AI Monitoring And FCRA: Employer Compliance Essentials

By **A.J. Dhaliwal, Moorari Shah and Jim Gatto** (November 22, 2024)

A.J. Dhaliwal

Moorari Shah

Jim Gatto

As companies increasingly adopt artificial intelligence tools for monitoring and evaluating employees, financial regulators — especially the Consumer Financial Protection Bureau — are intensifying their focus on compliance requirements, making it clear that these regulatory bodies have a significant impact on employers' operations and responsibilities.

The CFPB recently issued warnings to employers regarding the use of AI in employee surveillance, particularly emphasizing compliance with the Fair Credit Reporting Act, or FCRA.

Simultaneously, the Federal Trade Commission has taken action against AI practices that potentially infringe on consumer rights, indicating that employer surveillance may be next on the list for regulatory attention.

For companies, it is essential to educate human resources and compliance staff on these evolving regulatory expectations from the CFPB, FTC and state agencies, as failing to comply could lead to substantial penalties and reputational risk. Even with a potential change in priorities with the incoming administration, state regulators appear to be primed to take up any slack in regulatory scrutiny.

In addition to employee surveillance, employers must also be mindful of laws and regulations relating to use of AI in employment decisions.

This article expands on these agencies' perspectives, delves into insights from the CFPB's October circular and offers practical compliance steps for companies.

CFPB's Circular on AI-Driven Surveillance and FCRA Compliance

The CFPB's October circular, "Background Dossiers and Algorithmic Scores for Hiring, Promotion, and Other Employment Decisions," emphasizes the application of the FCRA to algorithmically derived reports and automated employment decisions.[1] According to the circular, AI-driven assessments fall under the definition of a "consumer report" if a third-party vendor is involved, triggering FCRA requirements for transparency, accuracy and fairness.

This circular signals a significant regulatory shift by highlighting that even nontraditional entities — such as those involved in algorithmic processing and data analytics for employment — could be regulated as consumer reporting agencies under the FCRA.

The CFPB provides key clarifications on how FCRA compliance applies to AI-driven surveillance in employment decisions, particularly spotlighting new expectations for transparency, consent and data accuracy when algorithmic tools are used. These include the following.

Disclosure and Consent

Employers must inform employees in writing if they use an algorithmic surveillance tool to collect or assess data. This transparency helps employees understand how their data is used and aligns with the FCRA's requirements for consent and notification.[2]

Failure to obtain explicit consent could expose employers to legal challenges, especially as employees demand clarity on how such data-driven tools impact their performance evaluations or employment status.

Adverse Action Notices

When an AI-driven decision negatively affects an employee, such as influencing disciplinary measures, promotion denials or termination, employers are required to provide an adverse action notice. This notice must explain the specific factors considered in the decision, granting employees insight into the data used.[3]

The CFPB's expanded view under the FCRA emphasizes the importance of adverse action notifications, particularly in situations where algorithmic assessments influence an employee's standing. It is crucial for employers to ensure that AI-driven assessments do not have unintended adverse impacts and to provide actionable recourse when they do.

Data Accuracy Standards

The FCRA mandates that data used in consumer reports must be accurate. Ensuring this accuracy is critical for automated systems to avoid errors that may misrepresent the employee's conduct or work history.[4]

Accuracy becomes particularly important when using predictive models that rely on data points that may not fully reflect an employee's actual behavior or performance.

The Expansive Scope of Consumer Reporting Agencies Under the CFPB's Guidance

The CFPB's broad interpretation of what qualifies as a consumer reporting agency has far-reaching implications. The CFPB's October circular reinforced this stance, signaling that a wide range of organizations could now be seen as consumer reporting agencies if they compile, analyze or aggregate personal information in ways that affect employment, credit or housing decisions.

For employers, this means that any third-party tools used to gather or analyze data about employees may now be classified as consumer reports if they contribute to employment decisions. This classification triggers additional compliance requirements under the FCRA, including obligations to ensure data accuracy, obtain consent and provide adverse action notifications.

The circular also suggests that technology vendors providing these services to employers may now bear their own set of compliance burdens as consumer reporting agencies.

