The Impact of Emerging Technologies on Employee Privacy

The use of technology in both the workplace and at home has become omnipresent in modern society. Technology advances that include a vast array of electronic communications, computer-based document creation and storage, and other endless futuristic developments have allowed for greater efficiency and organization in one's everyday life. Predictably, such advances have also invaded the employment sector with both positive and negative consequences. In the modern workplace, employees are generally required to perform their job tasks utilizing employer-provided devices and electronic systems, such as smartphones, computers and e-mail, which can allow for a high level of productivity. However, it also invariably creates opportunities for employees to use employer resources for non-work related personal use. It is also now possible to track with GPS devices exactly where and when employees travel. Employers have clear business related interests in monitoring and reviewing employees' use of employer resources, which can include information gathered from private e-mail, chats or social media accounts that employees have accessed using company technology or devices.

The balance between an employer's right to access such material, whether for liability or security purposes, or to ensure productivity, and an employee's right to a reasonable expectation of privacy in their communications continues to remain unclear. While several courts have addressed this issue in different contexts, no generally applicable rule has been established.

Massachusetts Privacy Act

Massachusetts law, like the law of virtually every other state, protects an employee's reasonable expectation of privacy in the workplace. The Massachusetts Privacy Act provides that:

A person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages.[2]

When information sought by an employer is such that an employee has a reasonable expectation of privacy and (1) the information is unrelated to job performance, or (2) the means used to obtain the information are unduly intrusive or offensive, or (3) the information is shared with people who do not need to have it, the employer's interests [in obtaining the information] are correspondingly weakened or extinguished.[3] If the information requested by the employer is job-related, a reviewing court will balance the degree of intrusiveness against the nature of the job (e.g., how much the information needed is to protect health and safety of the employees).

It would be difficult, if not impossible, to foresee all the workplace situations in which an employee's privacy rights could be implicated. The following will address some of the situations in which privacy concerns are most frequently raised, along with some suggestions for striking the appropriate balance between the need for an efficient and well-managed workplace and respect for employees' privacy.

Employee "Sexting" Case — *City of Ontario, California v. Quon*[4]

When the U.S. Supreme Court agreed in 2009 to review a workplace "sexting" case from California, employment lawyers were hopeful that the Court would seize the opportunity to provide much needed guidance about balancing the monitoring of employees' workplace communications and their privacy rights. Unfortunately, the Supreme Court did not offer as much guidance as employment lawyers had hoped. The Court purposely wrote the decision narrowly, and limited it to the rights of public employees. However, the Court's analysis provides some instructive guidance for employers

struggling with employee technology use in both the public and private sectors.

In *Quon*, the City of Ontario issued pagers with text message capability to Quon and other police officers in the police department. Before acquiring the pagers, the City announced a technology use policy that specified that the City reserved the right to monitor and log all network activity and notified employees that they should have no expectation of privacy when using such resources. Quon signed a statement acknowledging that he had read and understood the policy. The City paid for both the pagers and the usage plan, but required officers that exceeded the usage plan limits to pay any applicable overage charges. After Officer Quon exceeded the plan several months in a row, the police chief conducted a review to determine if the usage plan needed to be expanded to meet the messaging needs of the officers. The review included transcripts of Quon's messages for a two-month period, *excluding off-duty hours*, to determine if the overage charges were the result of work-related messaging or personal use. The review revealed that the majority of Quon's messages were personal, including several that were sexually explicit, and he was disciplined as a result.

Quon sued the City, alleging a violation of his Fourth Amendment right against unreasonable search and seizure, as well as the federal Stored Communications Act and California state law. The District Court determined that Quon had a reasonable expectation to privacy in his messages, but found for the City based on the legitimate reason for the search (to determine if the existing character limit was imposing work-related costs upon the officers). The Ninth Circuit subsequently reversed, finding that the search was not reasonable in scope based upon the City's failure to use "less intrusive" means to meet the legitimate work-related purpose.

