil Rights Council has an important opportunity to influence how existing civil rights laws will apply to emerging technologies like AI. Ideally, these regulations should provide clarity and constructive guidance within the context of existing laws and frameworks to effectively benefit both organizations and individuals.

Given these considerations, the Future of Privacy Forum recommends:

1. **Definition Alignment**: The Council's definition of "automated decision system" should align with similar regulations at the state and federal levels to facilitate greater clarity and compliance.

[1] Proposed Modifications to Employment Regulations Regarding Automated-Decision Systems, California Civil Rights Council (proposed May 17, 2024) (to be codified at Cal. Code. Regs. tit. 2 §§ 11008-11079), https://calcivilrights.ca.gov/wp-content/uploads/sites/32/2024/05/Automated-Decision-System-Regulations-Proposed-Text.pdf.
[2] *Best Practices for AI and Workplace Assessment Technologies*, Future of Privacy Forum (Sept. 2023), https://fpf.org/wp-content/uploads/2024/02/FPF-Best-Practices-for-AI-and-WA-Tech-FINAL-with-date.pdf.

2. **Role-Specific Responsibilities**: The Council should create legal standards for when a developer of an AI system becomes an agent or employment agency, accounting for role-specific responsibilities and capabilities in the AI system lifecycle.
3. **Data Retention and Privacy:** Data retention and record-keeping requirements should be reasonable and align with California consumers' rights to data privacy and data minimization.
4. **Additional AI Governance Measures**: The Council should conduct additional inquiries about the use of ADS and existing civil rights laws, including assessing whether automated systems are fit for purpose.

I. The Council's Definition Of "Automated Decision System" Should Align With Similar Regulations At The State And Federal Levels To Facilitate Greater Clarity And Compliance

Given shared goals and proposed regulatory activity regarding "automated decisionmaking systems" (ADS) between the Council, California Privacy Protection Agency (CPPA),[3] California Government Operations Agency,[4] and the California legislature,[5] the Council should aim to align its proposed definition of ADS with existing California state laws. Alignment across state lawmaking bodies will promote consistency in AI governance and mitigate potential conflicts arising from divergent terminology and definitions. As written, the Council's proposed definition of "automated decision system" is much broader than related state laws, regulations, and frameworks, raising potential challenges regarding consistency and clarity for organizations and individuals navigating these regulations.

Because AI systems vary widely in their functions, from simple algorithms to complex autonomous systems, not all AI technologies have the same impact on decision-making processes. To ensure focus and regulatory efforts are targeted toward technologies that play an impactful role in individuals' rights, Government Code § 11546.45.51, the CPPA Draft Regulations

---

[3] Draft Risk Assessment and Automated Decisionmaking Technology Regulations (proposed Mar. 2024) (to be codified at Cal. Code Regs. tit. 11 §§ 7001-7222), https://cppa.ca.gov/meetings/materials/20240308_item4_draft_risk.pdf

[4] *State of California: Benefits and Risks of Generative Artificial Intelligence Report*, California Government Operations Agency (Nov 2023) (pursuant to Executive Order N-12-23) https://www.govops.ca.gov/wp-content/uploads/sites/11/2023/11/GenAI-EO-1-Report_FINAL.pdf

[5] A.B. 2930, 2023-24 Regular Session (CA 2023); S.B. 1047, 2023-24 Regular Session (CA 2024); A.B. 2013, 2023-24 Regular Session (CA 2024); A.B. 3030, 2023-24 Regular Session (CA 2024); A.B. 2877, 2023-24 Regular Session (CA 2024); A.B. 1791, 2023-24 Regular Session (CA 2024); A.B. 3211, 2023-24 Regular Session (CA 2024); S.B. 942, 2023-24 Regular Session (CA 2024).

and Assembly Bill 2930 have required that the ADS role be "substantial" to the decision-making process and list certain technologies to be excluded as either low-risk or necessary to function.

