EMPLEE MONITORING AND SURVEILLANCE (WASHINGTON)

Employers are increasingly monitoring and conducting surveillance activities on their employees in order to protect the organization’s business interests and ensure a safe and productive work environment. The use of surveillance and monitoring techniques raises a number of legal issues, making it important for an employer to develop and implement effective monitoring and surveillance policies and practices. To avoid liability, protect everyone’s basic right to privacy and promote a respectful, trusting environment, employers need to have a basic understanding of privacy law and enforce whatever boundaries they can. Special rules apply to monitoring a unionized workforce and they are addressed below.

KEY QUESTIONS TO ASK BEFORE YOU BEGIN

1. Are there factors creating a need for surveillance in the workplace?
   a. Productivity concerns – do employees perform significant work without supervision, such that the employer has reason to check productivity, attendance, etc.?
   b. Misconduct concerns – are there concerns employees are using equipment for inappropriate or illegal purposes (e.g., running a side business, surfing porn, etc.)?
   c. Theft or vandalism concerns

2. To what extent are your employees using employer-owned equipment?

3. Will employees be permitted and/or encouraged to bring their own devices to work? (For more information on bring-your-own-device (“BYOD”) practices, please see the BYOD Keynote.)

LEGAL CONCERNS

The following areas of the law are implicated by monitoring and surveillance practices:

- Employee privacy – constitutional, statutory, and common laws
- Labor laws

Employers can reduce certain legal and business risks by intentionally creating a monitoring and surveillance policy that is clear and comprehensive as to the types of equipment and information subject to surveillance and places employees on notice of the diminished privacy expectations of the workplace.

I. PRIVACY IMPLICATIONS

A. THE LAW

1. Constitutional Law. Because “state action” is required to state a claim for invasion of privacy under the United States Constitution and the State of Washington Constitution, those Constitutions have extremely limited applicability to the private workplace.

2. Statutory Laws. Employer access to private employee online accounts and interception of voice or video communications may implicate The Stored
Communications Act, 18 U.S.C. § 2701 et seq., and/or the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510 et seq. The statutes have specific rules regarding circumstances under which an employer may obtain access or record (intercept) those kinds of communications.

3. Common law provides limited protection to employees’ communications. The common law invasion of privacy tort is comprised of three subcategories that may reasonably be implicated by the employment relationship: intrusion upon seclusion; public disclosure of private facts; and placing an individual in a "false light".

   • Turns on whether, under the circumstances, the employee had a "reasonable expectation of privacy" in the particular activity being monitored by the employer.
   
   • Courts have decided that no reasonable expectation of privacy exists for employees when using company’s computer or other electronic communications system or device for personal purposes.
   
   • There is no reasonable expectation of privacy in blog or internet posted comments, including social networking sites.

B. APPLICATION TO EMPLOYER SEARCHES, GENERALLY

At some point it may become necessary for an employer to conduct a search of employee property or work areas. This need may arise, for example, if an allegation is made of drug possession in the workplace, or if some other misconduct is suspected for which physical evidence is alleged to be located in an employee’s belongings.

Employee challenges to employer searches are based on a cause of action known as privacy torts.¹ The tort of invasion of privacy actually covers four distinct causes of action, but only one, “intrusion into an employee's seclusion,” is relevant to private sector workplace searches. An intrusion into seclusion occurs where an employer intentionally intrudes into an area in which the employee has a reasonable expectation of privacy and the intrusive act would be highly offensive to a reasonable person—for example, a restroom and locker room.

Fortunately, employee expectations of privacy are relatively easy to remove through a policy which informs employees of the company’s right to search both company and personal items when it feels the need to do so. See Archbright’s sample policy on Searches.

Notwithstanding a clear policy about privacy expectations, employers must always conduct any search in a reasonable manner because even authorized searches may violate an employee's privacy if done in a highly offensive manner.

¹ The Fourth Amendment to the Constitution, which prohibits "unreasonable searches and seizures" of persons and property, only limits action by government entities and employers, such as an unwarranted police search or drug testing of government employees. The U. S. and Washington State Constitutions do not prohibit private sector employer searches of employees or company property. Even public sector employers may engage in such searches if they are narrowly tailored to a legitimate business purpose and the employee has no expectation of privacy in the system or property at issue. Unfortunately, many employees believe incorrectly that they have some inherent constitutional right which prohibits employers from conducting workplace searches.
The following recommendations will reduce an employer's liability against lawsuits for workplace searches.

1. Remove employee expectations of privacy by implementing a policy that reserves the right to search areas including e-mails, internet usage and text messaging on company-provided systems, offices, work areas, desks, lockers, bags, cars on company property and personal belongings.

2. Conduct searches in response to a business related concern and limit any search to what is reasonably necessary for your needs. Simply searching for "anything of interest" raises the risk of the search being considered unreasonable.

3. Never conduct body searches. Never search employees' personal (i.e., Comcast, gmail) accounts, even if they access them from company computers.

