EMPLOYEE MONITORING AND WORKPLACE PRIVACY LAW

AMERICAN BAR ASSOCIATION
Section of Labor and Employment Law
National Symposium on Technology in Labor & Employment Law
April 6, 7, and 8, 2016
Washington, D.C.

V. John Ella, J.D., CIPP

JACKSON LEWIS P.C.

I. INTRODUCTION

Privacy issues for employers and employees have multiplied as computer technology creates many more ways to store, access, and share information than anyone could have imagined back in the days of paper records. Concerns about privacy rights and technology have led to the enactment of more state and federal laws and regulations governing privacy. Employers must therefore comply with privacy rights and expectations of their employees and develop appropriate policies and procedures.

Monitoring employees lies at the heart of these legal and privacy issues. Employee monitoring is attracting more interest as companies seek to gather and use data to increase efficiency. According to some, "Big Data" is the buzzword of the decade. As popularized in the book and movie Moneyball, big data can be mined to make companies and workplaces more efficient and more profitable. One product, called Humanyze™ asks employees to wear sociometric badges that use a combination of microphones, infrared sensors, accelerometers and Bluetooth to measure worker movements, face to face encounters, speech patterns, vocal intonations and posture to create data about how workers interact.

Privacy litigation in response to employee monitoring has not yet become a tsunami. Some speculate that Millennial workers are more likely to accept monitoring as part of their job whereas older generations are more sensitive about perceived privacy intrusions. Anecdotes suggest that lawsuits in this area may be on the rise, however. In 2015, a plaintiff in California sued her former employer after she refused to use an app, called "Xora", on her smart phone which would allow her boss to track her whereabouts 24 hours a day, 7 days a week and she was subsequently fired. *Arias v. Intermex Wire Transfer, LLC*, No. S-1500-CV-284763 SPC, Cal. Super. Ct. Bakersfield, Co., May 5, 2015. Employees at the Daily Telegraph in London, England protested when motion sensors, as part of a product called OccupEye, were installed at their desks, presumably to help with energy efficiency. The product is advertised as allowing bosses to see who is at their desk at any given time to help fit more staff into smaller spaces. The newspaper removed the devices after the outcry.

II. MONITORING OF EMPLOYEES

A. Reasons for Monitoring

As indicated above, a common for employee monitoring is to increase productivity and dissuade cyber-slacking and social "notworking." Monitoring is also important, and necessary, to protect trade secrets and confidential business information and to detect and dissuade improper behavior such as sexual harassment, fraud, theft, embezzlement, identity theft, and data breaches. Employee misuse of company-provided computers, smartphones, tablets, networks, or other digital devices to view, share, or transmit inappropriate messages, images, or other types of communications puts the employer at risk of liability in all of these areas. Inappropriate forms of communication by email and text messages, for instance, can expose the company to charges of sexual harassment, defamation, or hostile work environment. In addition, file-sharing technology can cause a range of problems by making sensitive corporate financial information, trade secrets, and other corporate information, as well as personal employee or customer information, readily

available to anyone on the network. Companies must also monitor the monitors to make sure that supervisors are not snooping on employees, and employees are not improperly accessing medical records or other confidential information. Thus, there are many legitimate business reasons for regulating and monitoring employee use of, and access to, digital information and communications.

In certain instances, employers may even be required to monitor employee communications on their IT systems when involved in ongoing litigation, government audits, and compliance investigations. Laws such as the USA PATRIOT Act may require monitoring and disclosing employee information and communications to law enforcement agencies, and may create a duty to report suspicious activity. Monitoring obligations also may arise from other laws and regulations, such as guidance from the Federal Trade Commission for endorsers, including employees who use social networking websites to connect with potential customers, and guidance from the Financial Industry Regulatory Authority on broker-dealer communications with the public via email, instant messaging, and social media websites. Further, some states, including Arkansas, Illinois, Michigan, Missouri, North Carolina, Oklahoma, South Carolina, and South Dakota, have mandatory reporting statutes that require information technology workers to report child pornography found on computers they are servicing. Ark. Code § 5-27-604; Cal. Penal Code 11165.7; 720 Ill. Comp. Stat. 5/11-20.2; Mich. Comp. Laws § 750.145c(9); Mo. Rev. Stat. § 568.110; N.C. Gen. Stat. § 66-67.4; Okla. Stat. Tit. 21 § 1021.4; Ore. Rev. Stat. § 163.693; S.C. Code § 16-3-850; S.D. Codified Laws §§ 22-24A-16, 22-24A-17, 22-24A-18; Tex. Bus. & Com. Code § 109.001-.003. In cases of child pornography or certain other illegal electronic conduct, employers must take particular care to preserve the evidence for legal authorities and to not destroy any equipment, emails, or files that may contain such evidence.

