Westlaw Today
powered by Reuters

10 tips for navigating privacy, cybersecurity and AI in the workplace

By Justin Peters, Esq., and Patricia Carreiro, Esq., Carlton Fields

APRIL 18, 2024

Employers are gathering more and more data on job applicants and employees. From using artificial intelligence ("AI") and credit scores for pre-employment screenings, biometrics for clocking-in and out, and digital technologies tracking employee engagement and production, technology is now an integral tool for addressing some of employers' greatest challenges.

This monitoring, however, is subject to an increasing number of laws and risks that employers must be aware of.

I. Increased privacy laws

Privacy rights are implicated in numerous ways in the workplace, from conducting background checks to monitoring employees' emails. In fact, several states have adopted privacy laws that address employee privacy rights and provide consequences for employers who violate them.

The average data breach costs $4.45 million, and compromised business emails accounted for $2.7 billion in losses in 2022 alone.

For example, the California Consumer Privacy Act, creates rights and obligations relating to the use, access, deletion, sales, and sharing of California job applicants and employees' personal information.

Among other things, employers must provide their job applicants and employees with a notice at collection and privacy policy outlining the employer's data practices, as well as respect certain privacy rights, such as the right to know and access the personal information collected, correct any inaccuracies, and limit certain data uses.

Other states, such as Connecticut, Delaware, and New York, require private employers to provide written notice to employees before electronically monitoring their email accounts and internet usage.

Additionally, several states, including Illinois, Texas, and Washington, have adopted laws explicitly focused on capturing and handling biometric data. Other states, such as California, Colorado, Connecticut, Iowa, and Virginia, have enacted comprehensive privacy laws that include biometric information in their definitions of personal information and impose obligations on the collection, use, and disclosure of such information.

Lastly, with the recent boom of AI, employers are also becoming increasingly curious and receptive to using new AI tools to perform workplace functions. States and local municipalities have responded by attempting to regulate the use of AI in the workplace, such as New York City's Local Law 144, which prohibits employers using an AI tool to make employment decisions unless proper notice is given and certain anti-bias measures taken.

II. Increased cybersecurity threats

With the increased use of technology throughout the workplace, cyberattacks, including hacking, have increased. In 2023 alone, cyberattacks impacted 343 million victims.[1] Between 2021 and 2023, data breaches are reported to have risen by 72%.[2]

These attacks can be extremely damaging to businesses and other organizations, particularly when class action litigation ensues. The average data breach costs $4.45 million,[3] and compromised business emails accounted for $2.7 billion in losses in 2022 alone.[4] The total annual cost of cybercrime is expected to reach $10.5 trillion by 2025.[5]

With labor and employment class actions already accounting for 40% of all class action lawsuits nationwide and data privacy and cybersecurity dominating the expected class actions arising from the use of generative AI, employers must remain cognizant of these threats and their exceedingly costly consequences.

III. Increased regulatory attention

Regulatory agencies are ratcheting up their focus on workplace privacy, data collection, and the increased use of AI, going after some of the largest employers in the country and securing substantial settlements.

FTC

The Federal Trade Commission ("FTC") has issued multiple policy statements regarding employee privacy, AI, and the risk of new

technologies in the workplace. See here[6] for its policy statement indicating its intention to pursue employers who use algorithmic tools in ways the FTC considers unfair or deceptive and here[7] for its warning on emerging technologies that misuse biometric information.

The FTC believes that the increasing use of biometric information and related technologies, including those powered by machine learning, raises significant privacy and data security concerns and the potential for bias and discrimination.

As recently stated by Benjamin Wiseman, Associate Director of the FTC's Division of Privacy and Identity Protection: "when it comes to surveillance and tracking, companies are collecting increasing amounts of personal information from workers," but "companies that mislead workers about their worker surveillance technologies, fail to be transparent with workers about their personal information collection, or deploy technologies in ways that harm workers without corresponding benefits, could face liability under the FTC Act."

EEOC

The U.S. Equal Employment Opportunity Commission has already issued guidance about AI and algorithmic decision-making tools and the potential for those tools to result in illegal discrimination under Title VII during the employment process.

OSHA

The Occupational Safety and Health Administration, which focuses primarily on employee safety in the workplace, has issued regulations[8] about the features of physical robots and robotic systems that present unusual hazards to employees.

To counter these risks and threats, employers should consider:

(1) Familiarizing themselves with the data and tools being used to evaluate job applicants and monitor employees, paying particular attention to the state residences of individuals to determine applicable law and associated obligations.

(2) Reviewing privacy notices and consents for transparency, consistency, and completeness, including ensuring all required elements are included and minimizing potential inconsistencies across multiple notices.

(3) Ensuring vendor contracts include required provisions for defining such vendors as "service providers" and providing for proper cybersecurity and oversight.

(4) Offering opt-outs, where required.

(5) Establishing a culture of compliance and training employees on the legal requirements implicated by particular practices.

(6) Investing in cybersecurity, including appropriately destroying data when no longer needed, overseeing third-party vendors, and rehearsing incident response plans.

(7) Implementing and enforcing policies around job applicant screening, employee monitoring, and the use of AI in the workplace.

(8) Rigorously testing algorithms before use and periodically afterward to ensure they do not discriminate based on protected classes.

(9) Crafting compliance programs around both current requirements and the risk of class action litigation, irrespective of its validity.

(10) Documenting their efforts.

Notes:

[1] https://bit.ly/4azPurz

[2] *Id.*

[3] https://bit.ly/3TLYmms

[4] FBI's Internet Crime Report 2022.

[5] https://bit.ly/3PLjmIM

[6] https://bit.ly/3xfmvdx

[7] https://bit.ly/3J4fYVF

[8] https://bit.ly/4aiJ6Vr

About the authors

Justin Peters (L) is an associate in **Carlton Fields'** national labor and employment practice. He represents employers in all aspects of private employment litigation, including defending claims for wrongful termination, discrimination, harassment, retaliation and leave-of-absence violations. He is based in Los Angeles and can be reached at jrpeters@carltonfields.com. **Patricia Carreiro** (R) is chair of the firm's cybersecurity and privacy practice. Based in the firm's Miami office, she is an experienced cybersecurity and privacy litigator who advises clients on privacy, cybersecurity and artificial intelligence. She can be reached at pcarreiro@carltonfields.com.

This article was first published on Westlaw Today on April 18, 2024.