4. Do not perform employee searches in public. Rather, conduct it in a private area with a management witness. If searching an employee work area, conduct the search when co-workers are not present if possible.

5. Never force a search on an employee or retain an employee in an area against his or her will. Treat employee refusal to cooperate with a search order as insubordination, forewarn the individual of the probable consequences of such refusal and discipline accordingly upon refusal.

C. APPLICATION TO EMPLOYER-OWNED EQUIPMENT VS. EMPLOYEE-OWNED DEVICES

No Expectation of Privacy in Employer-Owned Equipment

Employees must be educated that they have no expectation of privacy while using Company-owned equipment or resources. An effective policy will state clearly that the Company has the right, at any time, to monitor and preserve any communications that utilize the Company's networks in any way, including data, voicemail, telephone logs, internet use, network traffic, etc. Your employee handbook should advise employees that they should have no expectation of privacy in communications made using the company network. The policy will state, further, that no employee shall knowingly disable any network software or system identified as a monitoring tool. See Archbright's sample policy on Computer, E-mail and Internet Access in the workplace. If your employees have acknowledged receipt of the handbook, asserting an expectation of privacy while using company systems, including email, would be unreasonable.

Diminished Expectation of Privacy in Employee-Owned Devices

Employees have a limited expectation of privacy in personal devices used for work purposes. Accordingly, the bring-your-own-device "BYOD" policy must set forth circumstances under which monitoring and access to employee-owned devices will occur. See Archbright BYOD sample policy.

D. APPLICATION TO AUDIO AND VIDEO SURVEILLANCE

Special problems arise when an employer desires to monitor employees through audio or video surveillance. While the use of audio surveillance is most problematic and requires explicit consent by those being recorded, the use of video surveillance is
generally permitted so long as appropriate notice to employees is provided and limitations on scope and use are observed.

**Audio Recording**

Generally, the ability to secretly record a conversation depends on whether or not the participants have a “reasonable expectation of privacy.” If there is no expectation of privacy to a particular conversation between two or more parties, generally, any party can hit the record button. There may, however, be a greater expectation of privacy held by parties to a conversation when it comes to a non-party recording their conversation. A non-party would probably be violating the privacy rights of the parties to the conversation if their expectation of privacy was indeed reasonable under the specific circumstances.

So what about conversations in the workplace? With respect to verbal communications, the specific circumstances will dictate whether or not common law privacy rights are implicated. The law does not permit an employer, or anyone else, to simply declare that employees have no expectation of privacy in the workplace. Each situation calls for a separate analysis under the applicable laws.

In addition to common law privacy rights, federal laws regulate specific aspects of privacy. The federal ECPA prohibits the intentional interception or disclosure of any wire, oral, or electronic communication where there is a reasonable expectation of privacy. As its name infers, the Act means that you cannot “hack” into a system to spy on someone or listen in on a conversation to which you were not invited. There are two exceptions.

1. When one party to the communication consents.
2. When telephone extension equipment is used to monitor communications in the ordinary course of business. This situation occurs when, for example, your customer service call is “monitored for quality assurance.”

Washington law takes privacy protection one step farther. Washington is a “two-party consent” state, meaning that it prohibits individuals from intercepting or recording a private telephone call, in-person conversation, or electronic communication unless all parties to the communication consent. Specifically, RCW 9.73.030 (1)(b) makes it unlawful to record any private conversation without first obtaining the consent of all the persons engaged in the conversation, subject to a few very specific (and rare) exceptions. Whether a conversation or other communications is "private" depends on a number of case-specific factors, such as the subjective intention of the parties, the reasonableness of their expectation that the conversation would be private, the location of the conversation, and whether third parties were present. You should always get the consent of all parties before recording any conversation that common sense tells you is private.

Therefore, it is against the law for employers or employees to record a conversation without the consent of all parties involved. Even an employer who innocently comes into possession of an audio recording that was illegally obtained should beware. Suppose, for example, an employee provides a recording to you as “evidence” of wrongdoing in the workplace. If the evidence was unlawfully obtained in the first place, it would be subject to attack (exclusion) in a court proceeding. Employers performing investigations are well advised to perform a full and fair investigation of the allegations without relying on this recorded “evidence.”
**Video Recording**

Video surveillance is not expressly prohibited by the ECPA. Employers should be cautious of setting up video surveillance in areas of the workplace in which employees have reasonable expectations of privacy in order to avoid common law claims for invasion of privacy. For example, recording in a restroom would violate an employee’s reasonable expectation of privacy. Employers should also consider informing employees of the possibility of video surveillance and document the need for such surveillance. Cameras in plain sight in the workplace, qualifies as a notice of their use.

**E. APPLICATION TO VEHICLE AND EMPLOYEE TRACKING METHODS (GPS)**

Employers are increasingly utilizing Global Positioning System (GPS) software to track movements of company vehicles and even employees. Challenges to employers’ use of GPS monitoring have been unsuccessful to date, making GPS tracking a viable alternative for employers who proceed with caution. The same principles of common law privacy torts apply to the use of GPS technology, which means it is a sound practice for employers to place employees on notice of the reduced expectation of privacy in their movements.