The Supreme Court reversed the Ninth Circuit and found in favor of the City. Specifically, the Court found that regardless of whether Quon's expectation of privacy was reasonable, the City did not violate the Fourth Amendment because the search was based upon a legitimate business purpose and was reasonable in scope. The Court focused on Quon's assumed awareness of the possibility of a search based upon the City's technology use policy, as well as the narrow scope of the City's review of the transcripts. Unfortunately, the Court intentionally reached its decision on narrow grounds and failed to issue any useful guidance to employers or employees with respect to the general regulation of workplace technology use. Justice Kennedy highlighted the limited applicability of the decision, stating that "a broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted."[5]

Furthermore, because the Court confined its analysis to the public-sector workplace and the related Fourth Amendment implications, the context in which the decision is applicable to private employers remains unclear. Though the Court noted that the City's search would be "regarded as reasonable in the private-employer context," no other specific guidance is offered to the private-sector employer.[6] However, the Court's opinion does set forth several broadly applicable principles that both the private and public sector employer should embrace. First, employers should implement a detailed technology use policy that encompasses all forms of employer-provided communication devices (discussed in further detail below). This policy should clearly state that employees have either limited or no expectation of privacy when utilizing employer issued devices or systems in the workplace. The policy should be clearly communicated to employees because it will establish the employees' reasonable expectation of privacy when utilizing such equipment. Second, any employer initiated search of employee communications must have a legitimate business purpose and should remain as limited as possible to work-related transactions (such as limiting review to messages sent during work hours as in *Quon*).

Key Points Left Unaddressed By *Quon*

Boundaries of Privacy Expectations and Electronic Communications

Despite being presented with the opportunity to do so, and with the assistance of the parties' briefs

and 10 amici curiae, the Supreme Court declined to decide whether Quon's asserted privacy expectations were reasonable. Moreover, the Court declined to set any governing principles to assist in analyzing the issue.

In rendering its decision, the Court assumed for argument's sake that Quon had a reasonable expectation of privacy. It next assumed that the government's review of the text transcripts was a search under the Fourth Amendment, and further assumed that the principles governing a search of a physical office applied to the electronic sphere. The Court then rested its decision on the legitimacy of the search, holding that the search was reasonable and motivated by a legitimate work-related purpose.

In explaining its reservations to set broad precedent, the Court explained that the case "touches issues of far reaching significance."[7] The Court mentioned the *Katz* case from 1967, where the Court relied upon its own personal experience in determining that a right of privacy existed in a closed, public phone booth. In contrast, the Court explained that it "is not so clear that courts at present are on so sure a ground."[8] The Court noted that rapid changes in the dynamics of communication and information transmission have caused similar rapid change in what society accepts as proper behavior.[9]

Impact of the Stored Communications Act

Because the Court intentionally limited its analysis in *Quon*, several questions and issues remain as to what and how an employer is allowed to monitor and review in the context of workplace communications. One such issue is the applicability of the federal Stored Communications Act (SCA), which creates criminal and civil liability for, amongst other things, whoever intentionally accesses, without authorization, a facility through which an electronic communication service is provided and obtains unauthorized access to a wire or electronic communication while it is in electronic storage in such a system.[10] Though Quon raised an SCA claim, the merits of that claim were not before the Court. Therefore, the SCA's applicability to those specific circumstances remains unclear.

The SCA was passed in 1986 as part of the Electronic Communications Privacy Act, in an attempt to address the plethora of privacy breaches caused by the widespread use of the internet, which the Fourth Amendment is unable to address adequately.[11] In addition to prohibiting unauthorized access to stored communications, the SCA also prohibits "providers" of communication services from disclosing private communications to specific persons and/or entities.[12] In order to determine if an electronic communication is "in storage" so as to implicate the SCA, one must establish whether it has been downloaded to a computer or remains on a service provider's network. The statute delineates between "remote computing services" (RCS), which provide computer storage or processing services to the public, and "electronic communication services" (ECS), which is any service that provides the ability to send or receive wire or electronic communications. An ECS is generally prohibited from knowingly disclosing the contents of a communication to any person or entity while that communication remains in electronic storage, whereas an RCS is allowed to divulge the contents of a communication carried or maintained on its service to the subscriber of the service.[13] Courts have determined that e-mail stored on an electronic communication service provider's systems after it has been delivered, as opposed to e-mail that is stored on a personal computer, constitutes a stored communication subject to the SCA. Therefore, an employer is allowed to access stored e-mails on the electronic server it provides, but it may not intrude on systems hosted by third parties. A third party system would include communications that are transmitted from an employee's personal web-based e-mail account accessed through the company system (i.e. Gmail, Yahoo, etc.).