Law	Definition	Exclusions
Civil Rights Council Proposed Text	A computational process that screens, evaluates, categorizes, recommends, or otherwise makes a decision or facilitates human decision making that impacts applicants or employees.	Word processing software, spreadsheet software, and map navigation systems.
California Privacy Protection Act Draft Regulations (March 2024)	Any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking.	Web hosting, domain registration, networking, caching, website-loading, data storage, firewalls, anti-virus, anti-malware, spam- and robocall-filtering, spellchecking, calculators, databases, spreadsheets, or similar technologies.
Government Code § 11546.45.51	"High-risk automated decision system" means an automated decision system that is used to assist or replace human discretionary decisions that have a legal or similarly significant effect, including decisions that materially impact access to, or approval for, housing or accommodations, education, employment, credit, health care, and criminal justice.	N/A
Assembly Bill 2930	A system or service that uses artificial intelligence and has been specifically developed to, or specifically modified to, make, or be a substantial factor in making, consequential decisions.	Cybersecurity-related technology, including technology designed to 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 those actions.

Similarly, other jurisdictions regulating these tools have adopted a comparable approach.[6] As a result, California organizations processing personal information in an automated fashion for an employment decision may encounter conflicting AI governance applications and requirements both within the state and across state lines, due to differing definitions of AI across different laws and agency guidelines. In fact, the CPPA recently submitted a letter to the California legislature, arguing that the overlapping scope and requirements between AB 2930 and the CPPA draft regulations could cause confusion and make it difficult for businesses to comply, and thus the legislature should harmonize the bill language with the CPPA draft regulations.[7] Similarly, the Council should aim to align the modified regulations with existing laws and frameworks to provide a clear path forward for entities looking to offer or deploy this technology.

II. The Council Should Create Legal Standards for When A Developer Of An AI System Becomes An Agent Or Employment Agency, Accounting For Role-Specific Responsibilities and Capabilities in the AI System Lifecycle.

The California Civil Rights Council should establish a legal standard in their proposed modifications that would help clarify the degree of involvement, control, and influence that is required for an AI developer to become liable for discriminatory outcomes, based on the role and capability-specific responsibilities of developers and deployers and their relationship to one another.[8] Developers, who build AI systems, and deployers, who utilize such systems, are distinct but not mutually exclusive roles that require specific obligations to enhance accountability, compliance, and certainty.[9] For example, typically, developers define the AI system's purpose and scope, gather and preprocess training data, select or design algorithms, and train the model. Whether they assist the deployer in implementation or conduct ongoing monitoring once deployed by deployers/employers depends on the relationship between the parties.

---

[6] *See, e.g.* N.Y.C Admin. Code § 20-870 ("**automated employment decision tool**" means any computational process, derived from machine learning, statistical modeling, data analytics, or artificial intelligence, that issues simplified output, including a score, classification, or recommendation, that is used to substantially assist or replace discretionary decision making for making employment decisions that impact natural persons); Colorado SB 205 ("**high-Risk Artificial Intelligence System**" means "any artificial intelligence system that, when deployed, makes, or is a substantial factor in making, a consequential decision").

[7] "Agenda Item 7–Legislative Update and Possible Authorization for CPPA's Positions on Pending Legislation. AB 2930, Automated decision tools (Bauer-Kahan, as amended July 3, 2024), California Privacy Protection Agency (July 11, 2024), https://cppa.ca.gov/meetings/materials/20240716_item7_ab_2930.pdf

[8] *Best Practices for AI and Workplace Assessment Technologies*, Future of Privacy Forum (Sept. 2023), https://fpf.org/wp-content/uploads/2024/02/FPF-Best-Practices-for-AI-and-WA-Tech-FINAL-with-date.pdf.

[9] There may be cases where developers and deployers of an AI system are the same entity. In that case, the entity would need to be assessed through both lenses.