Proponents of monitoring argue that employers must take a proactive approach to ensure the work environment is free from hostile and harassing activity. If employees know that they are being monitored, then they might be more inclined to maintain efficient work habits, thereby increasing productivity. Monitoring also may minimize the risk of inadvertent or intentional data breach by documenting who has access, when, and for what purpose.

Employee morale is an important consideration when considering how and whether to monitor. Opponents of monitoring argue that a loss of trust and respect for employees may lead to higher turnover, loss of productivity and initiative, and the decay of a positive work culture. In addition, monitoring can be costly, and misuse of data collected during monitoring may result in liability for the company.

Regardless of which side one takes, the debate may be complicated by the requirements of the federal rules on preservation and production of electronic documents and data during litigation. An employer's obligation to collect, preserve, and produce electronic data e-discovery may also encompass monitoring to the extent that employees' electronic communications inside and outside the workplace are implicated

B. Methods of Monitoring Employee Use of Company I.T. Systems

Employers and in-house counsel face an increasingly difficult challenge in balancing (i) the enormous business potential of evolving digital technologies and the need for and enhanced ability to monitor employees' electronic activities with (ii) new and sometimes conflicting legal and ethical responsibilities to employees. Although monitoring may lower employee morale and increase distrust of management, technological advancements have provided employers with new tools to aid lawful surveillance of employees' use of company IT systems and equipment. Paradoxically, the more powerful these tools become, the more risks they create for invasion of privacy claims.

Methods of electronic monitoring range from occasional email audits to sophisticated software enabling employers to count keystrokes, record time and activities online, view computer screens in real time, and to record use of company networks. Software also can restrict access to certain internet sites and track social media activity. Most of this software can be installed without alerting users.

Employers have many choices among electronic monitoring software products and range of services. For example, a product may allow an employer to simultaneously:

- Monitor an unlimited number of networked computers;
- Track the amount of computer idle time for each worker;
- Record every keystroke made;
- Create a log of every internet site visited;
- Monitor all incoming and outgoing email;
- Highlight and "flag" designated key words and content; and
- Provide a real-time view of all activity occurring on each computer.

An email application program may record the following, whether business-related or not:

- The email sender and recipient;
- Number of words in the email;
- Amount of time the employee spent reading the email;
- Amount of time the employee spent composing the email; and
- Number of attachments and the content of the e -mail.

Other monitoring tools track the amount of time employees are not using their computers and screen computer use for select words, phrases, or images. Monitoring can be done in-house or outsourced to one of many firms that specialize in electronic monitoring and surveillance.

The activities of employees who work outside of employer facilities can be monitored by global positioning systems ("GPS") and other technologies that extend beyond communications. GPS, for example, not only monitors location, but through time and date stamps, can provide employers with vast amounts of information that could help employers allocate resources and track productivity. At the same time, such monitoring could become evidence of wage and hour violations and other employer compliance shortfalls.

Some of the basic considerations for in-house counsel when evaluating, implementing, or upgrading an employee monitoring system for workplace information include:

- Educating executive management on employee monitoring issues, including the organization's specific reasons for monitoring, the legal and practical issues, the relative benefits and estimated costs of different approaches (e.g., centralized vs. decentralized), and the need for periodic review and assessment in light of technological and legal advances;

- Forming a task force or working group to coordinate the development of a monitoring strategy, including policy development, communication standards, employee orientation and training programs, procedures related to monitoring and detection, disciplinary notification and action, and on-going quality reviews and audits;

- Reviewing the options and identifying the technologies to be acquired and implemented, such as might be needed to address a "Bring Your Own Device" ("BYOD") workplace;

- Coordinating the monitoring system with other corporate functions, such as information security, information management, legal, and human resources;

- Reviewing for compliance with constantly changing state and federal legal restrictions in this area;

- Overseeing the implementation process and conducting periodic quality and compliance audits.

