Lessons for employers using artificial intelligence and automated decision-making software

By Lauren Daming

Greensfelder, Hemker & Gale, P.C.

The allure of artificial intelligence (AI) and algorithm-based hiring technologies is strong because they are assumed to be more efficient and less biased than human decision-makers. Software vendors guarantee more secure authentication methods, reduced personnel costs, and better surveillance of remote workers. But these methods come with an equal number of challenges: privacy concerns, lack of transparency, and the absence of comprehensive and consistent regulation. As with any new technology, before adopting AI-based software, employers should balance these competing interests, recognizing that the sensitive information collected implicates regulation from a variety of legal fields, from employment to privacy to consumer protection.

Types of technologies and applications

Common applications of AI in the workplace include "chatbots" that screen job applicants, scanners that evaluate resumes based upon keywords, video interviewing software that evaluates applicant performance based upon facial expressions and movements, and testing or monitoring software that measures desired characteristics or skills. These programs potentially capture and analyze a variety of data points, including hand scans, facial geometry, voiceprints, keystroke patterns, facial expressions, video, and images. They can also capture personal information such as an individual's physical capabilities, emotional or mental state, and protected characteristics such as age, race, or sex.

Legal issues

Unfair and deceptive trade practices

The Federal Trade Commission (FTC) Act and state equivalents prohibit companies from engaging in unfair or deceptive acts and practices. The FTC recently aimed its regulatory spotlight on AI and automated decision-making, releasing two different sets of informal guidance in the last decade.[i] Late last year, the FTC announced its intent to pass rules regulating algorithmic decision-making software in order to prevent discrimination.

The FTC has also handled complaints regarding the unfair use of AI, including one related specifically to hiring tools.[ii] In that case, software vendor HireVue's program used AI to analyze thousands of data points about each job applicant's performance video interview footage, including word choice, intonation, emotions, and inflection.[iii] The complaint alleged that HireVue's product was unreliable and prone to racial and gender bias and could disadvantage applicants with disabilities due to its measurements of facial expressions and eye contact. HireVue argued that its software had undergone an algorithmic audit that revealed no bias concerns, but it ultimately discontinued the use of its AI-enabled features as a result of the complaint.

State regulation of facial recognition analysis and collection of biometric data

In the absence of federal privacy legislation, states and cities have addressed the use of AI, algorithms, and other advances in hiring technology. Two states, Illinois and Maryland, have adopted statutes that restrict how employers may use artificial intelligence and facial recognition technologies during the hiring process. The Illinois Artificial Intelligence Video Interview Act[iv] requires employers that use artificial intelligence in evaluating video interviews to inform applicants about this technology, describe how it works, and obtain their consent. Under Maryland's statute, an employer may not use a "facial recognition service" to create a facial template during an applicant's interview unless the applicant has given consent in writing.[v]

A New York City ordinance goes a step further by prohibiting the use of AI analysis of video interviews unless the software has undergone a bias audit.[vi] Illinois recently amended the AI Video Interview Act to require companies to submit certain demographic data to the state to be evaluated for potential bias.

The collection, use, and storage of biometric information, often used for timekeeping or security systems, is regulated by statute in three states: Illinois,[vii] Texas,[viii] and Washington.[ix] The strictest of those, the Illinois Biometric Information Privacy Act (BIPA), requires companies that use biometric information to: 1) maintain a policy regarding the storage and destruction of this data; 2) obtain the informed consent of individuals before collecting their biometric data; 3) store biometric data securely; and 4) refrain from disclosing biometric data except in limited circumstances.[x] New York's less expansive statute prohibits employers from requiring employees to be fingerprinted as a condition of employment, which could limit the use of some timekeeping methods.[xi]

Data breach statutes

Every state has a data breach statute that governs how companies must respond when certain types of sensitive information are improperly accessed or stolen. More than a third of the states have included biometric information among the categories of data protected under these statutes. For example, in Delaware's data breach statute, the definition of "personal information" includes "unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes."[xii] These definitions would likely extend to facial recognition, voice identification information, or keystroke patterns that are collected and analyzed in virtual interviewing or monitoring platforms. In these states, employers must be mindful that they could be subject to data breach notification obligations if data collected from virtual interviews such as facial recognition analysis data is compromised.

Discrimination and accommodations

The use of these technologies may also introduce problematic bias into hiring or other employment decisions and create the potential for claims of discrimination. Facial recognition software is notoriously unreliable in recognizing the faces of people in some communities. A recent report from the National Institute of Standards and Technology (NIST) that tested facial recognition algorithms found significantly higher rates of false positives in women, people of color, and older

people.[xiii] This unreliability can result in the software misreading the emotions of women or people of color and thereby rating a video interview performance less favorably.

