Webinar 9 – May 8, 2024

Technology and Cybersecurity in the Workplace – Legal Compliance

WEBINAR OUTLINE

Technology in the Workplace

Increased Regulatory Attention
Regulating AI Tools
Employee Monitoring Technologies

Cybersecurity Compliance

Increased Cybersecurity Threats
Employer Responsibilities and Best Practices

What to Expect in 2024

HRtelligence TIPS

WEBINAR CONTENT

Technology in the Workplace

Staying compliant with evolving global regulations and legal requirements is an ongoing challenge. Analytics and AI tools can identify potential issues and create a foundation for compliance. Technology can help ensure you stay compliant, efficient and prepared for future growth.

Employers have increasingly used technology in the workplace to monitor and evaluate applicants and employees. These tools range from systems that monitor employee activity on electronic devices to artificial intelligence (AI) that assesses job applicants or evaluates employee work product.

As reliance on these technologies has proliferated in the past several years, state and federal lawmakers have responded with increased scrutiny of these technologies, focusing in particular on two areas—employee monitoring and the use of AI in the workplace. These technologies involve different but intersecting legal concerns, including workplace discrimination and privacy.

Increased Regulatory Attention

Regulatory agencies are increasing focus on workplace privacy, data collection and the increased use of AI

- FTC - The Federal Trade Commission ("FTC") has issued statements employee privacy, AI, and the risk of new technologies in the workplace
- FTC and FCC Sign Memorandum of Understanding on Continued Cooperation on Consumer Protection Issues
- FTC v. Rite Aid Corp. - Rite Aid is prohibited from using facial recognition technology for security or surveillance purposes for five years to settle Federal Trade Commission charges that the retailer failed to implement reasonable procedures and prevent harm to consumers in its use of facial recognition technology in hundreds of stores.

The proposed order requires Rite Aid to implement comprehensive safeguards to prevent these types of harm to consumers when deploying automated systems that use biometric information to track them or flag them as security risks. It also requires Rite Aid to discontinue using any such technology if it cannot control potential risks to consumers. To settle charges it violated a 2010 Commission data security order by failing to adequately oversee its service providers, Rite Aid is also required to implement a robust information security program, which must be overseen by the company's top executives. https://www.ftc.gov/industry/technology/artificial-intelligence

EEOC
The EEOC has issued guidance on AI and algorithmic decision-making tools and the potential for those tools to result in illegal discrimination under Title VII during the employment process (see below).

https://www.eeoc.gov/newsroom/eeoc-releases-new-resource-artificial-intelligence-and-title-vii

Regulating AI Tools

Regulations targeting AI tools typically address the potential discriminatory impact of those programs and algorithms.

AI is the use of technology, such as computer systems or algorithms, to perform tasks that previously were performed by people.

Various federal and state anti-discrimination laws—including Title VII, the Age Discrimination in Employment Act and the Americans with Disability Act (ADA)—protect applicants and employees from a discriminatory disparate impact of facially neutral policies and practices. This means that a "neutral" AI program that assesses applicant resumes could run afoul of anti-discrimination laws if the program results in a disparate impact on members of a protected class.

Federal Law: Employers should take note of recent developments at the federal and state levels in this area.

EEOC
The EEOC recently issued guidance on the use of AI in employment and the risks that such tools pose with respect to disability discrimination.

The EEOC indicated its intent to hold employers liable for problems that come from software/algorithms/AI tools provided by a third-party vendor. The guidance identified several ways in which software/algorithms/AI tools can result in discrimination claims relating to disability:

- Failing to provide reasonable accommodations to applicants or employees with disabilities who need a reasonable accommodation in order to be fairly evaluated by the AI tool
- Inadvertently screening out applicants or employees with disabilities
- Inadvertently making a prohibited inquiry regarding a disability

Notes:
The EEOC recommended a list of "promising practices" to avoid discrimination, including training staff and third-party vendors to recognize and process reasonable accommodation requests, using tools that have been designed with individuals with disabilities in mind, informing applicants and employees that reasonable accommodations are available, clearly describing the traits and characteristics the AI tool is designed to assess, ensuring that the AI

tool measures abilities or qualifications that are essential functions, and ensuring that the AI tool will not ask applicants or employees questions that are likely to elicit information about a disability, unless such inquiries are related to a request for reasonable accommodation.