Ultimately, the decision of whether or not to monitor employees' electronic communications is largely dependent upon the federal and state privacy laws discussed in the previous section.

C. Notification Requirements

Connecticut and Delaware require employers to give notice to employees prior to monitoring their e-mail communications or Internet access. Connecticut Gen. Stat.§ 31-48d, Del.

Code § 19-7-705. Colorado and Tennessee require public entities to adopt a policy related to monitoring of public employees' e-mail. Colo. Rev. Stat. § 24-72-204.5, Tenn. Code § 10-7-512.

D. Emails and Internet Use

1. Work Email. It is well established that whatever an employee sends or receives on a company email account is the property of the employer and can be accessed or viewed by the company without notice. *See, e.g., McLauren v. Microsoft Corp.*, 1999 Tex. App. LEXIS 4103 (Tex. App. May 28, 1999) (no reasonable expectation of privacy for password protected personal folders on company network accessed through company computer); *TBG Insurance Services Corp. v. Superior Ct.*, 96 Cal. App. 4th 443 (Cal. Ct. App. 2002) (no reasonable expectation of privacy in an employer-owned computer located at employee's home); *Garrity v. John Hancock Mutual Life Insurance Co*., 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002) (no reasonable expectation of privacy in e-mails transmitted on employer's computer system; employer's interest in preventing sexual harassment is greater than employee's privacy interest); *Thygeson v. U.S. Bancorp*., 2004 U.S. Dist. LEXIS 18863 (D. Or. Sept. 15, 2004) (no reasonable expectation of privacy in personal folders on company network and accessed Internet sites). *See also, In re Reserve Fund Securities and Derivative Litigation*, 275 F.R.D. 154 (S.D.N.Y. 2011), citing *In re Asia Global Crossing, Ltd.*, 322 B.R. 247-258-59 (Bankr. S.D.N.Y. 2005) (discussing motion to compel discovery of personal emails from corporate server.)

2. Personal or Cloud-Based Email. Few employees have an expectation of privacy on employer emails. Many employees are discovering, however, that messages sent on private accounts can also be accessed under certain circumstances if they use a company-issued computer, smart phone or tablet. Former General and CIA Director David Patraeus even had his Gmail account accessed by the FBI. And as more employees perform more of their work on a computer, tablet or smart-phone, employers are increasingly tempted to monitor e-mail communications, to record employee activity through a technique known as "key-logging," or to use software to save and access "cached" files on a company's hard drive. These new techniques are continuing to drive litigation in this area. A few cases are of particular note:

In *Rene v. G.F. Fishers, Inc.*, 817 F. Supp.2d 1090 (S.D. Ind. 2011), the employer installed key-logger software on a company store computer. The key-logger software recorded all keystrokes made on the store's computer keyboard. It then periodically emailed the information to company managers who used the information to determine the plaintiff's password to her personal email account and personal checking account and to access them. After the plaintiff discovered that defendants were accessing her personal accounts, she confronted them and her employment was terminated. The court held that plaintiff's claims under the Stored Communications Act ("SCA") and the Indiana Wiretap Act survived defendants' motion to dismiss.

In *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N. J. S. 2010), the plaintiff-employee used a company-issued computer to send and receive emails through her personal, password-protected web-based email account. Some of her emails were with her personal

attorney. In this case, the employer had browser software that automatically saved a copy of each web page she viewed on the computer's hard drive in a "cache" folder of temporary internet files. After she quit and filed a discrimination lawsuit, the company created a forensic image of her computer, including her temporary internet files, and was able to retrieve the messages to and from her attorney. The New Jersey Supreme Court in *Stengart* held that the former employee had a reasonable expectation of privacy in her communications with her attorney through a web-based account and that her emails were privileged.

