Proskauer

California Takes Steps to Regulate the Use of AI for "Significant Employment Decisions"

California Employment Law Update on **November 25, 2024**

On November 8, 2024, the California Privacy Protection Agency (CPPA) voted 4-1 to proceed with formal rulemaking regarding automated decision-making technology ("ADMT"), which the draft regulations define as "any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking." If enacted, the regulations would impose sweeping requirements on employers who rely on assistance from artificial intelligence (AI) tools in making "significant employment decisions," which the regulations define to include "[h]iring; [a]llocation or assignment of work; salaries, hourly or per-assignment compensation, incentive compensation such as bonuses, or other benefits [];[p]romotion; and [d]emotion, suspension, and termination." The draft regulations take a similar approach to laws that have been enacted in New York and Colorado, in that they require certain disclosures and risk assessments, and require that employees and applicants be able to opt-out of being evaluated by AI in some contexts.

The key elements of the draft regulations include the following:

- **Pre-Use Notice** – Employers that use ADMT for significant employment decisions must inform "consumers"—which includes not only employees, but also independent contractors, and job applicants—about the employer's use of ADMT, the consumer's right to opt-out of ADMT, and the consumer's right to access ADMT prior to the employer's processing of any personal information.

- **Bias Review** – Employers that use physical or biological identification or profiling for a significant employment decision must conduct a bias review to ensure that the software does not discriminate based on "protected classes" (which is undefined in the current draft). It is unclear from the draft regulations whether the audit would need to assess the tool's effects on that particular employer's decision-making. In New York City, for example, employers may rely on bias audits that use data from other entities in some contexts (e.g., if the employer has never used the tool before or has shared its data to the auditor for inclusion in the audit).

- **Opt-Out** – Employers "must provide consumers with the ability to opt-out of ADMT" for significant employment decisions. However, employers may deny an opt-out request for decisions regarding hiring, allocation of work, and compensation if the ADMT has "accuracy and nondiscrimination safeguards," meaning the employer "has conducted an evaluation of" and "implemented policies, procedures, and training to ensure that the automated decisionmaking technology works as intended for the business's proposed use and does not discriminate based upon protected classes."

- **Cybersecurity Audits** –Employers that use ADMT for significant employment decisions must complete an annual cybersecurity audit to, among other things, "assess and document the effectiveness of" the employer's cybersecurity program "in preventing unauthorized access, destruction, use, modification, or disclosure of personal information," "[i]dentify and describe in detail the status of any gaps or weakness" in the employer's cybersecurity program," and "[d]ocument the business's plan to address the gaps and weaknesses." Businesses must use "a qualified, objective, independent professional" that may be "internal or external to the business."

- **Risk Assessments** – Employers that use ADMT for significant employment decisions must complete a risk assessment within "24 months from the effective date of the[] regulations," and thereafter must complete a risk assessment "every calendar year" before initiating the processing of personal information "to determine whether the risks to consumers' privacy from the processing of personal information outweigh the benefits to the consumer, the business, other stakeholders, and the public." Employers must submit the annual risk assessment to the CPPA. Among other requirements, the risk assessment must "identify [the] purpose for processing consumers' personal information" (which "must not be identified or described in generic terms, such as 'to improve our services' or for 'security purposes'"); the "method for collecting, using, disclosing, retaining, or otherwise processing personal information"; "the negative impacts to consumers' privacy associated with the processing"; and "safeguards that [the employer] plans to implement to address the negative impacts."

Now that the CPPA has published its notice of proposed rulemaking, the public comment period begins. The CPPA requested that the standard 45-day public comment period be extended due to the holidays. Thus, comments will be due in early 2025, but no specific date has been set.

We will continue to monitor these developments.

View original.

Related Professionals

- **Jonathan P. Slowik**
  Senior Counsel
- **Jennifer J. McDermott**
  Associate
- **Guy Brenner**
  Partner