LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Complying With Electronic Monitoring Laws In NY And Beyond

By **Harris Mufson and Lizzy Brilliant** (May 19, 2022, 12:22 PM EDT)

Harris Mufson

Lizzy Brilliant

Employers routinely monitor employees' use of electronic systems, including email, phone and internet. Reasons for monitoring employees' use of electronic systems vary depending on the employer and industry.

For example, many employers monitor employees to track performance and productivity. Others conduct surveillance to ensure compliance with internal policies and procedures, including prohibitions on discrimination and the disclosure of confidential information and trade secrets.

Some employers, including many in the financial services industry, are required to monitor employees for regulatory reasons. And employers from various industries use electronic surveillance to protect against cybersecurity breaches.

Following an emerging trend at the state level, starting May 7, all employers in New York have certain notice obligations regarding their surveillance practices. Specifically, employers must provide advance written notice to new employees that they do or plan to monitor or intercept their use of any electronic systems.

The notice must be in writing — either hard copy or electronic — and it must be acknowledged by new employees. New York employers need not obtain written acknowledgements from existing employees, but they will be required to post a notice in a "conspicuous place which is readily available for viewing" by existing employees subject to electronic monitoring.

Notably, the law does not apply to processes that are (1) designed to manage the type or volume of incoming or outgoing electronic mail or telephone voicemail or internet usage; (2) not targeted to monitor or intercept the activities of a particular individual; and (3) performed solely for the purpose of computer system maintenance and/or protection.

Moreover, employees whose communications or internet usage are monitored without notice cannot sue under the new law since there is no private right of action. Rather, employers who are determined to have violated the law will be subject to fines imposed by the Office of the New York State Attorney General.

Such fines can be up to $500 for the first offense, $1,000 for the second offense, and $3,000 for the

third and each subsequent offense.

An Emerging Trend

New York is the third state — after Connecticut and Delaware — to require private employers to provide notice of electronic surveillance to employees.

In 1998, Connecticut enacted a similar law that imposes fines against employers that fail to notify employees of their surveillance practices. The Connecticut law does create some exclusions that do not exist in New York.

For example, employers in Connecticut need not notify their employees of electronic monitoring if the employer has reasonable grounds to believe an employee is violating the law, is violating the legal rights of the employer or other employees, or is creating a hostile work environment and electronic monitoring would produce evidence of such conduct.

Connecticut also creates an exclusion for monitoring and intercepting electronic communications in the course of any criminal investigation.

Delaware's law prohibits employers from monitoring or intercepting "telephone conversation or transmission, electronic mail or transmission, or Internet access or usage" without providing employees with prior notice. Unlike the New York law, Delaware employers are required to receive written acknowledgments from new and existing employees or provide daily notifications to employees.

These electronic surveillance notification laws are part of a larger trend of new workplace privacy laws at the state and local level. Since 2012, at least 27 states have enacted laws limiting employers' ability to access employees' private social media and other online accounts.

For example, Illinois and Michigan prohibit employers from requiring or coercing employees or job applicants to authenticate access to or provide employers with passwords or account information related to the individual's personal online accounts. Laws in Delaware and Maine go further, barring employers from requiring or even requesting that employees or job applicants permit the employer to view private social media accounts.

Illinois, Texas and Washington have enacted laws that regulate collection, storage and disclosure of employees' biometric information. New York City recently passed the Biometric Identifier Information Law that prohibits commercial establishments from selling or sharing customers' and employees' biometric information.

And the California Consumer Privacy Act — as of now — requires at least notices to applicants and employees of how employers collect and use their data. Starting Jan. 1, 2023, the California Privacy Rights Act, which amends and expands the CCPA, is set to additionally provide employees with rights relating to the personal information collected by employers subject to the law, including rights to access, delete, opt out of the sale or sharing of, and correct their personal information.

Other Notice and Disclosure Requirements For New York Employers

New York's new electronic monitoring law adds to a laundry list of notice and disclosure requirements for employers in New York.

For example, New York employers are already required to provide employees with notice of their rights under New York Labor Law Section 740, which prohibits retaliation against whistleblowers, and Article 23-A of New York's Corrections Law, which sets forth the factors employers may consider in hiring an applicant convicted of one or more criminal offenses.

Effective Jan. 1, 2023, New York employers will also be required to provide notice to employees and applicants regarding any use of artificial intelligence tools to evaluate their prospects for hire and promotion.

Best Practices to Ensure Compliance

In light of the dramatic increase in remote work, employers should closely track the patchwork of privacy laws on the state and local level to ensure compliance.

In terms of the new requirements in New York, employers should draft new policies or update existing ones to ensure that the policies clearly notify employees what electronic systems and communications may be monitored and post that policy in an accessible location in the workplace or on their intranet site.

Employers should also prepare notice and acknowledgement forms for new employees to review and sign upon hire and ensure they are maintaining those forms in a secure file that can be easily accessed in the event of an audit. Employers may also consider reminding employees of their surveillance practices during routine trainings.

Harris M. Mufson is a partner and Lizzy Brilliant is an associate at Gibson Dunn & Crutcher LLP.