In *Pure Power Boot Camp Inc. v. Warrior Fitness Boot Camp LLC*, 759 F. Supp. 2d 417 (S.D.N.Y. 2010), plaintiffs operated a physical fitness center designed to replicate a military boot camp. Defendants, former employees, left to set up their own similar business and Plaintiffs sued for breach of fiduciary duty and other wrongful competition claims. Plaintiffs moved for injunctive release citing emails from defendants Hotmail, Gmail and Warrior Fitness Boot Camp accounts, and other personal on-line accounts, which they were able to access from computers on which the username and password fields were automatically populated. Defendants asserted a counter-claim under the SCA and prevailed. The district court awarded statutory damages of $1,000 for each violation, or a total of $4,000, denied a claim for actual damages, and reserved the issue of attorney's fees and punitive damages.

In *Fischer v. Mt. Olive Lutheran Church*, 207 F. Supp. 2d 914 (W.D. Wis. 2002), co-workers overheard a children's pastor discussing lewd acts over the church telephone. The head pastor hired a technology expert to examine the church's computer and access a personal email account. The head pastor also personally continued to access the personal email account. Based on his conduct, the children's pastor was terminated from the church. In suing the church, the former pastor sought damages for violation of his privacy. The court did not resolve the issue of whether there is a reasonable expectation of privacy in a web-based email account accessed through an employer's computer. Instead, the court found issues of material fact as to whether: (1) accessing the employee's personal account would be highly offensive to a reasonable person; and (2) an employee's email account is a place a reasonable person would consider private.

In another case involving web-based e-mail accounts, *Thygeson v. U.S. Bancorp*, 2004 U.S. Dist. LEXIS 18863 (D. Or. Sept. 15, 2004), the court held an employee had no reasonable expectation of privacy in the Internet websites he accessed while using his work computer. In that case, the plaintiff was a former employee who was fired for excessive Internet use and storing sexually inappropriate e-mails, from his web-based account, on the company network. The plaintiff sued, claiming the company invaded his privacy by monitoring the Internet sites he visited. In rejecting the plaintiff's claim, the court distinguished the facts in the *Fischer* case on three grounds: 1) the church accessed the content of e-mails on the plaintiff's personal email account by guessing at his password, but in the second case, the company accessed the record of the addresses of the web pages the employee had visited; 2) the church accessed the personal email account, which had information stored on the ISP's server; the company only gathered information available on its own network; 3) it was not clear whether the church had a policy regarding personal computer use and monitoring, but the company did have such a policy.

Neither *Fischer* nor *Thygeson* addressed the issue of whether there is a reasonable expectation of privacy in content contained on third-party servers accessed through an

employer's computers. Arguably, an employer will be less likely to be found to have invaded an employee's privacy if the employer: (1) monitors only its own internal networks; (2) does not monitor website content; (3) has an electronic communications policy in place which provides the employer may access e-mails at any time, and there is no expectation of privacy in such communications; and (4) requires employee acknowledgment of the policy.

(i) The Electronic Communications Privacy Act. The Electronic Communications Privacy Act ("ECPA") of 1988, amending the Federal Wiretap Act of 1968, regulates the monitoring of electronic communications, including e-mail. The ECPA imposes criminal and civil penalties against any person who intentionally intercepts an electronic communication. See Electronic Communications Privacy Act of 1986, Pub. L. No. 99 508,100 Stat. 1848 (codified as amended in various sections of 18 U.S.C.). Generally, employer monitoring of employee e-mails and website access will not be improper under the ECPA for at least two reasons:

- Employer monitoring of e-mail and website access likely does not meet the ECPA's definition of "intercept."

  and

- The ECPA contains an "ordinary course of business" exception that gives an employer the right to access an employee's e-mail if the messages are maintained on a system provided by the employer. However, the employer's interception must be in the ordinary course of business or more precisely, a "necessary incident to the rendition of the service or protection of the rights of [the provider's property] . . ." 18 U.S.C. § 2511(2)(a)(1) (2006).