While the EEOC's recent guidance focuses on disability discrimination, disparate impact concerns apply equally to other protected classifications as well. AI tools that disproportionately screen out individuals of a certain race or gender, for example, could run afoul of Title VII. Certain facial recognition software, which is often used in AI interviews, has been shown to misidentify faces of Black or other non-white individuals at a significantly higher rate than the faces of white individuals. And another now-discarded recruiting tool disfavored resumes that contained the word "women's" (such as with respect to a college or club sport) because it was programmed to target resumes that resembled those of current employees, who were largely male.

New York City: New York City enacted legislation, effective Jan. 1, 2023, restricting the use of AI in employment decisions unless employers take certain actions regarding the use of AI tools. The legislation targets any "automated employment decision tool," such as a score, classification or recommendation, that is used to substantially assist or replace discretionary decision making and defines "employment decisions" as decisions screening job applicants for employment or employees for promotion.

Prior to using these tools, New York City employers must:

- Conduct a bias audit no more than one year prior to the use of the tools, which must include testing of the AI tools' disparate impact on federally protected classes of individuals on the basis of race, ethnicity and gender. A summary of the results of the most recent bias audit must be made publicly available on the employer's website prior to the use of the tools.
- Provide a notice to applicants or employees at least 10 business days prior to the use of any of these tools. The notice must indicate that an automated employment decision tool will be used to evaluate the employee or candidate and that the candidate or employee may request an alternative selection process or accommodation, the types of job qualifications and characteristics that the tool will use in order to evaluate candidates or employees, and information regarding the data that will be collected.

Employee Monitoring Technologies

Employee monitoring technologies have become more prevalent in recent years, especially as the rapid growth of digital technology has streamlined surveillance platform use. However, workplace privacy is also a top priority. If you plan to use employee monitoring technology, it's crucial to understand how federal and state laws affect it and the best ways to implement these tools at your business.

What is monitoring in the workplace?

Employee monitoring refers to the methods employers use to surveil their workplaces, including staff members' whereabouts and activities. With employee monitoring, businesses aim to accomplish the following goals:

- Prevent internal theft
- Examine employee productivity
- Ensure company resources are being used appropriately
- Provide evidence for potential litigation

Employee monitoring methods include the following tools:

- **Employee monitoring software:** The best employee monitoring software shows managers how employees spend their work time. Functionality can include browser and application tracking, user activity screenshots and keystroke logging.
- **Time and attendance software:** The best time and attendance software gives your business a record of when employees work and take paid time off. These records are valuable for payment calculations and as evidence if there's a dispute over hours or vacation time. These digital systems also provide an accurate record of when employees start and end their days, helping you determine productivity levels.
- **Video surveillance:** Video surveillance systems can strengthen your business's security and productivity. Catching a thief on camera certainly reduces shrinkage costs.
- **GPS systems:** If a team's duties revolve around driving, businesses can install one of the best GPS fleet management systems to monitor driver safety, fuel efficiency and accountability.
- **Biometric technology:** Biometric time and attendance systems use fingerprint, facial, palm or iris scans to record work time. However, biometric system laws govern how biometric information is recorded, stored and used.

Regardless of the technology, some business owners may not know how far they can or should extend their authority to monitor employee activity. It's always best to turn to federal and state employee monitoring laws and regulations to establish limits.

What employee monitoring laws and regulations should you know?

Federal privacy laws, as well as most state privacy laws, give discretion to employers regarding how far they can go with employee monitoring programs. In some cases, depending on state and local laws, employers don't have to inform employees they're being monitored. However, some regulations do require employee consent.

Federal workplace privacy and employee monitoring laws.

Federal workplace privacy and employee monitoring regulations stem primarily from the Electronic Communications Privacy Act of 1986 (ECPA).

- **Business owners have the authority to monitor communications.** The ECPA allows business owners to monitor all employee verbal and written communication as long as the company can present a legitimate business reason for doing so.
- **Additional employee monitoring is possible with consent.** The ECPA also allows for additional monitoring if employees give consent. However, the ECPA consent provision can be tricky, as it might be inferred to allow monitoring of employees' personal and business communications.
- **Employers can legally look at sent employee emails.** Additionally, several federal court cases have determined that employers may legally look through employees' emails after they're sent. That's because the ECPA defines "electronic communications" as any electronic messages currently in transmission. Upon being sent, these transmissions become "electronic storage," which courts have determined employers can monitor.
- **Monitoring must be within reason.** In general, monitoring must be within reason. For example, video surveillance can be conducted in common areas and entrances, but surveillance in bathrooms or locker rooms is strictly prohibited and exposes a company to legal repercussions.
- **Business owners may need to store recordings.** Another issue arises when you retain recordings, especially of meetings. If you record meetings with employees, especially ones dealing with disciplinary actions or HR-related issues, you may be legally obligated to keep those recordings and turn them over to a court if litigation arises.

Monitoring computer web activity is separate and can fall under different legal precedents. Here's what you should know:

- **Employers can monitor web activity on company-owned computers.** Computer monitoring software solutions have various features. Some can show you precisely what employees are doing on their computers. You can monitor activities such as which websites employees browse on the business's Wi-Fi and what keystrokes they make on their company laptops. There is practically no reasonable expectation of privacy for an employee using a company device, so a good rule of thumb is to assume that anything employees do on their company-owned computer is visible to their employer.
- **Employers must carefully consider privacy laws.** While it's OK to monitor employees' computer usage to ensure they're not wasting time on social media and frivolous browsing, employers should know they risk acquiring too much information. Employers already have employees' personal data, and they can run amok of privacy laws, like HIPAA, if they disclose private information to anyone.
- **Employers must protect sensitive employee information.** Employers have the burden of protecting sensitive employee information, even if it comes from an employee's personal browsing history or private data stored on a company computer. If a data breach occurs and exposes certain sensitive information, it leaves the company vulnerable to litigation by the employee.

New York: Any private company that monitors employees in the workplace in New York must provide specific notice upon hire and in a "conspicuous place" all employees can see. An acknowledgment of monitoring must also be kept on file for each employee.

Cybersecurity Compliance

Increased Cybersecurity Threats

With the increased use of technology in the workplace, cyberattacks, including hacking, have increased.

- In 2023, cyberattacks impacted 343 million victims.
- Between 2021 and 2023, data breaches are reported to have risen by 72%
- Data privacy and cybersecurity class actions are expected to increase with the rise in the use of generative AI
- Employers should be aware of these threats and their costly consequences

Employer Responsibilities and Best Practices

Employers have a crucial role in fostering a culture of cybersecurity and providing the necessary tools and resources to protect their organization's digital assets. Here are some key responsibilities for employers:

1. Employee Training and Awareness
Employers should invest in regular cybersecurity training and awareness programs for employees. Educate employees on the latest cyber threats, such as phishing, ransomware, and social engineering attacks. Reinforce good security practices, password hygiene, safe web browsing, and incident reporting protocols. Create a culture of cybersecurity awareness where employees feel comfortable seeking guidance and reporting potential security incidents.

2. Robust Security Policies and Procedures
Establish clear and comprehensive security policies and procedures that outline acceptable use of technology, password requirements, data handling and encryption, and incident response protocols. Regularly communicate and enforce these policies to ensure employee compliance. Conduct periodic reviews and updates to align with evolving cyber threats and changing regulatory requirements.

3. Access Controls and User Privileges
Implement proper access controls and user privileges to limit unauthorized access to sensitive data and systems. Employ the principle of least privilege, granting employees access only to the resources required to perform their job functions. Regularly review and revoke access privileges

for employees who change roles or leave the organization to prevent lingering access vulnerabilities.

4. Regular Software Updates and Patch Management
Maintain an effective software update and patch management process. Regularly update operating systems, applications, and firmware to ensure the latest security patches are applied promptly. Consider implementing an automated patch management system to streamline this process and reduce the risk of unpatched vulnerabilities.

5. Collaboration and Continuous Improvement
Effective cybersecurity requires collaboration between employees and employers, as well as continuous improvement in response to emerging threats. Organizations should establish channels for employees to report security incidents, suspicious activities, or potential vulnerabilities. Encourage open communication and foster a sense of shared responsibility for cybersecurity. Regularly evaluate and enhance cybersecurity measures, conduct risk assessments, and stay informed about the latest security trends and best practices.

By embracing these cybersecurity best practices, employees and employers can work together to create a secure workplace environment. With robust security measures, ongoing training, and a proactive approach to cybersecurity, organizations can significantly reduce the risk of cyber incidents, protect sensitive information, and safeguard their reputation.

Source:
https://www.linkedin.com/pulse/cybersecurity-workplace-best-practices-employees-employers-temika

What to Expect in 2024

Focus on Algorithmic Bias and Artificial Intelligence.
The FTC continues to signal that AI and algorithms are an enforcement priority.

Increased focus on individual liability.
Regulators have been increasingly focused on individual liability.