The EEOC signaled a focus on the potential for disability discrimination inherent in AI and automated decision-making technology when it issued technical guidance in May 2022. The guidance advises employers of their obligation to ensure that hiring tools using algorithms or AI do not negatively impact applicants with disabilities.[xiv] It also emphasized that employers must provide reasonable accommodations for applicants who are adversely affected by AI or automated decision-making tools due to their disabilities. The employer's obligation to vet potential bias in AI-based hiring tools — even if the software is provided by a vendor — is a key component of an employer's responsibility in ensuring its hiring practices minimize potential for bias.

Best practices

1. Scrutinize vendors

In reviewing vendors, employers need to learn as much as they can about the technology, including the following:

- What types of data are collected? Are any types of data irrelevant to the purpose of the software collected?
- Who is able to access the data? Can the vendor share it with third parties?
- Is the data stored securely? Does the vendor have a privacy policy that accounts for compliance with applicable law and industry best practices?
- How long is the data stored?
- How do the algorithms, AI, or facial recognition technology accomplish their purposes? Are they reliable? Have they been audited for potential biases? Are the companies transparent about how their technologies work? Have they been designed with the needs of various users in mind?

By assessing this information, employers can consider whether AI or automated-decision making tools are serving their goals. This can also point companies toward vendors or software that are the best fit for their purposes.

2. Consider alternatives, opt-outs, and accommodations

By identifying the clear purpose of adopting automated decision-making models, alternative methods to reaching this goal can be assessed. A company looking to maximize remote worker productivity may decide to use work logs rather than remote monitoring software to limit the amount of personal information collected about its employees. A factory concerned with time theft may allow employees to choose between clocking in via facial recognition authentication or using a unique PIN. Employers who use computer-based tests to evaluate applicants' abilities could provide alternative test formats to accommodate individuals with disabilities. The EEOC's recent guidance is a good reminder that there is no one-size-fits-all solution to hiring and employee management functions. Even if AI-based programs are adopted for the purest of reasons, employers must still be open to exploring alternatives when necessary.

3. Be transparent and educate users about the technology's scope and purpose

Notifying applicants and employees of the types of technologies used for evaluation and monitoring is an important part of the process. This should include information about how the automated decision-making tools work, what characteristics or abilities are measured, and how the process may affect individuals differently. With this awareness, workers can consider how these technologies may potentially affect their privacy rights or negatively impact their job prospects. Candidates and employees will then have meaningful choices about whether to participate in the activity and whether to seek an accommodation or alternative arrangement.

4. Handle data responsibly

Evaluation tools that incorporate AI may collect incredibly sensitive and personal information. Once this information is collected, companies need to ensure that it is stored securely, maintained only as long as necessary, and destroyed when appropriate. Data security also requires limiting access to sensitive information to only those employees or third parties with a need to know.

5. Be consistent

Once an employer has made representations about its use of technology, the company must stay consistent and fulfill its promises to applicants and employees. Any deviation from these outward expressions of policy could form the basis for an unfair or deceptive act or practice claim. Additionally, it erodes trust — a central value for individuals increasingly concerned about their data privacy rights.

---

[i] FTC, Facing Facts: Best Practices for Common Uses of Facial Recognition Technology (Oct. 2012) *available at* https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf. FTC, Aiming for truth, fairness, and equity in your company's use of AI (April 19, 2021), *available at* https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai; Using Artificial Intelligence and Algorithms (April 8, 2020), *available at* https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-algorithms

[ii] The first FTC settlement related to facial recognition technology was finalized in May 2021. In that case, the FTC alleged that Everalbum, a photo storage app developer, deceived consumers about its use of facial recognition technology and its retention of data from users who deleted their accounts. As part of a consent agreement, the company agreed to obtain user consent for its facial recognition features. The company also agreed to delete any models or algorithms developed from users' photos and videos. *In the Matter of Everalbum, Inc.*, Decision and Order (May 6, 2021), *available at* https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_decision_final.pdf.

[iii] *In the Matter of HireVue*, Complaint (Nov. 6, 2019), *available at* https://epic.org/wp-content/uploads/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf.

[iv] 820 ILCS 42/1.

[v] Md. Code, Lab. & Empl. § 3-717.

[vi] Local Law No. 144 (2021) of City of New York.

[vii] 740 ILCS 14/1 *et seq*.

[viii] Tex. Bus. & Com. Code Ann. § 503.001.

[ix] RCW 19.375.010 to 19.375.900.

[x] 740 ILCS 14/15.

[xi] NY Labor Law § 201-A.

[xii] Del. Code Ann. tit. 6 § 12B-101 *et seq*.

[xiii] NIST, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (Dec. 2019), *available at* https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[xiv] EEOC, The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees (May 12, 2022), *available at* https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence.