Employment & Labor Law Alert

August 2022

A Privacy and Employment Law Primer: Recent Updates on Discrimination and Privacy Implications of Technology in the Workplace

Employers have increasingly used technology in the workplace to monitor and evaluate applicants and employees. These tools range from systems that monitor employee activity on electronic devices to artificial intelligence (AI) that assesses job applicants or evaluates employee work product. As reliance on these technologies has proliferated in the past several years, state and federal lawmakers have responded with increased scrutiny of these technologies, focusing in particular on two areas—employee monitoring and the use of AI in the workplace. These technologies involve different but intersecting legal concerns, including workplace discrimination and privacy.

Use of emerging technologies may differ between companies as it relates to the workplace and employment matters. Many companies use technology-enabled systems that monitor employees and aggregate data on employee behavior. Employers may elect to monitor employees' telephone communications, email, internet access, or usage of any electronic device or system, such as audio or video systems, GPS, or social media. Employers may also use biometric data (such as fingerprints) for timekeeping, door access or computer authentication systems. Similarly, employers have increased the use of AI to replace or assist with roles and duties related to human resources, including programs that assess resumes, comparing them with resumes of existing employees or with a list of criteria, or programs that analyze video recordings of applicants answering interview questions.

Unlike the EU's General Data Protection Regulation (GDPR), which provides for a comprehensive and consistent approach to data collection and data privacy with respect to the workplace and beyond, the U.S. regulatory landscape is increasingly a patchwork of increasingly complex and iterative approaches and requirements.

This primer provides guidance on a number of federal and state laws and regulations, many of them recently or soon to in effect, that apply to the use of technology in the workplace. Employers should be mindful of these laws and regulations as both federal and state regulators work to increase employee awareness of the use of technology and AI tools, protect employee privacy, and prevent the use of technology that may inadvertently discriminate against employees in a protected class. Employers that rely on these technologies may want to take steps to evaluate their programs, ensure compliance with applicable laws and protect against any potential discriminatory impact of the use of these tools.

Attorney Advertising

Regulating Employee Monitoring

Employers that choose to monitor employees should be mindful of significant legislation in this space at both the federal and state levels. Most of this legislation focuses on providing employees with adequate notice that their electronic activity will be monitored.

- **Federal Law:** The federal Electronic Communications Privacy Act (ECPA) prohibits an employer from intentionally intercepting the oral, wire and electronic communications of employees, unless the monitoring is done for a legitimate business reason or the employer obtained the employee's consent. Historically, both express and implied consent could suffice under the ECPA in certain circumstances, including the inclusion of a disclaimer in an employee handbook or electronic communications policy that explicitly provides notice to employees that the employee has no expectation of privacy in the use of the company's communications systems (emails, voicemails, IMs, Slack, etc.) and that the company maintains the right to monitor (or does in fact monitor) employee communications.
- **New York:** Layered on top of federal law, New York enacted heightened legislation that amended the New York Civil Rights Law requiring that employers secure employees' consent to electronic monitoring. The New York law, which went into effect May 7, 2022, applies broadly to an employer's monitoring of "any electronic device or system." New York employers are required to provide written notice to employees upon hiring that "any and all telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage by an employee . . . may be subject to monitoring at any and all times" and to obtain written acknowledgment from new hires. Employers also must post a similar notice in a "conspicuous place which is readily available for viewing."
- **Connecticut and Delaware:** Like New York's recently enacted legislation, a 1998 Connecticut law requires employers to provide prior written notice to employees of the types of electronic monitoring that may occur, but does not require affirmative acknowledgment. Delaware law, in August 2001, also requires employers to provide prior written notice regarding monitoring of phone transmissions, email, and internet access or usage. Delaware allows employers to choose between two methods of notification: (i) providing daily notice when the employee accesses the employer-provided systems or internet, or (ii) providing a one-time written or electronic notice to the employee and obtaining employee acknowledgment.

In addition to state laws that require employee consent and/or notice to monitor employee communications, employers should also be mindful of state laws that require employers to obtain consent from and/or provide notice to employees in order to engage in motor vehicle tracking for employees operating company-owned vehicles or vehicles that are owned/leased by employees but are nonetheless tracked and monitored by their employers. It is important to note that the laws that apply to monitoring employee communications do not apply to tracking technologies used on motor vehicles. Currently there are a handful of states in the U.S. that restrict driver tracking/monitoring for business purposes.

- **New Jersey:** New Jersey enacted legislation in April 2022 that requires employers to provide prior written notice in order to engage in motor vehicle tracking of employees using employer-owned vehicles and/or employees using their own vehicles for a business purpose. The notice must disclose that (i) geolocation tracking technology is being used by the employer and (ii) the intended uses of the geolocation data collected from the geolocation tracking technology.

In addition, there are various states that generally restrict the use of tracking devices on motor vehicles without the owner's consent. For example, both California and Minnesota have enacted legislation (in 1998 in California and in 1988 in Minnesota) that requires prior consent from the owner—and in California, the owner, lessor or lessee—of the vehicle in order to use any electronic tracking device to determine the location or movement of a person and does not have an exception for legitimate business purposes.