In *Bohach v. City of Reno*, a case with striking similarities to the issues presented in *Quon*, the court found that the city was allowed to access the electronic messages that police officers sent to each other over the Department's computerized paging system, as the city was the "provider" of the electronic communications service under the SCA.[14] Two police officers of the Reno Police

Department filed suit against the city for violations of federal wiretapping statutes and their constitutional right to privacy, when the Department retrieved their pager messages in the course of an internal affairs investigation. When the pagers were distributed to the officers, a standing order was issued that alerted users that all messages were permanently logged on the system and that certain messages (i.e. discriminatory) were prohibited. Based on this warning, the court found that only a diminished expectation of privacy on behalf of the officers could be reasonable, which was further supported by the system's built-in capacity to maintain all messages in electronic storage. For Fourth Amendment purposes, the court found that such a system is part of the "ordinary course of business" for police departments that serves the legitimate business objective of maintaining necessary records. In terms of the SCA, the court found that because the city was the provider of the electronic communication service at issue, there was no SCA violation because service providers are allowed "to do as they wish when it comes to accessing communications in electronic storage."[15] Similarly, in *Fraser v. Nationwide Mutual Ins. Co.* the court found that e-mails stored on an employer operated and administered system are within the SCA exception for all searches by communications service providers.[16]

However, the court in *Pure Power Boot Camp v. Warrior Fitness Boot Camp* found that an employer's ability to correctly guess an employee's personal e-mail account information does not constitute authorized access under the SCA.[17] The Employee Handbook explicitly stated that employees had no right to personal privacy in any matter stored in, received, or sent through the employer's system, which included the use of personal e-mail accounts on company equipment. When the defendant employee left the employ of Pure Power Boot Camp to form a competitor company, his former employer used the log-in information allegedly stored on a company computer in order to access a variety of personal e-mail accounts that had not been accessed on any employer resources. The employer claimed that the employee accessed his Hotmail e-mail account while at work on numerous occasions, which is how his username and password became stored on the company computers. The employer conceded that she used the stored information in order to successfully "guess" the log-in information for the employee's other private accounts. The court found that such employer access to an employee's personal account information was not authorized by the SCA. In response to the employer's argument that the technology use policy diminished any reasonable expectation to privacy on behalf of the employee, the court noted that the e-mails at issue were located on and accessed from third-party communication service provider systems, which was not addressed by the policy nor accessible to the employer under the SCA. In short, the court found that the employee's carelessness in failing to remove his log-in information from the company computer did not equal consent to the contents of his private e-mail communications.

Nationally, courts have also recently started to apply the SCA to cases involving social networking sites, such as Facebook and MySpace. In *Pietrylo v. Hillstone Restaurant Group d/b/a/ Houston's*, the court found that employees' managers had violated the SCA by knowingly accessing a chat-group on a social networking website without authorization.[18] The managers had accessed an invitation-only chat group created by an employee by utilizing the log-in information of another invited employee. The employee later testified that she had only given her MySpace account password to her manager because she believed she was required to given his position of authority. Similarly, in *Crispin v. Audigier, Inc.* the court found that Facebook and MySpace messages that are not publicly available are protected information under the SCA and cannot be subpoenaed for use in civil litigation if the user takes the necessary steps to ensure the material remains private.[19] Therefore, the court noted, whether a particular message or "wall posting" is subject to disclosure will hinge upon that individual's privacy settings and the extent of access permitted to the public.

