This article was published in *PLI Chronicle: Insights and Perspectives for the Legal Community*, https://plus.pli.edu. Not for resale.

PLI Chronicle

August 2023

AI in Employment: Privacy Regulation Is Here

Cassandra Gaedt-Sheckter

Emily Maxim Lamm

Gibson, Dunn & Crutcher LLP

Much ink has been spilled about the role of artificial intelligence (AI) in employment, especially in light of the developing menagerie of laws seeking to govern automated decision tools in the workplace. And rightly so—this is a burgeoning area with daily developments that must be carefully monitored. From enforcement of New York City's AI employment law beginning on July 5, 2023 to a barrage of proposed bills like U.S. Senator Casey's No Robot Bosses Act, there has seldom been a dull moment in 2023. However, amidst all of the buzz around automation in the workplace, privacy regulations have emerged as yet another piece of the employment puzzle.

Where Does Privacy Come In?

Privacy regulations play a key role in the effective governance of AI in the workplace. AI systems are increasingly processing personal data—ranging from demographic data to biometric data—by using algorithms to analyze and extract insights from various types of information to make predictions, recommendations, or even decisions for an employer. By implementing an AI system that collects and processes this personal data, the employer may be responsible for ensuring compliance with the evolving patchwork of laws governing the use of AI in employment decision making but also with many existing data protection laws, depending on their geographical scope and use.

Take for example an employer operating in Illinois that is using an AI-powered video interviewing platform. To verify the applicant's identity, the platform collects

voice prints, and to analyze the applicant's facial expressions, it collects facial geometry scans. In so doing, the platform is likely conducting an AI analysis and collecting biometric data for processing. Given the use of AI analysis in the applicant interview, the employer may need to ensure compliance with the Illinois AI Video Interview Act's requirements, including obtaining consent from the applicant to be evaluated by the AI tool and providing the applicant with information about the types of characteristics that the AI tool uses to evaluate them. But in addition, the employer would need to account for Illinois' privacy law relating to the collection, storage, and use of the biometric data.

For example, before biometric data is collected, the Illinois' Biometric Information Privacy Act (BIPA) requires informing individuals that a biometric identifier (e.g., retina or iris scan, voiceprint, fingerprint, facial geometry scan) or biometric information is being stored or collected and obtaining a written release from the individuals subject to the storage or collection. A written release is defined as "informed written consent or, in the context of employment, a release executed by an employee as a condition of employment." It also requires a publicly available written policy that "establish[es] a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." Given that BIPA's penalties range from $1,000 in damages per violation to $5,000 per intentional or reckless violation, the potential financial exposure is immense. And while requirements between the laws overlap, a consent and disclosure for one may not necessarily satisfy the other—companies will need to pay attention to ensure that any notices and consents sufficiently address both.

Beyond laws zeroing in on biometric data (such as BIPA) and well-established employee data privacy requirements under the Americans with Disabilities Act and the Genetic Information Nondiscrimination Act, comprehensive data privacy laws have rapidly been developing into a legislative patchwork, with varying applicability to the employment context. Indeed, comprehensive privacy laws have passed in Tennessee, Iowa, Indiana, Texas, and Florida, and various states before them (numbering a total of thirteen states); however, most of these laws specifically exempt employee and job applicant data. California is the notable exception.

So What's Up With the CPRA?

New Privacy Rights and Obligations Relating to Employees and Job Applicants

The California Consumer Privacy Act of 2018 (CCPA) was amended by California voters through the California Privacy Rights Act's (CPRA) in 2020, with an effective date of January 1, 2023. Although the CCPA originally had a "personnel" information exemption, the CPRA sunsetted the exemption, and proposed bills to further extend the exemption were not adopted. The exemption therefore expired on January 1, 2023, and the personal information of employees, job applicants, directors, and independent contractors became subject to the CCPA/CPRA.

Under the CPRA, employers must inform California residents about employment-related personal information collected as well as how that data is subsequently used. Specifically, the notice must be provided at the time personal information is collected and include the period for which the data will be retained, whether the data will be sold or shared, a list of third parties used to collect the data or to whom the data is disclosed, and a description of the categories of sensitive personal information collected (e.g., genetic data, SSN, racial or ethnic origin, precise geolocation). Individuals must also be informed of their rights under the CPRA, which include the right to delete, the right to opt-out of the sale of their personal information, the right to limit the use of sensitive personal information, the right to know, and the right not to be discriminated against for exercising rights under the CPRA. While these rights are robust, there are some potentially applicable exceptions. For example, personal information retained to comply with an employer's legal obligations (e.g., for EEO-1 reporting purposes) is not subject to the right to delete, and use of sensitive personal information to provide services—and not infer characteristics—would not be subject to a right to limit.