(ii) The Stored Communications Act. While the ECPA amendments to the Wiretap Act prohibit an interception of an electronic communication, the Stored Communications Act ("SCA") prohibits such intrusions on stored communications. Like the ECPA, the SCA has a "provider" exception for employers who provide electronic communication service. However, the SCA's exception is broader because it does not require the employer access the information in the ordinary course of business. Under the SCA, an employer may access stored e-mails on services it provides. Although the SCA affords broad protection to employers monitoring their own e-mail systems, the SCA does not provide similar protection for systems hosted by third-parties, e.g., web-based e-mail accounts stored on third-party servers. As such, an employer will be unable to establish a provider exception. See *Rene*, 817 F.Supp.2d at 1096-1097 and *Fischer*, 207 F. Supp. 2d at 925-26 (holding a triable issue of fact existed as to whether the defendant church violated the SCA by accessing an employee's Hotmail account). For this reason, employers should be wary of accessing information not contained on their internal networks, without the user's authorization.

3. Social Media

(i) State Legislation. A number of states have enacted laws prohibiting employers from requiring current or prospective employees to disclose a user name or password

for a personal social media account (like Facebook). California, Illinois, Maryland, Michigan, Nevada, New Mexico, New Jersey, Utah, Washington, and Wisconsin have passed such laws. Ark. Code § 11-2-124; Cal. Lab. Code § 980; Colo. Rev. Stat. § 8-2-127; 820 Ill. Comp. Stat. 55/10; Md. Lab. & Empl. Code § 3-712; Mich. Comp. Laws § 37.273; Nev. Rev. Stat. § 613.135; N.J. Stat. § 34:6B-6; N.M. Stat. Ann. § 50-4-34; Or. Rev. Stat. § 659A.330; Utah Code Ann. § 34-48-201; Wash. Rev. Code § 49.44.200; Wis. Stat. § 995.55. Delaware's applies only to students at colleges and universities.

(ii) Discipline for On-Line Behavior. Employee terminations based on the content of an employee's Facebook post or blog have become an everyday occurrence. Bloggers have even coined a term for being fired as a result of a blog post: "dooced." Other examples of employees who have been fired for the content of their blog posts include: a congressional aide who fired for blog posts about her promiscuous sexual activities with older men; an employee of a search engine site fired for discussing the company's finances on a blog; an employee of a coffee company fired after making various blog posts about the company, its customers, and management; an employee of a newspaper fired after posting complaints about the workplace. Not surprisingly, and as discussed above, some employees who are fired for such conduct are suing their employers. Other employees and job applicants are hiring companies to scrub clean their presence on Google and the Internet to erase embarrassing information. Before taking adverse employment action, based on employee conduct relating to electronic communications, employers should consider whether there are legal constraints preventing or limiting such action.

(iii) National Labor Relations Act. Employees who post on Facebook, send emails, or blog about their working conditions or employer may be protected under Section 7 of the National Labor Relations Act ("NLRA"). 29 U.S.C. §§ 151-169 (2006). The NLRA affords employees (even those who are not unionized) the right to engage in "concerted activity." This includes the right to discuss the terms and conditions of their employment (and even to criticize their employers) with co-workers and outsiders. The National Labor Relations Board ("NLRB") over the past couple years has taken an aggressive and expansive stance in this area and is scrutinizing any complaints about discipline or discharge based on comments about the workplace. The NRLB is also cracking down on policies that purport to limit an employee's ability to discuss working conditions. This is a developing area and it remains to be seen if there is push back by the Courts, and a full discussion is outside the scope of this presentation. Before disciplining an employee for online activity, however, an employer must determine if the employee was potentially engaged in a protected concerted activity.

E. GPS and RFID. Some employers have experimented with Global Positioning Systems (GPS) trackers in company vehicles, or even smart phones, to monitor their employees, leading to some complaints about the intrusion into employee privacy. Radio Frequency Identification Devices (RFID) are a similar technology. Some states, including Missouri, North Dakota and Wisconsin, have passed laws prohibiting employers from requiring that an employee have a microchip containing an RFID device planted in the employee's body. Mo. Rev. Stat. § 285-035-1; N.D. Cent. Code § 12.1-15-06; Wis. Stat. § 146.25.