Under the Council's proposed modification, a developer may be de facto considered an "agent" or "employment agency," with corresponding obligations and liabilities.[10] However, not all developers can influence or control how AI systems are deployed and used by third parties. Bias can (but does not always) arise from an AI system's use of the deployer's biased or low quality data, rather than the developer's training or design. For example, in the Federal Trade Commission's action against Rite-Aid for unfair use of a facial recognition system, Rite-Aid purchased "off-the-shelf" facial recognition from a vendor for anti-theft purposes.[11] Nonetheless, the Commission found that Rite-Aid was responsible for causing algorithmic discrimination due to Rite-Aid's use of low quality images, use of the system more frequently in areas with higher minority populations, failure to conduct ongoing monitoring and testing, and lack of employee oversight or controls.[12] Accordingly, allocation of responsibility and accountability for discrimination arising from the use of an AI system must account for specific factors related to the roles of both developers and deployers/employers.

The Equal Employment Opportunity Commission (EEOC) has stated that "a software vendor acts as an employer's agent if the employer has given [the vendor] significant authority to act on the employer's behalf," which "may include situations where an employer relies on the results of a selection procedure that the agent administers on its behalf."[13] In a recent anti-discrimination lawsuit involving a software vendor, the EEOC filed an amicus brief in which they explained their position that "developers may be liable under federal discrimination laws when they exercise sufficient control over the employment decisionmaking process."[14] However, the court stated,

---

[10] § 11008(b) "Agent." Any person acting on behalf of an employer, directly or indirectly, including, but not limited to, a third party that provides services related to making hiring or employment decisions (such as recruiting, applicant screening, hiring, payroll, benefit administration, evaluations and/or decision-making regarding requests for workplace leaves of absence or accommodations) or the administration of automated-decision systems for an employer's use in making hiring or employment decisions; *see also* § 11008(h) "Employment Agency." Any person undertaking, for compensation, services to identify, screen, and/or to procure job applicants, employees or opportunities to work, including persons undertaking these services through the use of an automated-decision system.

[11] *Federal Trade Commission v. Rite Aid Corporation*, Case No. 2:23-cv-5023, Stipulated Order for Permanent Injunction and Other Relief (Dec. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2023190_riteaid_stipulated_order_filed.pdf

[12] *Id.*

[13] *Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964*, EEOC (May 18, 2023), https://www.eeoc.gov/laws/guidance/select-issues-assessing-adverse-impact-software-algorithms-and-artificial

[14] *Mobley v. Workday, Inc.*, 2024 U.S. Dist. LEXIS 11573, (N.D. Cal. 2024); Brief for Equal Employment Opportunity Commission as Amicus Curiae Supporting Plaintiff, Mobley v. Workday, Inc., Case No. 3:23-cv-00770-RFL (N.D. Cal. 2024).

"[m]any software vendors do not qualify as agents because they have not been delegated responsibility over traditional employment functions."[15] Nonetheless, the law is still evolving.[16]

III. The Rules' Data Retention And Record-Keeping Requirements Should Be Reasonable And Align With California Consumers' Existing Rights To Data Privacy And Data Minimization.

To minimize the risk of individuals' personal data being misused or breached, and uphold California citizens' privacy rights,[17] the Council should align and clarify the proposed regulations' record and data retention requirements with existing privacy rights and obligations under the California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), and regulations set forth by the CPPA (hereinafter "the California privacy laws"). The proposed modifications in 11013(c), require employers and covered entities to retain "automated-decision system data," defined to include all data used to train the machine-learning algorithm and *personal data* of individual applicants and employees, for "four years from the date of the marking of the record or the date of the personnel action involved, whichever occurs later." The developers or providers of automated decision systems (ADS) must similarly retain this data for "at least four years following the last date on which the automated decision system was used…". As currently written, these retention requirements may not only result in Californian's personal data being retained beyond what is reasonably necessary, but they also raise questions about if they are meant to override or cede to existing California privacy rights to delete such data or opt-out of automated decisionmaking technology.