In contrast, however, the court in *Romano v. Steelcase Inc.* found that there is no reasonable expectation of privacy in information published on social networking websites.[20] The plaintiff claimed permanent injuries as the result of an accident allegedly caused by a defective chair, to the extent that she was no longer able to participate in or enjoy a wide range of activities. Contrary to these claims, however, the public portions of her Facebook and MySpace accounts revealed she had

an active lifestyle and had traveled to different parts of the country during the time period she was supposed to have been incapable of partaking in such activities. When the plaintiff refused to answer questions regarding the materials posted on her social networking accounts, the defendants sought a subpoena to obtain full access to her current and "historical" information on Facebook and MySpace. The court found that the information sought by the defendants was both material and necessary to the defense of the matter, in light of the fact that publicly posted pictures displayed the plaintiff participating in the active lifestyle she asserted the defendants had taken from her. Further, the court noted that both social networking sites' policies self-described as online communities where users can share life activities with a network of mutual friends, as well as warned that there is no complete guarantee to privacy. The court stated that the plaintiff could not have a reasonable expectation to privacy in her postings, given that she consented to the disclosure of her personal information with others by utilizing the sites, which by their very nature and purpose allow users to view the personal information of others.

Several other courts have recently followed the *Romano* court's line of reasoning, even in instances where the SCA is not raised as an obstacle to a claimant or defendant's social networking profile. In *Equal Employment Opportunity Commission v. Simply Storage Management, LLC et al.,* the court found that plaintiffs alleging severe emotional trauma and harassment against their employer must produce all information from their social networking profiles and postings that relate to their general emotional and mental states during the relevant period of the alleged injury.[21] The Equal Employment Opportunity Commission (EEOC) filed suit on behalf of two claimants that alleged the defendant businesses were liable for sexual harassment by a supervisor. The defendants sought access to the claimants' social networking profiles, in their entirety, on the grounds that the injuries alleged implicated all of their social communications, whereas the EEOC argued that production should be limited to content that directly addressed the issues raised in the complaint. The court noted that the discoverability of social communications in light of emotional and mental health claims required a defined set of appropriately broad limitations. In discussing such limits, the court specified that classifying one's social networking site as "private" or "locked" does not establish a legitimate basis to shield the related communications from discovery.

Ultimately, the court found that social networking content must be produced when it is relevant to a claim or a defense in the matter. However, the court clarified that such a relevancy standard cannot be used to assert that *all* the content of a claimant or defendant's social networking material is relevant to the case, but rather only those communications that are probative of a claim or defense in the litigation. Similarly, in response to a motion to compel, a Pennsylvania court recently found that there is no "social network site privilege" protecting a personal injury claimant's Facebook and MySpace accounts, and ordered disclosure in instances where there is an indication that such sites contain information relevant to the prosecution or defense of a lawsuit.[22]

Though the issue of authorized access under the SCA has yet to be fleshed out in-depth within the social networking context, it does appear that the SCA creates an exception for an unauthorized third party to view materials posted on a website such as Facebook or MySpace. Within the sphere of electronic communications, the SCA exempts from liability "conduct authorized … by a user of that service with respect to a communication of or intended for that user."[23] Based upon this exception, there is speculation that an employer can view an individual's online posting on a social networking website if one of that individual's "approved friends" either willingly allows the employer to utilize his or her access information or prints out the material for the employer to review. This interpretation of the SCA is bolstered by *Konop v. Hawaiian Airlines, Inc.*, in which the court discussed the exception under the SCA that allows intended recipients of electronic communications (i.e., an individual's approved social networking "friend") to authorize third parties to access those communications.[24]

In *Konop*, an employee created a website where he posted updates critical of his employer. The employee created a list of eligible individuals allowed to view the website, which required the equivalent of a user name and password to gain access to the contents of the website. The terms and

conditions of use prohibited eligible users from disclosing the contents of the website to any other individuals. The employer's vice-president asked two employees eligible to access the website for their permission to use their names and password to enter the site, which they granted. The court's decision hinged on the fact that neither employee had ever accessed the website, therefore neither qualified as actual "users" under the SCA's exception. Because of the employees' failure to qualify as "users", the court found that neither could legally authorize a third party to access the contents of the website.

Though the ultimate outcome of the case was unfavorable to the employer, the court's discussion of "authorized users" indicates that the employer would not have been liable if both employees had accessed the website even once, thus qualifying as users authorized to grant access to third parties. Furthermore, in stark contrast to the facts of *Pietrylo* (discussed above), it should be noted that the employees in *Konop* willingly authorized their employer to utilize their access information. While the available case law is limited, courts have already established that an employer that gains access to an electronic communication protected under the SCA through the use of coercive means will be found liable for unauthorized access.[25]

Sampling of State Specific Interpretations

Individual states have also begun to apply, and in essence create through case law, privacy laws within the context of an employee's right to privacy in communications within the workplace. Some states have also enacted legislation that requires employers to inform employees if they are monitoring workplace electronic communications.

