Current Developments in Workplace Privacy

Prepared by:
Barbara G. Stephenson
Sheehan & Sheehan, P.A.

LORMAN EDUCATION SERVICES
June 2016

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 700 available
- ☑ **Slide Decks -** More than 1700 available
- ☑ **White Papers**
- ☑ **Reports**
- ☑ **Articles**
- ☑ **... and much more!**

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: **www.lorman.com/pass/?s=special20**

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

Current Developments in Workplace Privacy

A. EMPLOYEE SURVEILLANCE

1. Overview

Increasingly-sophisticated technology provides an employer with multiple forms of employee surveillance. Drones are even emerging in this area. Nevertheless, just because an employer can surveil its employees in multiple ways, should it? An employer should consider the practical and legal consequences before any type of surveillance program is initiated.

2. Legal Limits

Regarding the use of audio surveillance, New Mexico is a "one party consent state," which means that at least one party to a conversation must consent to its recording. *See* NMSA § 30-12-1(C) and (E). In other words, an employer can record telephone or in-person conversations without an employee's consent and, absent company policy, an employee can engage in the same activity.

No New Mexico statutes restrict video surveillance, although common law has created a prohibition providing an employee with a "reasonable expectation of privacy" in such areas as bathrooms or dressing rooms. Video surveillance of employees, which frequently is done for reasons of loss prevention, safety or security, most likely will be done in areas where work is being done. Employees should have no reasonable expectation of privacy in these areas.

In addition to the common sense restrictions on video or audio recording in private spaces at work, before conducting surveillance, employers should have a clear and concise video surveillance policy describing the scope and methods of surveillance. In the case of *Hernandez v. Hillsides, Inc.*, 211 P.3d 1063 (S. Ct. Cal. 2009), the court found that because a

hidden surveillance system in an employee's office was narrowly tailored in time, location, and scope and installed to prevent overnight downloading of pornography, there was no invasion of privacy. The *Hernandez* decision notwithstanding, employers may well be advised to clearly mark surveillance cameras and put employees on notice that their activities may be recorded.

3. NLRB Ruling

The most significant recent development on the subject of recording at work involved a policy which prohibited ***employees*** from recording. Nevertheless, this decision is equally applicable to employer activities.

In December 2015, the National Labor Relations Board ("NLRB") in *Whole Foods Market, Inc.*, 363 NLRB No. 87 (December 24, 2015), struck the Whole Foods policy that barred employees from recording at work. The policy prohibited employees from recording conversations, phone calls, images, or company meetings with any recording device (cell phones, digital recording devices, and digital cameras) unless management approved in advance or unless all parties to the conversation consented. Employees also were barred from recording discussions with each other. The policy's stated purpose was to eliminate chilling the expression of views that might exist if one person was concerned that a conversation with another was being secretly recorded.

In finding the Whole Foods policy unlawful, the NLRB ruled that photography and audio or video recording in the workplace, as well as the posting of photographs or recordings on social media, are protected by Section 7 of the National Labor Relations Act ("NLRA") as long as "the employees are acting in concert for their mutual aid and protection and no overriding employer interest is present." The NLRB feels that recording images of protected

picketing, documenting unsafe workplace equipment or conditions, documenting and publicizing discussions about terms and conditions of employment, documenting inconsistent application of employer rules, and recording evidence to preserve it for later use in employment-related actions are examples of protected activity. Consequently, the recording by employees of activities of this type cannot be prohibited. The reverse of this, of course, would be that an employer cannot surreptitiously record employee activities of this type.

It is felt that the NLRB's decision still allows an employer to have a "no recording" policy where there is a valid business reason. For example, a recording restriction should be defensible if its purpose is to protect an employer's confidential processes, recipes, security systems, technology or other proprietary information or to protect customer, client or patient privacy. The burden will be on the employer to prove a valid business reason justifies the manner in which a "no recording" policy is drafted.

Under the *Whole Foods* decision, as noted, employers clearly cannot surveil activities protected by Section 7 of the NLRA. Where employers do use video or audio surveillance, they must be able to show they have a valid business justification for that surveillance.