Impact on Technology and Background Report Providers

The CFPB's emphasis on the FCRA broadens the compliance landscape for companies using data-driven employee assessments, especially as tech firms increasingly provide

background checks and data analytics to streamline hiring. The CFPB has highlighted how background dossiers and algorithmic scores used in employment are equivalent to consumer reports, regardless of their digital or automated nature.

This interpretation of the FCRA affects not only traditional background report providers, but also a newer class of vendors that offer AI-driven insights and predictive analytics on employees.

Companies relying on AI-driven background checks must establish processes to disclose specific data sources and reasoning behind negative decisions, ensuring transparency for employees. Since the FCRA mandates clear reasoning for any adverse actions, employers and tech companies alike are tasked with designing systems that can explain AI decisions — something not always feasible with machine learning's complex models.

The Expanding Responsibilities of Data Providers and AI Surveillance Vendors

The CFPB's circular implies that data providers, such as AI-driven surveillance technology vendors, could be subject to consumer reporting agency obligations if their systems influence employment decisions.

Vendors that provide insights into employee behaviors, productivity or interpersonal dynamics might need to comply with FCRA standards, which include accuracy, adverse action notifications and disclosure requirements. This expansion means that even companies not traditionally associated with consumer reporting must reconsider their responsibilities when providing data used in hiring or employment decisions.

Vendors and service providers will need to adopt practices that enhance the transparency and accuracy of their data and algorithms, as well as ensure their clients understand FCRA requirements. The CFPB's growing focus on tech companies underscores the need for these vendors to implement consumer protection safeguards as they develop and deploy AI products for employment purposes.

The FTC's Role and Recent Actions in Regulating AI Surveillance

The FTC has also been actively involved in regulating AI-driven practices, primarily focusing on transparency, fairness, and preventing unfair or deceptive practices under the Federal Trade Commission Act.[5] The FTC's approach emphasizes transparency, accountability and bias prevention, with implications for companies using AI in employee surveillance.[6]

Setting the Stage for AI Compliance

Several years ago, the FTC took action against Everalbum Inc., an online photo album service that used subscribers' photos to train and model for an AI facial recognition tool the company was developing without clear disclosure or consent of that use.

The FTC's 2021 settlement with Everalbum establishes that companies using AI must be transparent about data use and obtain user consent.[7] The penalty for misuse of user content was algorithmic disgorgement, which required Everalbum to delete certain data and the AI models it created. This precedent suggests that AI-based employee surveillance tools must meet similar standards, requiring clear communication and employee consent.

Algorithmic Fairness and Transparency

The FTC's guidance highlights that AI tools should be free from hidden biases and designed to be explainable. Employers must conduct regular bias audits, especially for tools that affect employment-related decisions like hiring, promotion and retention. Companies need to ensure their AI tools are justified, fair, and aligned with ethical and legal standards.[8]

Compliance Challenges for Employers Using AI Surveillance

Employers may face the following compliance challenges from using AI surveillance.

- Employers must balance productivity monitoring with employee privacy, especially since AI algorithms can misinterpret behavior patterns.
- Transparency around AI data collection is essential. Employers should clearly communicate the purpose and extent of monitoring in alignment with the FCRA's transparency requirements.
- AI algorithms can introduce unintentional bias. Regular bias audits are crucial to prevent discriminatory practices and align with FTC fairness standards.
- AI surveillance aggregates sensitive data, posing privacy and security risks. Ensuring strong data security can help mitigate these risks and comply with FTC guidance.

State and Local Regulatory Efforts on AI in Employment

States and local governments are increasingly focused on regulating AI in employment, with an emphasis on transparency, fairness and antidiscrimination.

New York City has taken a leading role with its Automated Employment Decisions Tools Law, which became effective in July 2023.[9] This AI bias law requires employers using automated employment decision tools to conduct annual bias audits to ensure fairness.

The New York City law also requires employers to notify job candidates when AI-driven assessments are part of the hiring process, a requirement that aims to promote transparency around how AI tools affect hiring decisions. Penalties for noncompliance include significant fines, making New York City's approach one of the strictest in the nation.

Other states are following suit by exploring similar AI legislation, reflecting a broader trend toward responsible AI use in hiring and monitoring practices. For instance, California, Illinois and Maryland have proposed or considered AI-related bills that address the privacy, fairness and transparency of automated employment tools. Indeed, states are approaching AI regulation in varied ways, with some aiming to require disclosures, conduct regular audits or enforce privacy protections.