In Massachusetts, the general privacy statute discussed above has been applied in the context of an employee's right to privacy with respect to e-mails sent over a company e-mail system. In *Garrity v. John Hancock Mutual Life Ins. Co.* the court found that the defendant's legitimate business interest in protecting its employees from harassment in the workplace outweighed the employees' privacy interests.[26] The employer alleged that the employees regularly received sexually explicit e-mails on their office computers, which they would subsequently send to fellow co-workers. The employer's technology use policy explicitly prohibited obscene messages and noted that the inappropriate use of e-mail would be subject to disciplinary action, up to and including termination of employment. The policy clearly noted that situations could arise that may necessitate a company review of e-mail messages and other documents, which the employer periodically reminded employees and warned them of several instances where employees were disciplined for policy violations. Because the employees admitted that they were aware of the policy, and the employer's noted ability to access the e-mail on the company system, the court found that there was no reasonable expectation to privacy in the content of the e-mails.

In New Jersey, one court has found that an employer has an affirmative duty to investigate employees' computer activities and to take prompt and effective action to stop unauthorized use.[27] The employee involved was sending pictures of his ten-year old step-daughter to internet pornographic websites from his work computer and over the employer's internet system. The company technology use policy stated that the employer reserved the right to review, audit, access and disclose all messages sent or received over the system and prohibited access to non-business nature websites. The policy noted that any employee that violated the terms and conditions would be subject to discipline, which could include discharge. The employer was aware of the employee's conduct for a period of time, as a result of computer monitoring and several co-workers' complaints, however the employee was not confronted or disciplined for his conduct. The young girl's mother sued the company for negligence and the employer raised "employee privacy" as a defense.

The court determined that the company was on notice, through personnel complaints and monitoring, that the employee was viewing child pornography on his computer and that such imputed knowledge created a duty to act on behalf of the employer. Because public policy favors the exposure of crime,

particularly child pornography, the court found that the company had a duty to report the employee's activities to law enforcement authorities and to take effective internal action, up to and including termination of employment. The court also discussed the implication of the employee utilizing the employer's resources to conduct such illegal activity and, quoting from the Restatement Second of Torts, stated that the employer had a duty to exercise control over the employee given the clear risk of harm to others. Employers that monitor e-mail and internet use should be aware that, according to this court, they may have an active duty to view and act upon any unauthorized or illegal activity discovered through their monitoring efforts.

In California, the court in *TBG Ins. Services Corp. v. The Superior Court* found that the "use of computers in the employment context carries with it social norms that effectively diminish the employee's reasonable expectation of privacy to his use of his employer's computers."[28] The employer had provided the plaintiff employee with two computers for business use; one to use at work and one for working from home. The employee signed the employer's technology use policy and agreed that his computers could be monitored by his employer, but was ultimately terminated for misuse of the office computer. Therefore, based upon the employer's clear ban on personal use and it's notification of monitoring, the court found that the employee had no reasonable expectation of privacy to the contents of the computer. Furthermore, the court held that prior notice that an employer will monitor technology use for compliance with the company policy, and consenting to such monitoring, further defeats a claim that the employee had a reasonable expectation to privacy. In arriving at its decision, the court looked to the "community norm" of the workplace environment within the 21st-century computer-dependent major businesses; more than three-quarters of which monitor, record and review employee communications on the job.

E-mail Privacy – Attorney-Client Communications

Several of these same states are currently struggling with yet another issue left unaddressed by the *Quon* decision – does an employee waive the attorney-client privilege when he or she sends an electronic message to a personal attorney over the employer's internet system and/or with a company issued e-mail address? The preservation of the attorney-client privilege within the context of one's workplace is an area of the law that is currently widely debated and ultimately remains unclear.