B. WORKPLACE SEARCHES

1. Overview

Although current discussions about workplace searches may focus on "electronic searches" of email and electronic devices, employers still may need to search lockers, desks, equipment, and the like in order to protect proprietary information, for reasons of safety, and other legitimate business purposes. Such searches should be done under a written policy communicated in advance to employees. Public employers must conduct searches with caution.

These employers are "public actors" having obligations under the United States and New Mexico Constitutions and searches may violate Fourth Amendment rights on searches and seizures. Whether a search of a public employee's desk or locker is lawful depends on whether there was an expectation of privacy as to the area searched. If so, was a search reasonable under the circumstances? *See O'Connor v. Ortega*, 480 U.S. 709, 719 (1987). Public employees generally have a reasonable expectation of privacy as to their own desks and other facilities not shared with others. The scope of a search must be "reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the misconduct." *Id.* at 717.

Private employers may have latitude in searches because there is no constitutional right to be free from "unreasonable searches and seizures" by private employers. Nevertheless, depending on the circumstances, there still may be a claim for common law invasion of privacy. The employer will bear the burden of articulating legitimate business reasons sufficient to justify the invasion of an employee's privacy.

2. Searches of Lockers and Desks

a. *Narotzky, et al. v. Natrona County Memorial Hospital Board of Trustees, et al.*, 610 F.3d 558 (10th Cir. 2010). Here a group of doctors of a public employer claimed constructive discharge based on a warrantless search of their lockers. Summary judgment for defendants was affirmed. The doctors had held staff privileges at defendants' medical center under a staffing agreement. After expiration of the agreement, many medical instruments were missing and surveillance tape showed medical group staff leaving with various equipment, bags, and boxes. Lockers for the group were searched, although no missing equipment was found. In denying plaintiffs' Fourth Amendment claim, the Court found the

search reasonable in its inception and scope. The medical center legitimately suspected its property might be in the group's lockers. Further, before the search, medical center staff attempted to contact the group through email and phone about the missing equipment, but received no response. Under the circumstances, the medical center acted reasonably in conducting the search.

b. *K-Mart Corp. v. Trotti*, 677 S.W.2d 632 (Tex. App. – Houston (1st District) 1984). In this still-applicable case, K-Mart was sued after searching an employee's locker. The employee had used her own lock and K-Mart had not required that she provide the combination. The court held the employee had a reasonable expectation of privacy which K-Mart violated and that $100,000 in punitive damages was not excessive. This result likely was based on the fact that K-Mart failed to have a clear policy telling its employees that company-provided lockers were subject to search at any time and that if private locks were used, either a key or combination must be given to an employee's supervisor. K-Mart had no such policy.

3. Searches of Phones

a. *Garcia v. City of Laredo, et al.*, 702 F.3d 788 (5th Cir. 2012). Garcia, a Laredo, Texas police dispatcher, claimed defendants accessed her cell phone contents without permission and in violation of the Stored Communications Act, 18 U.S.C. § 2701(a) (2006). The court found that stored text messages and pictures on the phone did not fit the definition of "electronic storage." The phone was accessed by internal affairs investigators and their investigation resulted in Garcia's termination.

b. *City of Ontario, California v. Quon*, 560 U.S. 746 (2010). Here, the City's routine search of an employee's pager yielded text messages with sexual content. The

Supreme Court found that City-provided equipment could be searched if there was a "legitimate work-related purpose." The Court also noted that even though the employee had some expectation of privacy, the police department's review was justified. The department had told the employee and co-workers they should not expect privacy when using their pagers and they also were told that personal use would be tolerated to a certain degree. Plaintiff was told if he exceeded the monthly allotment of texts, he would have to pay the difference. The employee exceeded the limit and when his supervisors reviewed his texts, they found that the vast majority of them were personal.

