ADVOCACY
TALENT
IMPACT
What you need to compete.

State Laws Governing Employee Electronic Surveillance

The rise in remote work has led to a rise in employers using electronic monitoring software. Billed as a way to maintain productivity outside the office, these programs offer employers a range of features, including keystroke logging, email surveillance, location-based tracking apps for company-owned cell phones, screenshots of workers' computers and, in some cases, access to webcams. According to the Society for Human Resource Management (SHRM), by June 2020, 26% of employers were passively tracking their remote employees.

Excessive, clumsy, or improper employee monitoring can cause significant employee morale problems and, worse, create potential legal liability for privacy-related violations of statutory and common law protections. Advancements in technology have made it easier to monitor remote employees, and by extension easier to violate the law for employers that are not careful.

When agencies make the decision to implement new electronic monitoring and surveillance tools, they need to plan carefully, have the right team in place, review policies and applicable state and federal law, and be prepared to address problems when they arise. A best practice, and in line with all employee electronic surveillance laws, is to get employees' consent for monitoring in writing.

Below is a summary of current federal and state laws and regulations governing notice of monitoring of employee e-mail communications and internet access.

Federal

At the federal level, the only limit to employer surveillance comes from the Electronic Communications Privacy Act (ECPA), a law passed by Congress in 1986. ECPA prohibits employers from deliberately eavesdropping on purely personal conversations that an employee may have at work. ECPA does not, however, prevent the employer from eavesdropping on business-related conversations, or protect purely personal communications that occur through means other than the spoken word (such as email).

The Stored Communications Act (SCA) is part of the ECPA and prohibits an entity providing an electronic communication service to the public from knowingly divulging the contents of an

electronic communication. It applies only to communications in which the employee had a reasonable expectation of privacy. When an employer makes it clear that certain communications are not protected, the SCA likely will not apply.

Some observers have argued that the ECPA's electronic monitoring restrictions do not apply to Internet use because viewing websites does not involve a "communication." However, agencies should not risk additional liability when the safest route is to establish and implement a clear policy governing appropriate workplace Internet use and expressly reserving the right to monitor such use without further notice.

New York

In November 2020, New York Governor Kathy Hochul signed into law a bill that will require New York private sector employers to provide written notice to employees before engaging in electronic monitoring of their activities in the workplace. Civil Rights (CVR) Chapter 6, Article 5, Section 52-C*2 will take effect six months after enactment, i.e. May 7, 2022.

Under the law, electronic monitoring in the workplace includes monitoring of employees' telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage of or by an employee by any electronic device or system, including but not limited to the use of a computer, telephone, wire, radio, or electromagnetic, photoelectronic or photo-optical systems. As part of the law, prior written notice of the electronic monitoring must be issued at the time of hiring and must be acknowledged by the employee in writing or electronically. In addition, the notice must be posted in a conspicuous place readily available for viewing by employees.

With no private right of action included, the New York attorney general has exclusive enforcement authority. Failure to comply with the law's notice requirements may subject the employer to a civil penalty of $500 for the first offense, $1000 for the second offense, and $3000 for the third and each subsequent offense.

Connecticut

Pursuant to Connecticut Gen. Stat. § 31-48d, employers who engage in any type of electronic monitoring must give prior written notice to all employees, informing them of the types of monitoring which may occur. "Electronic monitoring" means the collection of information on an

employer's premises concerning employees' activities, or communications by any means other than direct observation, including the use of a computer, telephone, wire, radio, camera, electromagnetic, photo-electronic or photo-optical system, but not including the collection of information for security purposes in common areas of the employer's premises which are held out for use by the public. This requirement, thus applies to employer monitoring of email, voicemail, telephone use, computer use, Internet use, and the use of other similar technology.

An ordained exception to the required written notification, if an employer has reasonable grounds to believe that employees are engaged in illegal conduct and electronic monitoring may produce evidence of this misconduct, the employer may conduct monitoring without giving prior written notice.

Both private and public sector employers are covered by the statute. If an employer is found to be in violation, the state's Labor Commissioner can direct the state's attorney general to levy a civil penalty of $500 for the first offense, $1,000 for the second offense, and $3,000 for the third and each subsequent offense.

Delaware

Per Delaware Code § 19-7-705, an employer is not permitted to monitor or intercept an employee's telephone conversations, email or internet usage without prior notice in writing or alternatively notification, day of, each time the employee accesses the employer-provided email or Internet access services. Exceptions are allowed for processes that are performed solely for the purpose of computer system maintenance and/or protection, and for court-ordered actions. The law also provides for a civil penalty of $100 for each violation, enforceable by the state's attorney general.

In addition, both **Colorado** and **Tennessee** have employee electronic surveillance laws for employees of state agencies, institutions, or political subdivisions.

Given New York's recent action and the ongoing adaptation to a new rise in remote work, we expect that there may be additional state laws introduced in the 2022 session. SHRM's toolkit on managing workplace monitoring and surveillance can serve as an additional resource on this topic.