Regulating Privacy Rights in the Workplace

Various states have enacted legislation to protect the rights of individuals in the workplace as they relate to the use of individuals' personal information and even more specifically their biometric information.

- **California:** California's comprehensive privacy laws—the California Consumer Privacy Act of 2018 (CCPA)

and its 2020 successor, the California Privacy Rights Act (CPRA)—do not expressly address the monitoring of employee communications. Employers with a California presence may wish to consider the possible applicability of the CCPA's current general notice requirements, however. Gov. Gavin Newsom signed several amendments to the CCPA in October 2019, including Assembly Bill 25 and Assembly Bill 1355, which clarify how the CCPA applies to the workforce and indicate that employers must (i) safeguard personal information of employees and (ii) provide notice to employees regarding the collection and use of personal information by the employer.

When the CPRA goes into effect on Jan. 1, 2023, employers must comply with the requirements of the CCPA and CPRA amendments with respect to job applicants, employees, independent contractors, owners, emergency contacts and beneficiaries. Under the CPRA, these individuals must be informed that the employer is collecting their personal information, how that information is being used and to whom it is being disclosed. Under the CPRA, these individuals also must be given notice of their rights under the law and be able to exercise their options through easily accessible self-service tools, such as obtaining their personal information, deleting or correcting it, opting out of its sale, and opting out of its being shown across business platforms, services, businesses and devices.

In addition to providing employees and other individuals in the workplace certain rights with respect to how their personal information is used by their employer, many states specifically regulate the collection of biometric information. California, Colorado and Virginia treat biometric information as sensitive data. Biometric privacy laws have been enacted in a number of other jurisdictions, including Illinois, Texas, Washington state, and New York City.

- **Illinois:** Illinois was the first state to enact a law restricting the collection and storage of biometric information, and it remains on the front line for advancement of jurisprudence on the subject. The Illinois Biometric Information Privacy Act (BIPA), enacted in October 2008, requires entities, including employers, that collect biometric data to follow a number of protocols, including maintaining a written policy about the collection and storage of biometric data, providing owners of biometric information (in this case, employees) with written notice of these practices and obtaining informed consent from individuals subject to biometric data collection. Under BIPA, companies may not "sell, lease, trade, or otherwise profit [from]" an individual's biometric information; may not "disclose, redisclose, or otherwise disseminate" an individual's biometric information without consent; and must "store, transmit, and protect from disclosure" an individual's biometric information using "the reasonable standard of care" in the entity's industry.

Regulating AI Tools

While laws and regulations addressing employee monitoring largely focus on protecting employee privacy and ensuring that employees receive adequate notice of monitoring, regulations targeting AI tools typically address the potential discriminatory impact of those programs and algorithms. AI is the use of technology, such as computer systems or algorithms, to perform tasks that previously were performed by people. Various federal and state anti-discrimination laws—including Title VII, the Age Discrimination in Employment Act and the Americans with Disability Act (ADA)—protect applicants and employees from a discriminatory disparate impact of facially neutral policies and practices. This means that a "neutral" AI program that assesses applicant resumes could run afoul of anti-discrimination laws if the program results in a disparate impact on members of a protected class. Indeed, at an American Bar Association conference in Berlin, Germany, in May 2022, U.S. Equal Employment Opportunity Commission (EEOC) Chair Charlotte Burrows noted that she and the commission are particularly interested in guidance that could protect people with disabilities from bias in AI tools. As she noted, as many as 83% of employers, and as many as 90% among Fortune 500 companies, are using some form of automated tools to screen or rank candidates for hiring, leading to a renewed focus on understanding what is "under the hood" of the AI tool.

- **Federal Law:** Employers should take note of recent developments at the federal and state levels in this area. The EEOC recently issued guidance on the use of AI in employment and the risks that such tools pose with respect to disability discrimination. The EEOC indicated its intent to hold employers liable

for problems that come from software/algorithms/AI tools provided by a third-party vendor. The guidance identified several ways in which software/algorithms/AI tools can result in discrimination claims relating to disability:

- Failing to provide reasonable accommodations to applicants or employees with disabilities who need a reasonable accommodation in order to be fairly evaluated by the AI tool
- Inadvertently screening out applicants or employees with disabilities
- Inadvertently making a prohibited inquiry regarding a disability

The EEOC recommended a list of "promising practices" to avoid discrimination, including training staff and third-party vendors to recognize and process reasonable accommodation requests, using tools that have been designed with individuals with disabilities in mind, informing applicants and employees that reasonable accommodations are available, clearly describing the traits and characteristics the AI tool is designed to assess, ensuring that the AI tool measures abilities or qualifications that are essential functions, and ensuring that the AI tool will not ask applicants or employees questions that are likely to elicit information about a disability, unless such inquiries are related to a request for reasonable accommodation.

While the EEOC's recent guidance focuses on disability discrimination, disparate impact concerns apply equally to other protected classifications as well. AI tools that disproportionately screen out individuals of a certain race or gender, for example, could run afoul of Title VII. Certain facial recognition software, which is often used in AI interviews, has been shown to misidentify faces of Black or other non-white individuals at a significantly higher rate than the faces of white individuals. And another now-discarded recruiting tool disfavored resumes that contained the word "women's" (such as with respect to a college or club sport) because it was programmed to target resumes that resembled those of current employees, who were largely male.

Several states and cities have enacted, or are in the process of enacting, legislation imposing specific requirements targeting the potential disparate impact of AI tools.

- **New York City:** New York City enacted legislation, effective Jan. 1, 2023, restricting the use of AI in employment decisions unless employers take certain actions regarding the use of AI tools. The legislation targets any "automated employment decision tool," such as a score, classification or recommendation, that is used to substantially assist or replace discretionary decision making and defines "employment decisions" as decisions screening job applicants for employment or employees for promotion.

  Prior to using these tools, New York City employers must:

  - Conduct a bias audit no more than one year prior to the use of the tools, which must include testing of the AI tools' disparate impact on federally protected classes of individuals on the basis of race, ethnicity and gender. A summary of the results of the most recent bias audit must be made publicly available on the employer's website prior to the use of the tools.
  - Provide a notice to applicants or employees at least 10 business days prior to the use of any of these tools. The notice must indicate that an automated employment decision tool will be used to evaluate the employee or candidate and that the candidate or employee may request an alternative selection process or accommodation, the types of job qualifications and characteristics that the tool will use in order to evaluate candidates or employees, and information regarding the data that will be collected.
- **Illinois:** Illinois enacted legislation, the Artificial Intelligence Video Act, effective Jan. 1, 2020, governing the use of AI to evaluate video interviews of applicants. The law requires Illinois-based employers to notify applicants that "AI may be used to analyze" a video interview to "consider the applicant's fitness for the position." Employers must explain how the AI tool works and what characteristics it uses to evaluate applicants. Finally, the law requires the employer to obtain consent from the applicant and prohibits the use of such tools if consent is not granted. The law was amended in 2021, effective Jan. 1, 2022, to require

employers that rely "solely" on AI analytical tools to select candidates for an in-person interview to collect and report the race and ethnicity of both candidates who are and are not offered an in-person interview and of those who are hired. That data will be analyzed by the state, which will then produce a report on whether the data collected discloses a racial bias.

- **California:** The California Fair Employment and Housing Council on March 15, 2022, published draft modifications to its employment anti-discrimination laws that would impose liability on companies or third-party agencies administrating AI tools that have a discriminatory impact. The draft regulations would make it unlawful for an employer or covered entity to "use ... automated-decision systems, or other selection criteria that screen out or tend to screen out an applicant or employee ... on the basis" of a protected characteristic, unless the "selection criteria" used "are shown to be job-related for the position in question and are consistent with business necessity." This codifies under California state law a disparate impact standard for AI tools.

What Employers Should Be Doing Now

As both the federal government and state officials continue to enact legislation throughout the U.S. that impacts employers that use AI tools, monitor employees and/or collect employee data, companies should:

- **Assess:** Review the company's use of AI tools and consider whether the tools and use are covered by applicable law, and/or review all company practices surrounding the collection, usage, storage or transmission of any employee information covered by applicable state and local laws.
- **Audit:** Conduct bias audits of AI tools used by the employer, or ensure that third-party vendors are conducting these analyses. While not all laws require these analyses, most employers are likely subject to some kind of anti-discrimination laws and should ensure that programs they use are not running afoul of those laws. Companies should consider conducting these audits in partnership and collaboration with legal counsel.
- **Write:** Be sure that your company has clear written policies that address the procedures for collection, storage, use, transmission and destruction of employee information, including specific time frames.
- **Communicate:** Be sure to notify all individuals—employees and applicants—about the use of AI tools where required by applicable law and/or notify all individuals—employees and others—about your employee monitoring, motor vehicle tracking and monitoring, and data collection policies, including information about how such data will be secured to protect individual privacy interests.
- **Obtain Consent:** Obtain consent in a format that can be stored and, if necessary, produced as evidence of compliance with applicable law in the event of litigation.
- **Train and Consult**: Counsel is available to assist with risk assessment, policy development and training to ensure compliance with applicable laws and regulations.

Related Professionals

Ian Carleton Schaefer . . . . . ischaefer@loeb.com
Jessica B. Lee . . . . . jblee@loeb.com
Eyvonne Mallett . . . . . emallett@loeb.com
Bianca Lewis . . . . . blewis@loeb.com
Lauren Richards . . . . . lrichards@loeb.com

This is a publication of Loeb & Loeb and is intended to provide information on recent legal developments. This publication does not create or continue an attorney client relationship nor should it be construed as legal advice or an opinion on specific situations.

© 2022 Loeb & Loeb LLP. All rights reserved.

7051 REV1 08-18-2022