4. Searches of Vehicles

a. *Bastible, et al. v. Weyerhaeuser Company, et al*, 437 F.3d 999 (10th Cir. 2006). Plaintiffs were terminated after a search found firearms in their vehicles in employee parking lots in violation of defendants' policies. The policies prohibited possession of firearms by employees, including in defendants-provided parking lots used by employees. Employees with weapons in their vehicles were terminated. The Tenth Circuit denied plaintiffs' claim of infringement of constitutional rights and affirmed summary judgment for defendants. This type of claim in 2016 could have a different result since Oklahoma now has a law prohibiting employer policies from barring employees keeping guns locked in their vehicles in employer parking lots. An ensuing claim for injunctive relief brought by employers who forbade their employees from bringing firearms onto company property was initially successful; however, the Tenth Circuit found the action was preempted by the Occupational Health and Safety Act and the district court's injunction was reversed. *See Ramsey Winch, Inc., et al. v. Henry*, 555 F. 3d 1199

(2009). Oklahoma law was again amended in November 2015 so that employees now may store ammunition in their locked vehicles parked at work.

b. *Related Firearms Issues.* Texas prohibits employers from barring employees with a license to carry a concealed handgun from transporting or storing a firearm in a locked, privately-owned motor vehicle in an employer-provided parking area. In New Mexico, employers can still prohibit firearms in the workplace. Under Sections 29-19-12 and 30-14-6 NMSA 1978, property owners may prohibit the carrying of firearms onto property they lawfully possess by posting or verbally notifying persons entering the property. Further, even though a loaded firearm may be carried or transported, either openly or concealed, in a vehicle without a permit, employers still may ban firearms from private property, specifically parking lots and other employer-owned areas. Some legal commentators suggested that the location of a parking lot in relation to the workplace may be a factor in determining if firearms can be prohibited in vehicles. If a parking lot is very close to a workplace and an employee can easily return to his or her car to retrieve a gun, then a ban on firearms in vehicles might be more defensible.

5. GPS Tracking

a. *United States v. Jones*, 132 S. Ct. 945 (2012). Here, the Supreme Court considered Global Positioning System ("GPS") tracking on a vehicle and whether this constituted a search under the Fourth Amendment. Jones was suspected of drug trafficking and police investigators received a warrant to attach a GPS device under his car. The Court unanimously found that this was a search under the Fourth Amendment and that Jones' Fourth Amendment rights had been violated. The Court rejected the government's argument there was no reasonable expectation of privacy in one's movement on public streets and emphasized that

the Fourth Amendment provided some protection for trespass onto personal property. Although not an employment case, courts may apply the case's analysis and find that an employer's location monitoring of an employee amounts to an invasion of that employee's privacy interests. Employers are especially cautioned about requiring attachment of a GPS to employee-owned vehicles.

b. *Brookshire v. Buncombe County*, No. 1-10-cv-278 (U.S.D.C. W.D.N.C. January 18, 2012). This decision was issued less than a week prior to *Jones* and involved a public employee discharged for falsifying timesheets and improper use of a county vehicle. The district court found the former employee failed to show a Fourth Amendment unreasonable search violation from the use of GPS tracking on his county-owned vehicle. The GPS data did not match employee's timesheets. Significantly, the employee also had signed an agreement acknowledging that he had no expectation of privacy in items stored in the truck and that the vehicle could be searched at any time without notice. The decision, however, turned primarily on the prevailing view of the federal courts that there could be no reasonable expectation of privacy of a person traveling in a vehicle on a public highway. This case points out that, for private employers, if GPS is used on company-owned vehicles, the employees should be required to sign an agreement acknowledging that they have no expectation of privacy in the vehicle or items located inside the vehicle and that the employer has the right to access the vehicle without notice, including engaging in GPS monitoring.

c. *Elgin v. Coca-Cola Bottling Co.*, 2005-WL-3050633 (E.D. Mo. November 14, 2005). Here, the private employer attached a GPS device to a company-owned vehicle used by the employee to service vending machines. This was done after a cash shortage

was reported on several machines. The court rejected the plaintiff's claim, noting that the employer owned the vehicle and the only information revealed by the alleged "intrusion" was the whereabouts of the company vehicle.

C. MONITORING OF EMPLOYEE COMMUNICATIONS

1. Overview

Policies on the use of company-provided communications devices are common and usually allow reasonable, limited personal use noting that employees have no reasonable expectation of privacy in such use. If regular monitoring of the use of these systems is done, employees should be notified in advance through a written policy. Such policies also should describe prohibited activities such as downloading of pornography, violating copyright laws, engaging in cyber harassment, and the like.