In *Stengart v. Loving Care Agency*, the New Jersey Supreme Court recently found that the attorney-client privilege is not waived when an employee sends an email to a personal attorney over the employer's internet system from a personal e-mail account.[29] The employer's technology use policy allowed for personal use of the employer's system and did not clarify that the content of e-mails sent via personal accounts could be forensically retrieved and read by the employer. The court noted that the employer's allowance for occasional personal use created doubt regarding whether those e-mails were company or private property. Because of the ambiguities created by the policy the court found that the employee had a reasonable expectation of privacy, which was reinforced by her use of a password protected personal e-mail account, to ensure her communications remained confidential.

Similarly, in *Nat'l Econ. Research Assocs., Inc. v. Evans*, a Massachusetts Superior Court judge held that the attorney-client privilege is not waived when an employee uses a private e-mail account on an employer-owned computer.[30] The employee had utilized a password protected personal e-mail account on a company issued laptop computer to send messages to his attorney. The employee had tried to delete all such communications from the laptop before returning it, but the messages were ultimately saved as screen shots on the employer's hard drive and were recovered with the assistance of a forensic expert. The judge specified that if an employer seeks to read an employee's attorney-client communications unintentionally stored on a company-owned computer, that were initiated via a private, password-protected e-mail account accessed through a separate internet server, the employer's policy must plainly communicate to the employee that:

"1) all such e-mails are stored on the hard disk of the company's computer in a 'screen shot' temporary file; and

2) the company expressly reserves the right to retrieve those temporary files and read them."[31]

However, the judge also noted that if an employee uses a company issued e-mail address to communicate with a personal attorney, the attorney-client privilege will likely be waived if the employer has implemented a technology use policy that clearly indicates that there is no personal use allowed and no reasonable right to privacy.

In comparison, a New York lower court held that an employee's communications with his attorney transmitted over the employer's e-mail system, via a company issued e-mail address, were not protected by the attorney-client privilege. *Scott v. Beth Israel Medical Center, Inc.****[32]*** The employee at issue, a physician working in a hospital, had sent several e-mails to his attorney from his company issued e-mail address via the company network prior to his termination. The court found that the employer's clear "no personal use" e-mail policy, that also allowed for employer monitoring of the system, diminished any reasonable expectation of employee privacy. Therefore, the court noted that such a clearly defined policy, in conjunction with the employee's knowledge of such terms and conditions, diminished any expectation of confidentiality.

Though this area of the law remains in flux, the courts that have dealt with the attorney-client privilege in this context appear to place a heavy emphasis on the terms and conditions of employer-provided technology as specified by the technology use policy. In instances where the policy has allowed for personal use the courts appear more likely to find that the attorney-client privilege has not been waived based upon the employee's reasonable expectation of privacy. As reflected by these courts, as well as the Court in *Quon*, the employer's clearly defined technology use policy is absolutely vital in all matters that pertain to an employee's right to privacy in communications.

The Ultimate Lesson Learned: A Clear and Detailed Technology Use Policy is Crucial Post-*Quon*

As noted, the *Quon* decision clearly indicates that employers should implement clear technology use policies that define the parameters in which employees may access and utilize employer-provided devices and systems. This principle is further reinforced by those state courts that have dealt with employee communication privacy issues in the workplace. The policy should clearly define the specific types of technology and media that is covered. However, given the ongoing and constant emergence of new technologies the policy should remain broad enough to apply to such advances without the need for constant revisions. A well-drafted policy will affirmatively state that an employee has no reasonable expectation to any documents created on or transmitted via an employer-owned system. Also, the policy should clarify if information that employees believe has been deleted is still accessible by the employer. Employers should ensure that the policy emphasizes that all such information will be disclosed should an investigation into that employee's activities or employment ensue. This should include a warning that such disclosure covers even those employees that may not be under investigation specifically, as their communications with the employee at issue can also be subject to review.

One of the issues that arose in *Quon* was the City's inconsistent enforcement of the technology use policy, which was merely emphasized by one supervisor's statement that an audit into the specific use of the pagers would be unnecessary if the officers paid for the overage charges. This inconsistent enforcement of the policy created the possibility that Quon had a reasonable expectation of privacy in his messages, despite the policy's clear warning that such privacy was non-existent. Therefore, in order to avoid unintentional changes to the policy, an employer should identify a senior official with the authority to alter the terms and conditions of the policy and clearly state that no other management staff has the capacity to modify it.