These state initiatives reflect a national trend toward greater oversight, and employers will need to stay current on state-specific regulations to ensure compliance and address ethical considerations related to AI-driven decisions in the workplace.

Key Takeaways for Employers

In light of regulatory focus from both the CFPB and FTC, below are essential takeaways for employers implementing AI-driven surveillance systems.

Ensure transparency and disclosure.

Employers should clearly disclose AI surveillance practices to employees, detailing data collection and analysis and the implications for employment decisions. Compliance with the FCRA requires these disclosures to be clear, timely and accessible.

Educate HR teams.

HR staff must be trained to recognize compliance requirements set forth by the CFPB, FTC and state regulators, including understanding FCRA mandates and implementing clear communication protocols.

Obtain informed consent.

FCRA compliance requires employers to obtain informed consent when gathering sensitive data. In practice, this means securing written or digital consent before implementing AI-based monitoring tools.

Conduct bias audits regularly.

To align with the FTC's fairness guidelines, companies should conduct bias audits to detect and correct any discriminatory patterns in their AI systems. Regular audits also mitigate potential discrimination risks.

Develop clear adverse action protocols.

Employers must establish clear protocols for adverse action notices in cases where AI influences negative employment decisions. These notices should explain specific reasons for the decision and give employees the opportunity to contest the data's accuracy.

Focus on data accuracy and fairness.

The CFPB's focus on accuracy underscores the need for employers to regularly monitor algorithmic inputs to avoid unjustified decisions. Employers should commit to rigorous data accuracy standards and quality controls.

Future Outlook: AI Regulation and the Potential Impact on Employers

AI technology's integration into the workplace has led to both productivity gains and compliance challenges. The combined efforts of the CFPB and the FTC to address AI-driven surveillance are a signal that this technology will face increased regulatory attention, particularly as companies deploy AI tools to monitor workers, evaluate performance and make employment decisions.

Employers can expect regulatory developments addressing data transparency, bias prevention and privacy protections. Possible future regulations may include:

- Detailed transparency standards or regulations that outline exactly how employers must disclose AI-driven data collection, use and analysis practices to employees;

- Bias auditing requirements that make employers perform regular bias audits on AI systems and report these findings, ensuring that AI-driven decision-making processes are unbiased and fair; and

- Data privacy and retention rules to account for the large amounts of personal data that AI surveillance often aggregates. New regulations may dictate how long employers can retain this data and specify privacy standards.

As the FTC, CFPB and other agencies continue to address these issues, employers that take proactive steps toward compliance will be better positioned to adapt to evolving standards. By following these takeaways, employers can ensure their AI surveillance practices are both effective and legally compliant.

A.J. Dhaliwal is a partner and co-leader of the consumer finance team at Sheppard Mullin Richter & Hampton LLP.

Moorari Shah is a partner and co-leader of the consumer finance team at the firm.

Jim Gatto is a partner and co-leader of the artificial intelligence team at the firm.

[1] See https://files.consumerfinance.gov/f/documents/cfpb_Background-Dossiers-and-Algorithmic-Scores-circular_2024-10.pdf.

[2] See 15 U.S.C. § 1681b.

[3] See 15 U.S.C. § 1681m.

[4] See 15 U.S.C. § 1681e(b).

[5] See 15 U.S.C. § 45.

[6] See https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-algorithms.

[7] See https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_decision_final.pdf.

[8] Note also that as part of its Artificial Intelligence and Algorithmic Fairness Initiative, the U.S. Equal Employment Opportunity Commission engaged in its first enforcement against iTutorGroup Inc. for using an AI tool that exhibited discriminatory results by weeding out resumes of older applicants. The matter settled, with iTutorGroup paying a hefty fine. See https://www.eeoc.gov/ai and https://www.eeoc.gov/newsroom/itutorgroup-pay-365000-settle-eeoc-discriminatory-hiring-suit.

[9] See https://rules.cityofnewyork.us/wp-content/uploads/2023/04/DCWP-NOA-for-Use-of-Automated-Employment-Decisionmaking-Tools-1.pdf.