Bloomberg Law

Professional Perspective

Legal Implications of Using AI, Biometrics, or Bots in the Workplace

Evan Nadel and Natalie Prescott,
Mintz, Levin, Cohn, Ferris, Glovsky and Popeo

Legal Implications of Using AI, Biometrics, or Bots in the Workplace

Contributed by Evan Nadel and Natalie Prescott, Mintz, Levin, Cohn, Ferris, Glovsky and Popeo

Companies using artificial intelligence, biometrics, or bot technology should keep four critical laws on their radar. These unique laws have nationwide implications for all large companies and employers. Although they originate in Illinois and California, many states may follow their lead. Additionally, these laws are so sweeping that many companies may benefit from uniformly adopting them nationwide.

The Illinois Artificial Intelligence Video Interview Act regulates usage of AI in the hiring process. Illinois also pioneered biometric privacy laws with its Biometric Information Privacy Act, which has been followed by five other states. California has passed the much-discussed California Consumer Privacy Act, as well as its less-known but also important Bolstering Online Transparency Act, which mandates clear disclosures for companies using bot technology. Executives, leaders, and human resources professionals should understand these laws and become the gatekeepers with respect to compliance.

AI Workplace Concerns

From analyzing market data to evaluating troves of electronic data to simply searching for key data, AI tools can serve a wide range of businesses. It can also improve worker efficiency and profitability, as well as implementation of solutions aimed at billing, pricing, and marketing to better serve customer needs.

It is not surprising, therefore, that companies are beginning to turn to AI for productivity tracking, workplace surveillance, employee tracking, ergonomic tracking, or even to equip workplace safety devices. Yet, this is a new and unexplored legal landscape, and legislators are struggling to keep up. Key challenges for companies looking to integrate AI include:

- Workplace privacy concerns
- Worker displacement
- Human oversight
- Lack of AI experts in the workplace (legal, information technology, executive, human resources, etc.)
- Algorithmic biases, which can impact privacy and security and may be difficult to reverse
- Use of algorithms to hire, fire, or discipline workers
- Criminal activity
- Ownership of and responsibility for data
- Intellectual property rights, trade secrets, data breach, property damage, personal injury, etc.
- Future of AI-related litigation
- Anticipating and defending against litigation
- Invasion of personal privacy

Many companies are beginning to explore using algorithms and machine-learning technology. But, AI use brings with it legal challenges and concerns, including worker displacement, privacy implications, and bias. It remains to be seen how large companies can enjoy the benefits, growth, and efficiencies that AI solutions aim to provide, while also accounting for potential pitfalls and legal challenges. These challenges are especially pronounced due to a lack of regulations governing AI technology in the workplace.

Regulation Challenges

States and the federal government have been slow to regulate AI use. It remains unclear how it will be regulated in the future, to what extent those regulations will be enforced, and which enforcement mechanisms will govern.

The Illinois Artificial Intelligence Video Interview Act is a state-level exception. AIVIA is ahead of its time in that it governs use of a technology that a limited number of companies are implementing. Specifically, it regulates use of AI in recording and analyzing video interviews of potential job candidates. While many companies use AI in the resume-vetting process, such as when scanning thousands of resumes to identify the most suitable candidates, they do not go as far as similarly vetting new hires at the interview stage. Presumably, AI can be used to analyze a candidate's body language, interpersonal skills, facial expressions, vocal tone, and even whether the applicant is being truthful during the interview.

The use of such technology presents a number of challenges, from algorithmic biases to human oversight, privacy concerns, and potential data breach issues for any stored videos. It is unclear whether any U.S. companies actually rely on such technology, and specifically during the interviewing process itself. Nevertheless, AIVIA is an important step towards AI workplace regulation that should not be overlooked. Many states may follow the lead and expand this law to all types of hiring or employment-related decisions, not just to video recordings.

On the federal level, Congress has considered AI technology, especially in the employment and banking context, but has moved very slowly. Capitol Hill appears to be more focused on trying to understand the potential impact of AI, rather than actually regulating it, as evidenced by some legislation initiatives. For instance, S.1558, the Artificial Intelligence Initiative Act, seeks to implement a National Artificial Intelligence Research and Development Initiative. H.R.2575 aims to establish the AI Center of Excellence with its AI in Government Act of 2019. The more substantive initiative is H.R.2231, the Algorithmic Accountability Act of 2019, which seeks to require companies that use, store, or share personal information to audit their algorithms for bias and to conduct automated decision system impact assessments and data protection impact assessments.

Technology development moves faster than the law. In addition to a lack of comprehensive regulatory framework, even when piecemeal regulations and state laws are ultimately adopted, AI technology will always outpace any AI-related regulations. This is the challenge that AIVIA, CCPA, BIPA, and the B.O.T. Act are only beginning to address.

AIVIA

Illinois enacted AIVIA in Aug. 2019, with an effective date of Jan. 1, 2020. AIVIA is the first law of its kind in the U.S. It regulates employers' use of AI during the interviewing and hiring process. Specifically, if employers use AI to analyze the video recordings of the applicants' job interviews, the employers must: disclose that AI will or may be used to analyze the interview, explain how AI works and what characteristics it uses in the evaluation, and obtain consent. Recordings made during the interview cannot be shared, except as necessary for hiring purposes. Finally, the videos must be destroyed within 30 days upon request.

AIVIA does not prescribe penalties or remedies and does not expressly provide for a private right of action, which will present problems and legal challenges with respect to its enforcement. AIVIA also does not specify whether it applies outside of Illinois. One potential interpretation is that AIVIA applies only to interviews of Illinois residents. Another is that it applies to any Illinois employers or to those employers looking to fill job openings in Illinois.

What does AIVIA mean for human resources professionals? If the company is looking to use AI technology as a part of its hiring process—specifically, through video recordings—HR should be on alert. Those in charge of interviewing and hiring decisions will need to be trained on the legal requirements of AIVIA and understand its implications. And, while AIVIA is arguably limited in scope to either Illinois companies or residents, businesses should be on the lookout for copycat laws being adopted by other states. In short, knowledge of the law, proper training, and compliance are key for those executives and human resources professionals whose companies plan to use video-recording AI technology during job interviews.

CCPA

In addition to AIVIA, companies should be aware of other laws that will impact the workplace. One such key law is the CCPA. The CCPA was signed into law in 2018, with an effective date of Jan. 1, 2020. The CCPA is the first comprehensive privacy regulation in the U.S. It was heavily influenced by the EU's GDPR, and the two laws have some significant similarities.

Much has been written and presented on this subject, and the CCPA has even been dubbed the newest "privacy battleground."

The CCPA applies to businesses that collect personal data of California consumers, regardless of where the companies are located. The companies are subject to the CCPA if one of the following applies: they earn $25 million or more a year in revenue; they annually buy, sell, or share personal information of 50,000 or more consumers, households, or devices for commercial purposes; or they derive half or more of their revenue from selling consumer personal information. The CCPA also requires companies that employ California residents to provide those employees with compliant privacy notices.

Additionally, AB 25 exempts from the CCPA certain human resources data for California residents if that data was collected specifically for hiring or employment purposes. Notably, this is a one-year exemption, which will "sunset" in 2021. Not all employee data is protected for the duration of 2020, however. Rather, human resources professionals must carefully scrutinize the personal data of their employees. If the company's employee also happens to be its consumer, their personal data collected in the consumer context is still protected by the CCPA. Likewise, if the personal data of employees was collected for "voluntary" activities (such as discount or fitness programs, for example) and then used outside of work, this information will remain protected under the CCPA.

Many states have introduced copycat laws, some seeking to impose narrower, and some broader, obligations than the CCPA. However, most of these laws either have not passed or have been withdrawn or postponed. Additionally, the U.S. Congress is considering a comprehensive federal privacy legislation of its own, which would trump any state-specific laws. However, this big push for a federal privacy law has yet to gain significant traction.

BIPA

Illinois was the first state to regulate biometric information when it passed BIPA in 2008. BIPA has generated an onslaught of privacy class actions, especially in recent years. It prohibits the unlawful collection and storing of biometric information. It defines "biometric information" to include retina scans, iris scans, fingerprints, palm prints, voice recognition, facial-geometry recognition, DNA recognition, gait recognition, and even scent recognition. It imposes significant penalties for violations, ranging from $1,000 for each "negligent" violation to $5,000 for each "willful" violation.

Illinois again positioned itself as the leader in the privacy field, as BIPA remains the only biometric regulation that provides for a private right of action. Five other states have followed its lead and passed their own biometric privacy laws in recent years (Arkansas, California, New York, Texas, and Washington), but none have the same enforcement bite as BIPA.

Biometric laws significantly impact the workplace because compliance issues most frequently arise in the employment context. Since many businesses and large companies increasingly rely on biometric technology, this raises a number of privacy concerns. For example, companies utilize the employees' biometric information to monitor when employees clock in and out, or to restrict access to secure areas, to provide system login and regulate online access to sensitive data, or for productivity and ergonomic tracking. Despite its obvious advantages, use of biometric technology at work similarly raises legal concerns and opens the doors to privacy and discrimination claims.

B.O.T. Act

The B.O.T. Act, SB 1001, went into effect in California on July 1, 2019. This law, also known as the chatbot disclosure law, is another law that is one of its kind. It regulates "bots," which are defined as "automated online account[s] where all or substantially all of the actions or posts of that account are not the result of a person." It mandates companies that are using a bot to communicate with their customers or the public online to disclose this fact (for example: "I'm a bot."). The penalty for violating this law is $2,500 per violation.

Specifically, the B.O.T. Act requires all bots that attempt to influence the purchasing or voting behavior of California residents to conspicuously disclose themselves as bots. The law has the potential to address the challenges of misinformation dissemination online, including reducing the impact of false news. It can address such issues as overinflated follower counts, fake likes, and engineered retweets and reposts, reducing the seeming newsworthiness and importance of certain posts and stories. As with many other laws, however, it remains a work in progress. It is fairly ambiguous, sweepingly includes chat bots on companies' websites, and provides for AG enforcement and no private right of action.

At many companies, sophisticated software bots may replace dozens or even thousands of workers. Bots are the modern-day "digital employees" that can perform a wide variety of repetitive tasks, such as generating reports, providing virtual assistance, creating and sending invoices, verifying documents or signatures, and even communicating with consumers.

Increased reliance on bot technology and other digital technology may cost workers jobs, impact hiring, promotions, and raises, and trigger employment-discrimination and invasion-of-privacy claims. While automation does allow for many routine tasks to be performed better, faster, and inexpensively, it can also lead to invasion of the employees privacy and dictate hiring decisions that may be discriminatory under the law. Progress is inevitable, but it requires meaningful changes to privacy and employment laws, and regulators have been slow to keep up.

The absence of clear guidelines should not deter executives and human resources professionals from becoming privacy leaders at their respective organizations and beyond. Microsoft set a strong example when it announced that it will honor the CCPA across the U.S. This earned the company positive publicity and recognition and simplified compliance obligations for its leadership.

Conclusion

The laws discussed in this article are unique and apply only to discrete groups of individuals. However, the companies that operate nationwide will benefit greatly from adopting these state-specific requirements on a national basis. After all, a case-by-case or state-by-state approach is impractical in many situations. Human resources professionals and executives should lead by example, and understanding the key laws that implicate privacy rights or digital technology is the first step in the right direction.