Despite the CPRA only permitting enforcement beginning on July 1, 2023, no time has been lost to ensure compliance with these new obligations. Indeed, on July 14, 2023, California Attorney General Bonta announced an "investigative sweep" into some large employers over their compliance with the CPRA's requirements regarding the handling of employees' and job applicants' personal information.

More California Regulation Ahead

The California Privacy Protection Agency (CPPA) was established by the CPRA to implement and enforce the law. In recent months, the CPPA has made clear that it views itself as not only the preeminent data privacy regulator but also the regulator best poised to tackle automated decision-making.

On February 10, 2023, the CPPA launched a comment period on proposed rulemaking that included automated decision-making, one of the topics it was tasked by the CPRA with considering. On May 15, 2023, members of the CPPA Board raised concerns about A.B. 331—a proposed bill garnering much media attention that would have required deployers to perform an impact assessment for automated decision tools used in employment—because CPPA had already been tasked with regulating automated decision-making and, as CPPA Board Member Alastair Mactaggart put it, is "the only realistic AI regulator in North America." Shortly thereafter, on May 18, 2023, California's A.B. 331 was killed by California's Assembly Appropriations Committee.

One month later (on July 14, 2023), the CPPA hosted a board meeting in which it discussed potential language for consideration in the context of future regulations governing automated decision-making (ADM) technology. The draft language under discussion would define ADM technology as "any system, software, or process—including one derived from machine-learning, statistics, or other data processing or artificial intelligence techniques—that processes personal information and uses computation as whole or part of a system to make or execute a decision or facilitate human decisionmaking." ADM technology also expressly includes profiling. CPPA therefore appears to be considering a broad definition that goes beyond the definitions considered under the European Union's Artificial Intelligence Act and General Data Protection Regulation. The CPPA also proposed "potential thresholds" for risk assessments ranging from using ADM technology in furtherance of an array of decisions, including the provision or denial of employment or contracting opportunities or compensation, to processing personal information to train AI more generally.

Key Considerations

In light of the developing privacy regulations affecting and intersecting with AI and employment considerations, companies using AI in an employment context should take note:

- **AI in Employment and Privacy Nexus:** The evolving landscape of AI in employment requires careful attention to privacy regulations alongside legal considerations for automated decision tools in the workplace.
- **Collecting and Processing Personal Data:** AI systems process personal data for insights and predictions, including demographic and biometric information. This raises compliance requirements under both developing AI laws and established data protection regulations.

- **CPRA's Impact on Employment Data:** The CPRA has been—and is likely to continue to be—a game changer in extending privacy rights to include employment-related personal information and thereby require the disclosure of data collection practices to employees and applicants.
- **CPPA and Future Regulation:** The CPPA is emerging as a pivotal regulator for data privacy and automated decision-making. Proposed regulations by CPPA suggest that more expansive and potentially stringent rules for automated decision-making technologies are on the horizon.

Conclusion

In the intricate tapestry of AI integration in the workplace, privacy is a vital piece. As AI becomes increasingly ubiquitous in the workplace, the interplay between employment practices and privacy regulations warrants increasingly careful attention.

Cassandra Gaedt-Sheckter is a partner in the Palo Alto office of Gibson, Dunn & Crutcher and serves as co-chair of the firm's Artificial Intelligence practice group. She is also a member of Gibson Dunn's Privacy, Cybersecurity and Data Innovation practice group, where she focuses on privacy and AI regulatory compliance counseling and program development, regulatory enforcement matters, and transactional representations.

Emily Maxim Lamm is an associate in the Washington, D.C. office of Gibson, Dunn & Crutcher. Her practice focuses on employment litigation, counseling, and investigations. Emily has substantial expertise advising companies on regulatory compliance with the legal and policy developments surrounding artificial intelligence (AI) and other emerging technologies across the employment lifecycle.

			
PLI Programs you may be interested in	PLI Press Publications you may be interested in	To submit an article for consideration, please contact the editor at editor.plichronicle@pli.edu or visit pli.edu/PLIChronicle/contribute for more information	**Sign up for a free trial of PLI PLUS at** pli.edu/pliplustrial

Disclaimer: The viewpoints expressed by the authors are their own and do not necessarily reflect the opinions, viewpoints and official policies of Practising Law Institute.

This article is published on PLI PLUS, the online research database of PLI. The entirety of the PLI Press print collection is available on PLI PLUS—including PLI's authoritative treatises, answer books, course handbooks and transcripts from our original and highly acclaimed CLE programs.