Notes:
In 2022, FTC had named the CEO of Drizly individually in its complaint alleging data security failures at the company. This past October, the U.S. Securities and Exchange Commission (SEC) filed a complaint against the chief information security officer (CISO) of SolarWinds Corporation based on allegations that they 1) fraudulently made materially false and misleading statements and omissions related to SolarWinds' cybersecurity posture; 2) fraudulently misled the public after the discovery of cyberattacks; and 3) failed to maintain adequate internal accounting controls to protect SolarWinds' critical assets from cyberattacks. SolarWinds and its CISO dispute the allegations and are defending against the SEC's complaint.

New breach reporting requirements for non-bank financial institutions.
Starting in May 2024, non-bank financial institutions will be required to report certain data breaches and other security events to the FTC under the Gramm Leach Bliley Act Safeguards Rule.

Institutions such as mortgage brokers, motor vehicle dealers, and payday lenders will have to notify the FTC no later than 30 days after discovering a "notification event," defined as unauthorized acquisition of unencrypted customer information impacting at least 500 people. This could include any instance where unencrypted information is accessed by a third party without the consumer's consent.

New requirements for financial institutions under NYDFS Cybersecurity Rule amendments.
Under amended Cybersecurity Rules from the New York Department of Financial Services (NYDFS), state-licensed financial institutions will have to notify the NYDFS within 72 hours of a cybersecurity incident, with continuous updates on material changes or new information about the incident.

In the event of extortion payment, covered entities need to provide details about the payment within 24 hours of it being made, including the reasons for the payment, alternatives considered, and due diligence performed to ensure compliance with rules and regulations. Additional amendments create new requirements for larger "Class A entities," including a requirement to obtain an independent audit.

All covered entities will also need to 1) have a senior governing body (i.e., board or equivalent) with sufficient understanding to exercise effective cybersecurity oversight, and 2) require the CISO to timely report material cybersecurity issues to the senior governing body or senior officer.

Cyber incident reporting for companies in critical infrastructure sectors.
In March 2022, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Pursuant to CIRCIA, on April 4, 2024, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) officially published its Notice of Proposed Rulemaking (NPRM) detailing significant new cybersecurity reporting requirements. If adopted, this proposed rule would require companies in critical infrastructure sectors to report on certain cybersecurity incidents within tight timelines: 72 hours for "substantial cybersecurity incidents," and 24 hours for ransomware payments.

Covered entities include those that function in an industry that is among the 16 critical infrastructure sectors like energy, defense, government facilities, chemical, communications, and emergency services.

The public has until June 3, 2024 to submit comments.

Potential new requirements for certain LLMs and cloud providers under the AI executive order. In October 2023, President Joe Biden issued an executive order (EO) on Safe, Secure, and Trustworthy Artificial Intelligence (AI), which treats the development of large language AI models as a potential threat to national security and calls on a number of federal agencies to issue rules in 2024 addressing various aspects of these threats.

For example, entities that develop certain foundational models will become subject to new reporting requirements to the Department of Commerce (DoC), such as a requirement to share the results of "red-team safety tests." Certain cloud providers will be obligated to report any rental by a foreign person of U.S. cloud server space to train large AI models with potential capabilities that could be used in malicious cyber-enabled activity.

The U.S. Department of Homeland Security (DHS) and various other agencies are tasked with issuing guidance to mitigate AI systems' threats to U.S. critical infrastructure (e.g., power grids, water supplies, transportation, and communication networks), and other risks including chemical, biological, radiological, nuclear, and cybersecurity risks.

As both the federal government and state officials continue to enact legislation throughout the U.S. that impacts employers that use AI tools, monitor employees and/or collect employee data, companies should:

- **Review Existing Technologies Utilized**: Review the company's use of AI tools and consider whether the tools and use are covered by applicable law, and/or review all company practices surrounding the collection, usage, storage or transmission of any employee information covered by applicable state and local laws.

- **Audit**: Conduct bias audits of AI tools used by the employer, or ensure that third-party vendors are conducting these analyses. While not all laws require these analyses, most employers are likely subject to some kind of anti-discrimination laws and should ensure that programs they use are not running afoul of those laws.

- **Policies**: Implement and enforce policies around job applicant screening, employee monitoring, and the use of AI in the workplace. In addition, be sure that your company has clear written policies that address the procedures for collection, storage, use, transmission and destruction of employee information.

- **Communication**: Be sure to notify all individuals—employees and applicants—about the use of AI tools where required by applicable law and/or notify all individuals—employees and others—about your employee monitoring, motor vehicle tracking and monitoring, and data collection policies, including information about how such data will be secured to protect individual privacy interests.

- **Obtain Consent**: Obtain consent in a format that can be stored and, if necessary, produced as evidence of compliance with applicable law in the event of litigation.