F. Video Surveillance. Surveillance cameras are sometimes used by employers to conduct internal investigations or monitor employee behavior. In general, with

regard to surveillance cameras, an employee's reasonable expectation of privacy may extend to areas exclusively reserved for employee use like bathrooms or locker-rooms. Reported cases also distinguish between video camera surveillance of employees using visible cameras and surreptitious video surveillance with secret cameras. The general rule is that an employer may photograph employees in plain view, at their workstations and during working hours, for time and motion studies, or as part of an investigative process. *See Smith v. Colorado Interstate Natural Gas Co.*, 777 F. Supp. 854 (D. Colo. 1991). *See also Munson v. Milwaukee Board of School Directors*, 969 F.2d 266 (7th Cir. 1992) (no invasion of privacy when the employer photographs or films an employee in a place open to the public where employee was observed from public streets to ascertain his residence). In 2015, the NLRB's Division of Advice determined that an employer's use of GPS tracking to monitor a unionized employee under investigation of misconduct did not constitute a material, substantial and significant change in the terms and conditions of employment and was not subject to mandatory bargaining.

Where the cameras are hidden, however, the employer generally needs to demonstrate a legitimate business reason for the surveillance and should position the cameras only in areas where the employees do not have a reasonable expectation of privacy. In New York and other states, possibly including Minnesota, the audio function should be turned off unless the employer has the employee's consent due to wiretap laws.

Whether an expectation of privacy is reasonable has been litigated in several cases. In one case, an employee who filed a claim for work-related damages was held to have waived an expectation of privacy and to expect that there might be an investigation by the employer, including secret filming. *See Jasmantas v. Subaru-Isuzu Automotive, Inc.*, 139 F.3d 1155 (7th Cir. 1998) (ADA plaintiff filmed by employer gardening in yard to refute claim of disability).

The Iowa Supreme Court, however, upheld a decision allowing an invasion of privacy claim by an employee against her employer for placing video cameras in the company bathroom, even though the evidence showed that the cameras were not functional. *Koeppel v. Speirs*, 808 N.W.2d 177 (Iowa 2011).

Questions about video surveillance frequently arise with regard to public or quasi-public employers under the Fourth Amendment of the Constitution. In *Thompson v. Johnson County Community College*, 930 F. Supp. 501 (D. Kan. 1996), security personnel sued the college on federal statutory, constitutional and state law grounds for monitoring the plaintiffs' locker area with silent video surveillance. The court granted the college summary judgment on all counts of the plaintiffs' claims. In Count I, the plaintiffs alleged the monitoring violated the Electronic Communications Privacy Act, by "conducting video surveillance in the workplace." The court found the ECPA does not prohibit the use of silent video surveillance as in this case. In reaching that conclusion, the court noted that recording a video image does not violate the ECPA. Rather, it is "the interception of an oral communication that subjects the interceptor to liability." In Count II, the plaintiffs claimed their Fourth Amendment rights were violated by defendants' "warrantless video surveillance searches of the security personnel locker area." The court first had to determine whether plaintiffs had a reasonable expectation of privacy: "To establish a reasonable expectation of privacy, plaintiffs must demonstrate that they had subjective expectation privacy in the security personnel locker area, and that this expectation was

objectively reasonable." The court found the plaintiffs did not have a reasonable expectation of privacy in the locker area because the locker room was not enclosed. "Plaintiffs' activities could be viewed by anyone walking into or through the storage room/security personnel locker area," said the court.

In *Vega Rodriguez v. Puerto Rico Tel. Co.*, 110 F.3d 174, 184 (1st Cir. 1997), the First Circuit Court of Appeals held that, because employees of a quasi-public telephone company lacked an "objectively reasonable expectation of privacy in the open areas of their workplace, the video surveillance conducted by their employer does not impact their federal constitutional rights." The court found the employees did not have a fundamental right to privacy under the Constitution to be free from video surveillance in the workplace and that the employees' substantive due process rights were not violated.