As an initial matter, data minimization is a requirement in California privacy laws that limits the collection, use, retention, and sharing of personal information to what is necessary and proportionate to achieve the intended purpose. This serves important functions, such as reducing

---

[15] See, *Mobley v. Workday, Inc.*, 2024 U.S. Dist. LEXIS 11573, Defendant Workday Inc.'s Brief In Response to Brief of the Equal Opportunity Commission, at 1 (arguing that this case was the first time the EEOC has stated that a software vendor can be liable under federal antidiscrimination statutes based on how its customers use its software in the hiring process).

[16] *Mobley v. Workday, Inc.*, Order Granting in Part and Denying In Part Motion to Dismiss, Case No. 23-cv-00770-RFL (July 12, 2024) "For example, if an employer used a spreadsheet software program to sort workers by birthdate and then filtered out all applicants over the age of forty from consideration, the software vendor would not have acted as the employer's agent for purposes of the anti-discrimination statutes, because the spreadsheet is not participating in the determination of which employees to hire." *The Court determined that the software vendor did not qualify as an employment agency and dismissed the claim.*

[17] Robinson & Cole LLP, *The Risks of Excessive Data Retention and Tips for Information Security*, The National Law Review (Jan. 11, 2024) https://natlawreview.com/article/risks-excessive-data-retention-and-tips-information-security.

the risk of harm from data breaches, the likelihood of accidental data leaks, and the potential for misuse of personal information that perpetuates significant harms.[18] The proposed rule requiring developers to retain data for four years following the last date on which the ADS was used, however, is unclear and could run afoul of data minimization principles. It is ambiguous whether the "date of last use" refers to the last use related to the specific individual whose data was collected or the last use of the ADS system by the employer in general. If an employer integrates an ADS into its everyday business model and hiring practices with no specified end date, this lack of clarity could result in personal data being indefinitely retained by a developer with whom the individual has no ongoing relationship, thereby increasing the potential risk of harm. Similarly, the proposed four year retention requirements for employers and covered entities may contradict other data minimization standards, particularly when federal guidance from the EEOC requires personnel records to be kept only for one year after the employee leaves or is terminated.[19]

Additionally, California privacy laws grant individuals the right to delete their personal information and opt-out of automated decisionmaking technologies.[20] Under the proposed retention requirements, it is unclear whether an employee or applicant can request the deletion of their personal information from an employer or prospective employer. These privacy laws allow certain processing activities required for compliance with other laws to be excluded from their scope, which could mean that employees or applicants lack deletion rights. However, this interpretation would conflict with the California privacy laws' unique design to protect and provide rights to both consumers and employees.[21]

---

[18] Eric Null, Isedua Oribhabor, and Willmary Escoto, *Data Minimization: Key to Protection Privacy and Reducing Harm*, Access Now (May 2021), https://www.accessnow.org/wp-content/uploads/2021/05/Data-Minimization-Report.pdf

[19] U.S. Equal Employment Opportunity Commission, Recordkeeping Requirements, https://www.eeoc.gov/employers/recordkeeping-requirements#:~:text=EEOC%20Regulations%20require%20that%20employers,from%20the%20date%20of%20termination (last visited June 28, 2024). .

[20] California Consumer Privacy Act of 2018, Sec. 1798.105. *Consumers' Right to Delete Personal Information*, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5; Draft Regulations (March 2024), California Privacy Protection Agency, Sec. 7221. "Requests to Opt-Out of the Business's Use of Automated Decisionmaking Technology", https://cppa.ca.gov/meetings/materials/20240308_item4_draft_risk.pdf

[21] Kung Feng, *Overview of New Rights for Workers under the California Consumer Privacy Act,* UC Berkeley Labor Center (Dec. 6, 2023) (stating that the CCPA was the first step for workers to gain basic rights around their workplace data whereas U.S. workers are otherwise unprotected from employers using digital workforce management technologies), https://laborcenter.berkeley.edu/overview-of-new-rights-for-workers-under-the-california-consumer-privacy-act/

Further, in the event that an employee or candidate initially permits being subject to an automated decisionmaking system, but later exercises their right to opt-out right, it is unclear whether the employer must still maintain the personal information used. In that scenario the ADS provider is likely considered a processor of the employer and similarly must delete such data under the California privacy laws. As noted above, extensive maintenance of personal information contrary to the candidate or employees' desires may run afoul of data minimization standards. Therefore, the Council's proposed modifications should clarify whether and to what extent California workers' privacy rights impact employer and developer recordkeeping requirements.