2. NLRB Developments

The NLRB has been increasingly aggressive on employer monitoring of employees' communications, just as it has with recording and surveillance issues. *See* discussion in Section A above. In a December 11, 2014 NLRB decision in *Purple Communications, Inc.*, 361 NLRB No. 126 (December 11, 2014), the NLRB significantly expanded the right of employees to use their employer's email systems for union organizing and other activities protected by Section 7 of the NLRA. Under this decision, employees who are given access to their employer's email system for business purposes can use that system on non-working time to engage in a wide range of protected communications, including union support and comments critical of the employer's employment-related policies, practices, and management decisions. This decision also may apply to other employer-owned devices such as smart phones.

Purple Communications reversed a 2007 decision in *Register Guard* where the NLRB held that an employer may completely prohibit employees from using its email system for non-business purposes, including union organizing, discussion of terms and conditions of employment, and other activities protected by Section 7 of the NLRA, as long as the ban was not applied in a discriminatory manner. *Register Guard* held the fact that employees were allowed to use an employer's email for business purposes did not provide a legal basis for allowing expanded use of the system for non-business purposes.

The new standard set out in *Purple Communications* presumes that employees who have rightful access to their employer's email system through their work have a right to use email for union organizing, discussions about terms and conditions of employment, and other statutorily-protected communications on non-working time. To rebut this presumption, an employer must demonstrate that special circumstances necessary to maintain production or discipline justify restricting these employee rights. Under *Purple Communications*, employers must permit employees to use employer's computers and email systems to engage in union organizing activity and similar protected activities.

3. Social Media

Social media policies also now are common among employers. Employers have legitimate concerns about protecting proprietary information, preventing harassment, and protecting clients or customers. If a social media policy is enacted, however, an employer must consider the limits of *Purple Communications*. While a policy which prohibits denigration of clients, customers, co-workers, or the dissemination of protected information will likely be defensible, employers should take care as to how they attempt to limit criticism of the company.

For example, pre-*Purple Communications*, a California Pizza Kitchen employee was fired for criticizing the new uniforms on the company's Twitter page. It is not clear whether, under *Purple Communications*, such comments might not be found to be within the protected scope of criticism of an employer's employment-related policies, practices, and management decisions.

D. OFF-DUTY BEHAVIOR

1. Overview

An employer seeking to control its employee's off-duty behavior can implicate both state and federal anti-discrimination laws, along with other state laws. Unlike some states, New Mexico does not have laws which prohibit "lifestyle discrimination." Nevertheless, employers should be reluctant to seek to control off-duty conduct which has no bearing on the employee's ability to perform the essential functions of the job.

2. Smoking

New Mexico is one of several states in which it is unlawful to refuse to hire or to discharge, or otherwise disadvantage any individual, with respect to terms of employment, because the individual is a smoker or non-smoker. *See* NMSA § 50-11-1 et seq. This law is even referred to as the "Employee Privacy Act." The statute does not excuse compliance with applicable state laws, local ordinances or employer policies regulating smoking on the premises of the employer during working hours.

3. Medical Marijuana

Even though medical marijuana may be lawfully used outside the workplace, if any employee reports to work and tests positive for marijuana, he or she may still be terminated for violating an employer's drug policies.

4. NLRA Protections

The National Labor Relations Act ("NLRA") makes it illegal for an employer to monitor or conduct any surveillance of employee union activities, including off-the-job meetings or gatherings. Any employer who sends anyone to eavesdrop on such meetings would be in violation of the NLRA.

5. Political Activities

Some states such as California prohibit employers from preventing employees from engaging or participating in politics, including running for elected office. In Texas, an employer cannot reduce or threaten to reduce an employee's wages or other employee benefits for voting for or against a particular candidate or for refusing to disclose how he or she voted. New Mexico has no such statutes; however, employers should be cautious as to what details they seek about such activities. Generally, there is no legitimate business reason for employers asking about their employees' off-duty political activity. Further, where employers have employees covered by collective bargaining, union contracts may specifically prohibit an employer from taking actions against an employee based on his or her political activities.

6. Social Media

As discussed above in Section C, while employers can enact social media policies, they must be careful not to interfere with concerted activities protected under the NLRA. Further, under state law, an employer is prohibited from asking an applicant for passwords in order to access that individual's account or profile on a social networking web site or to demand access in any manner to an applicant's account or profile. *See* NMSA 50-4-34 et seq.