At least one state court has held, however, that with respect to hidden surveillance cameras, employees have an "actual, subjective expectation of privacy that society would recognize as objectively reasonable," in areas reserved exclusively for their use, such as break rooms. *Hawaii v. Bonnell*, 856 P.2d. 1265 (Haw. 1993). The court held "the defendants had an objectively reasonable privacy expectation that they would not be videotaped by government agents in the employee break room'." *Id.* at 1297 (quoting *U.S. v. Taketa*, 923 F.2d 665, 677 (9th Cir. 1991)).

A growing number of states are enacting legislation to prohibit or limit employee monitoring. Connecticut law prohibits an employer from using "any electronic device to record or monitor employee activities in areas designated for health or personal comfort or for safeguarding of employee possessions, such as restrooms, locker rooms, or lounges." Conn. Gen. Stat. Sec. 31-48b. California, West Virginia, Rhode Island and Michigan have similar laws prohibiting video cameras in bathrooms or locker rooms.

Video surveillance usually is conducted by someone other than the employer. If a third party interprets the data for the employer (i.e., edits the tape, draws conclusions, etc.) the third-party might be considered a consumer reporting agency triggering application of the FCRA (explained below). If the video surveillance company merely makes the tape and delivers it without interpretation, however, or merely installs and operates workplace surveillance equipment, then this should constitute an excluded communication based upon the transaction or experiences of the person making the observation. The videographer should not ask questions about the target or take any other action that would turn the observation into an investigative consumer report.

G. COMMON LAW

Most states recognize a common law tort for invasion of privacy. *E.g.*, *Lake v. Wal-Mart*, 582 N.W.2d 231 (Minn. 1998). In *Lake*, the Minnesota Supreme Court recognized three types of invasion of privacy: (1) intrusion upon seclusion, (2) appropriation of likeness; and (3) publication of private facts. Depending on the circumstances, therefore, it is possible for an employee to sue her employer for invasion of privacy. In Minnesota, however, such lawsuits have usually been unsuccessful for the plaintiff.

1. Intrusion upon Seclusion. The tort of invasion of privacy based intrusion upon seclusion requires (a) an intrusion; (b) that is highly offensive; and (c) made into a matter in which a person has a legitimate expectation of privacy. Generally, employees have less of a legitimate expectation of privacy in the workplace than at home or in other contexts. Questions arise, however, concerning electronic or video employee monitoring and testing of employees.

In *Groeneweg v. Interstate Enterprises*, No. A04-1290, 2005 Minn. App. LEXIS 405 (Minn. Ct. App. 2005), the Minnesota Court of Appeals held that a former employee did not have a cause of action under an intrusion upon seclusion theory where she alleged that having two co-workers present in the meeting in which she her employment was terminated was an invasion of her privacy.

Similarly, in *Murdock v. L.A. Fitness, Int'l*, No. 12-975, 2012 U.S. Dist. LEXIS 154478 (D. Minn. 2012), the court dismissed an invasion of privacy claim brought by a former employee. In *Murdock*, a manager posted a message on the employer's Facebook page stating:

> For those commenting and speculating about our group fitness/coordinator who isn't there anymore – first, shame on you for gossiping about a man's career, and the decisions of his supervisors on an open forum. Second, my understanding as one peripherally aware of the decision, it had nothing to do with his abilities as an instructor. That wasn't the extent of his job though, and some serious HR/Administrative issues arose surrounding his other responsibilities and parting was the decision. That is all that needs to be said.

Id.

In *Swarthout v. Mut. Serv. Life Ins. Co.*, 632 N.W.2d 741 (Minn. Ct. App. 2001), an intrusion upon seclusion claim survived a motion for summary judgment where the defendant insurance company altered a signed medical release to obtain private medical information.

2. Appropriation of Likeness. The appropriation of likeness version of invasion of privacy stands for the proposition that one who "appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of privacy." *Jalin Realty Capital Advisors, LLC v. A Better Wireless, NISP, LLC*, No. 11-165, 2013 U.S. Dist. LEXIS 2461 (D. Minn. Jan. 8, 2013) at *32, citing *Lake* at 235. Theoretically this could arise in the workplace context where an employer uses a photograph of an employee without permission for advertising or marketing purposes.