At a minimum, the employee handbook should place employees on notice that their movements are being tracked. For example, for vehicles equipped with GPS monitoring, the handbook should state that all vehicles are tracked through GPS, allowing the company to track vehicle movement 24 hours a day. The policy should explain what the GPS tracks; for example, in the case of vehicle tracking, the GPS would track location, miles, speed, etc. Finally, employees should be placed on notice of the consequences for deviating from location requirements or discovery of other legal or policy violations through the GPS data obtained by the employer.

**II. LABOR LAW IMPLICATIONS**

**A. “PROTECTED CONCERTED ACTIVITY”**

The National Labor Relations Act (NLRA) guarantees employees the right to organize and engage in other concerted activity for mutual aid or protection, or to refrain from engaging in such activities:

Section 7 – Employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection, and shall also have the right to refrain from any or all of such activities...

Section 8(a) – EMPLOYER UNFAIR LABOR PRACTICES. (a) It shall be an unfair labor practice for an employer –

Section 8(a)(1) – INTERFERENCE, RESTRAINT, COERCION. (1) To interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in Section 7.

- Under the NLRA, it is unlawful for an employer to observe or spy on employees who may be engaging in union activities. Supervisors must refrain from listening in on employee conversations regarding union activities, observing
who attends meetings or in any other way trying to determine who the union activists may be.

Monitoring of employee communications and activities can amount to prohibited “surveillance” under the NLRA if the employees are engaging in protected, concerted activity. This is true even if the workforce is not unionized, and even if a union is not actively campaigning to organize a bargaining unit at the organization. An organization that implements an otherwise neutral policy of surveillance and monitoring should be especially careful not to state or imply that the purpose of those efforts is to ascertain employee opinions about terms and conditions of employment. Moreover, an employer’s use of evidence obtained through monitoring or surveillance activities should be limited to addressing the specific investigatory concerns from which implementation of the monitoring arose in the first place.

B. MANDATORY SUBJECT OF BARGAINING

For employers who have a unionized workforce or are in the process of negotiating a first union contract, installation and use of video surveillance cameras is a mandatory subject of bargaining. Installation and use of such cameras are analogous to physical examinations, drug/alcohol testing requirements, and polygraph testing, all of which the National Labor Relations Board has found to be mandatory subjects of bargaining. It is an unfair labor practice to set up surveillance of a union workforce without bargaining with the union. An employer must bargain with unions over use of hidden cameras and provide information about such cameras, despite an employer's claims that bargaining over cameras would defeat the purpose of having them and that bargaining would be too cumbersome. Some guidelines for bargaining over the use of video or audio surveillance include:

1. When an employer bargains over hidden cameras, its negotiations may include the purposes for surveillance and the general buildings or types of work areas where hidden surveillance may be used.

2. An employer and union representatives may also bargain over whether hidden cameras can ever be used in the workplace. In the event that an employer cannot come to an agreement with unions on hidden video surveillance, but does not want the issue to cause a wedge in other subjects of bargaining, cameras are not the only way that a company can investigate employee misconduct. A company may use private investigators to uncover such misconduct.

3. Installing directly visible cameras may also be a solution.

4. As mentioned above, an employer and a union may bargain over the general areas in which hidden cameras may be used. This does not, however, suggest that the employer must disclose each location. Instead an employer may bargain with the union to install cameras in certain types of work areas without detracting from the secrecy of the precise location.

5. Another possible issue that can be bargained over is the level of suspicion that must be held by the employer before hidden cameras are utilized. Such an agreement does not jeopardize the investigative value of hidden cameras since the specifics of location are not at disclosed. While perhaps cumbersome, its results may eliminate disputes with a union whose membership fears hidden cameras being installed without cause.
6. During the bargaining process, employers can also agree not to use cameras as a sole basis for disciplining employees as another way to preserve the efficacy of using hidden cameras. In such a situation an employer would agree to investigate further if the hidden cameras revealed suggestions of employee misconduct and find additional means to discipline such misconduct.

7. The NLRA requires parties resolve their differences through good-faith bargaining; it simply directs an employer to initiate an accommodation process, and bargain to agreement or impasse with the union. The law does not eliminate an employer’s management right to use hidden or direct view cameras. If the disclosure of the location of the cameras defeats their purpose the employer can provide that information to the union under a confidentiality agreement to preserve the level of confidentiality necessary to allow for the continued effective use of such devices.

CONCLUSION

Employee monitoring and surveillance practices raise a myriad of legal and human resources issues. Prior to implementation, monitoring and surveillance policies should be closely scrutinized for their potential impacts on employee privacy and labor laws. Employers should always consult an Archbright attorney in developing and before implementing policies in the workplace.

DISCLAIMER: This information is general in nature and is meant as a best practices guide for members of Archbright. As such, it is not intended to be, nor should it be used as, legal or management advice. If you have a question about a specific situation, please contact an Archbright professional staff member at (206) 329-1120.