MARCH 15, 2024 | AI/TECHNOLOGY, PRIVACY & DATA SECURITY

FTC Targets Employers Utilizing Worker Surveillance Technologies

When used appropriately, worker surveillance technologies like time and attendance software, video surveillance systems, GPS tracking software, and biometric technology can benefit employers in a variety of ways, including by boosting productivity, identifying internal and external cybersecurity threats, and even preventing or responding to workplace accidents. However, employers must be careful that employee monitoring programs do not run afoul of an increasingly wide range of regulators, now including the Federal Trade Commission.

In recent comments, FTC Division of Privacy and Identity Protection Associate Director Benjamin Wiseman outline the Commission's commitment to protecting worker privacy. The Commission is the nation's primary privacy regulator and its privacy enforcement tool is Section 5 of the FTC Act, which prohibits unfair, deceptive, and anticompetitive trade practices. In recent years, the Commission demonstrated its willingness to pursue novel technological issues through enforcement actions against companies utilizing AI facial recognition technologies. Wiseman warned that businesses that infringe on worker privacy risk becoming targets of FTC enforcement actions, stating:

Companies that mislead workers about worker surveillance technologies, that fail to be transparent with workers about their collection of personal information, or that deploy technologies in ways that harm workers without corresponding benefits may face liability under the FTC Act.

Wiseman specifically highlighted a focus on worker surveillance tools that collect sensitive information like geolocation and biometrics, pointing to recent actions as demonstrative of how the FTC will apply its Section 5 powers in the employment context. For instance, the FTC recently resolved cases against Data Broker X-Mode Social and Rite Aid due to their mishandling of consumer data and surveillance technologies. X-Mode Social faced allegations of selling geolocation data without adequate safeguards. Whereas Rite Aid was charged for haphazardly deploying facial recognition technology, resulting in erroneous identifications of customers.

In addition to its enforcement actions, Wiseman also pointed to the FTC's prior policy statements as guidelines for potential enforcement in the employment context:

- In a 2022 policy statement addressing gig work, the FTC outlined the application of the FTC Act to worker context – emphasizing that companies risk violating the FTC Act if they deploy surveillance technology to extensively monitor gig workers without transparently disclosing its impact on compensation or performance

assessment.

- Additionally, in a separate policy statement issued last year concerning biometric technologies such as facial recognition and iris scans, the FTC warned that companies engaging in deceptive practices or failing to inform users about their usage may violate the FTC Act.

While employers have the right to monitor their employees' activities at their place of work and in their use of business equipment, it is essential that employers are mindful of the potential for Section 5 enforcement actions when employing any monitoring software that drifts beyond those realms. When considering monitoring and collecting employee data, employers should assess whether the information collected serves a legitimate business purpose and was collected with employee consent. For employers balancing workplace privacy and legitimate business purposes, setting clear, transparent, and well-defined policies is not just a good practice, but a powerful tool in mitigating this new legal risk. If you have questions about how the Commission's new enforcement priorities might impact your organization, please reach out to the Labor and Employment Practice Group at Conn Maciel Carey, LLP.