3. Publication of Private Facts. Publication of private facts occurs when there is information communicated to the public about facts that are not of a legitimate concern to the public and the publication is or would be highly offensive to a reasonable person. In Minnesota, the publication must be to the public or to so large a number of persons that the matter must be regarded as substantially certain to become public.

The Minnesota Supreme Court affirmed dismissal of a publication of private facts claim against an employer in *Bodah v. Lakeville Motor Express, Inc*., 663 N.W.2d 550 (Minn. 2003). *Bodah* began as a class action filed on behalf of over 200 truckers who claimed that their employer, Lakeville Motor Express, had wrongfully disseminated their Social Security numbers when it sent out a list of employee names and Social Security numbers to its terminal managers, as part of a records check. Approximately four months after the transmittal occurred, the employer notified the affected employees of the transmission and assured the employees that the terminal managers had been instructed to destroy or return the list immediately. The class filed a lawsuit alleging that the dissemination of Social Security numbers violated constituted a violation of the class members' right to privacy. Relying on the definition of publication provided by the Restatement (Second) of Torts, the Minnesota Supreme Court reasoned that the employees' privacy rights were not violated because the dissemination of private facts – the social security numbers – was not to the "public at large." The Court determined that if the dissemination of private information is limited to a "single" or "small group" of person, the act is not tortious in nature. While *Bodah* appears to limit employees' invasion of privacy claims to situations in which the transmission of information was widespread, or public in nature, this case should serve as a reminder that employers must take care with the storage and transmission of confidential employee information.

Similarly, in *Johnson v. Campbell Mithun*, 401 F. Supp. 2d 964 (D. Minn. 2005) a Minnesota federal district court rejected a claim by an employee who claimed that her employer violated her right to privacy when it informed approximately 12-15 individuals, both employees and clients, that she suffered from multiple sclerosis. The court determined that because the disclosure was not "accessible to the public at large," it did not qualify as public in nature for purposes of maintaining an invasion of privacy claim. While the *Johnson* court took an equally restrictive view of what qualifies as a "publication," employers should still consider the need to maintain the confidential nature of employees' medical records and curtail access to medical records.

III. POLICIES, HANDBOOKS, AND AGREEMENTS

There are several privacy-related policies or handbook provisions that every employer should consider implementing, separately or in combination, and which should be reviewed carefully. All of them should be examined for compliance with the NRLA. Several states including Massachusetts, Connecticut, California, Oregon and Texas have enacted an affirmative obligation to safeguard personal information used by a company in its business, including a requirement to establish a Written Information Security Program ("WISP").

The policies every business should consider include the following:

- Electronic Communication Policy
- Social Media Policy
- Bring Your Own Device (BYOD) Policy
- Sexual Harassment Policy
- Confidentiality and Non-Disclosure Policy.
- Written Information Security Program (WISP)

It is critical for employers to implement an effective electronic communications policy. While such a policy will not necessarily insulate an employer from all potential liability, it will reduce employees' expectations of privacy and provide the employer with more discretion to take action against employees who engage in electronic misconduct. In drafting such a policy, employers should consider at least the following provisions:

- Company equipment, including computers and electronic systems, is designed primarily for business use only.
- Employees should not have an expectation of privacy when it comes to the use of company e-mail.
- Employees must abide by non-disclosure agreements or confidentiality policies;
- If employees have personal blogs they must clearly communicate that any views in their blogs are their own and not those of the employer.
- Company policies governing the use of corporate logos and other brands also apply to electronic communications.
- Only individuals officially designated may "speak" (whether orally, electronically or in writing) on the company's behalf.
- Employees are prohibited from making discriminatory or defamatory comments when discussing the employer, the employee's superiors or co-workers, and/or competitors.
- Employees must comply with all other company policies with respect to their electronic communications including rules against conduct that may result in unlawful sexual harassment.
- Employees may not use or download unlicensed software.
- The company reserves the right to take disciplinary action against an employee if the employee's electronic communications violate company policy.

IV. CONCLUSION

Workplace privacy and employee monitoring is a more challenging area of the law than ever before. Employers and their attorneys need to develop sound policies and procedures to adapt and comply with evolving regulations, laws and technology.

4821-0501-3295, v. 1