IV. The Council Should Conduct Additional Inquiries about the Use of ADS and Existing Civil Rights Laws, Including Assessing Whether Automated Systems Are Fit For Purpose.

Even ADS that are properly tested for bias can still cause discriminatory impact. The Council should conduct additional inquiries related to the use of ADS and the impact of existing civil rights laws. As noted by leading computer science ethicists, Arvind Narayanan and Sayash Kapoor, there are notable limitations to what AI can accomplish, and in some cases, discriminatory impact may result from entities developing or deploying "AI snake oil."[22] In the employment context, Narayanan states that millions of people who apply for jobs are subject to algorithmic tools that, based on an individual's body language, speech pattern, and tone, assess whether an individual is a good candidate for employment.[23] However, emotion recognition tools for assessing job candidacy are not only less accurate across demographic populations but are also widely considered pseudoscience.[24] Even if these systems were equally accurate across demographics, there is not a scientifically-established correlation between emotional characteristics and employment qualifications, which may potentially lead to further discrimination, especially against individuals from diverse cultures and those on the neurodiversity spectrum.[25]

---

[22] Arvind Narayanan and Sayash Kapoor, *AI Snake Oil: What Artificial Intelligence Can Do, What It Can't, and How to Tell the Difference,* Princeton University Press (Sep. 24, 2024).

[23] Arvind Narayanan, *How to Recognize Snake Oil,* Presentation at Princeton University with the Center for Information Technology Policy, https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf

[24] Lisa Feldman Barrett, Ralph Adlophs, et. al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, Psychological science in the public interest: a journal of the American Psychological Society, 20(1), 1–68, (2019), https://pubmed.ncbi.nlm.nih.gov/31313636/.

[25] Kat Roemmich et al., *Values in Emotion Artificial Intelligence Hiring Services: Technosolutions to Organizational Problems*, 7 Proc. ACM Hum.-Comput. Interact. 109, 109:5, 109:21-22 (2023), https://dl.acm.org/doi/pdf/10.1145/3579543; *see also* Jay Stanley, *Experts Say 'Emotion Recognition' Lacks Scientific Foundation*, American Civil Liberties Union (2019), https://www.aclu.org/news/privacy-technology/experts-say-emotion-recognition-lacks-scientific.

Best Practices for AI and Workplace Assessment Technologies, developed by FPF in coordination and consultation with leading companies, civil society, and other experts, recommend that organizations do not use facial characterization or emotion inference technologies in the hiring process and that hiring tools should be "fit for their intended purpose."[26] To prevent discriminatory impacts and overall harm, AI tools must be validated and tested to ensure they solve the problems they are designed for.[27] Accordingly, the Council should consider existing AI governance measures, such as "fit for purpose" tests, that further support civil rights protections.

Conclusion

FPF appreciates the opportunity to comment on these issues, and we welcome any further opportunity to provide resources or information to assist in this vital effort. If you have any questions regarding these comments and recommendations, please contact Adonne Washington at awashington@fpf.org (cc:info@fpf.org).

Sincerely,

Tatiana Rice, *Deputy Director U.S. Legislation*
Adonne Washington, *Policy Counsel Mobility, Location, & Data*

The Future of Privacy Forum
https://fpf.org/

[26] *Best Practices for AI and Workplace Assessment Technologies*, Future of Privacy Forum (Sept. 2023), https://fpf.org/wp-content/uploads/2024/02/FPF-Best-Practices-for-AI-and-WA-Tech-FINAL-with-date.pdf.
[27] *Id.*