Employers should also consider annual updates to the policy, if necessary, and require that each employee sign or electronically acknowledge their understanding and acceptance of these terms. It might prove beneficial to circulate the policy via e-mail on an annual or semi-annual basis to minimize claims that employees were unaware of the policy's existence. Also, employers should conduct trainings for upper management to ensure that all staff remains in compliance with the specifications of the technology use policy.

OTHER PRIVACY CONSIDERATIONS

Global Positioning Systems

Global Positioning System (GPS) devices make it easy for employers to keep track of the location of company vehicles. A GPS device can record and display a vehicle's location and route to establish a history that an employer may access at any time. Using GPS to track trucks or company cars can help companies analyze route efficiency, help improve safety, and deter thefts. For all the pluses of GPS, there are drawbacks. Because GPS devices can also pinpoint where employees who use company vehicles are and where they have been, the technology has raised new worker privacy concerns that HR professionals need to recognize. Many cell phones now come equipped with GPS capabilities, further broadening an employer's ability to track employees.

Currently, there are no federal or state statutes expressly prohibiting the use of GPS devices in an employment situation. However, employees who resent being tracked or see it as unduly intrusive could use state privacy statutes and common law tort principles to sue for an end to tracking.

One of the first lawsuits involving an employee's challenge to the use of a GPS device was a Missouri case, *Elgin v. St. Louis Coca-Cola Bottling Co.**[33]*. During an investigation of theft, the bottling company installed GPS devices in a number of company vans that employees were permitted to drive during off-duty, as well as working, hours. One of the employees who had been cleared of wrongdoing sued the employer for, among other things, intrusion of seclusion. The court found the use of the GPS tracking device did not constitute a substantial intrusion upon the employee's seclusion because "it revealed no more than highly public information as to the van's location."[34] Because the van was the employer's property, "its use of the tracking device on its own vehicle [did] not rise to the level of being highly offensive to a reasonable person."[35] *Elgin* was a win for employers.

In Connecticut, The Electronic Monitoring Act requires employers to notify employees of any electronic monitoring that may be conducted in the workplace.[36] The Act applies to all Connecticut employers, both private and public sectors, regardless of the employer's size. The statute defines "electronic monitoring" to include the collection of information on an employer's premises that concerns employees' activities or communications by any means other than direct observation.[37] Despite such clear statutory language, the court in *Vitka v. City of Bridgeport* found that the installation of GPS devices in city-owned vehicles did not violate the Electronic Monitoring Act.[38] The data that the city retrieved from the GPS devices was inconsistent with the daily reports that the employees submitted to document their daily activities. Based upon this GPS data, the city instituted disciplinary proceedings against the employees. The court found that such monitoring of employee activities was permitted under the Electronic Monitoring Act, because a provision restricting the use of electronic surveillance in areas designed for personal comfort (i.e., bathrooms and locker rooms) was inapplicable outside that specific context. Further, the court noted that based upon the plain and unambiguous language of the statute, this type of monitoring was not subject to the advance notice requirements of the Act because it occurred on public roads and not on the employer's premises.

There may be no laws against using GPS to track employees, but using the devices can expose employers to liability under state and federal labor laws. In 2006, the city of Modesto, California, installed a GPS unit in the city truck driven by the president of a local municipal employees' union.

He filed a complaint with the state labor board alleging that the city violated labor laws by doing so. Although the union attorney representing the president acknowledged that public employees should not expect a right to privacy while using city vehicles in their work, he claimed the monitoring was directed at gathering information on the president's union activities. Likewise, in 2003, the general counsel of the NLRB issued a memorandum that agreed with an NLRB finding that a nonunion employer had violated the NLRA by installing GPS units in the trucks of two employees who were known union organizers. The employer had placed the GPS devices in just those two of the eight trucks the company owned. The GPS units tracked the two employees' movements, even during nonworking hours, and would have shown whether they went to a common location or visited the homes of other employees. The NLRB counsel said installing the units interfered with the employees' labor rights. The counsel reasoned that the employees were subjected to increased scrutiny without a legitimate business justification.

In summary, employer surveillance of employee activities using GPS or similar technology should not violate employee privacy if it's used for legitimate business reasons and is not abused. For example, instead of tracking all employee activities, it may be more prudent for employers to limit GPS surveillance to on-duty activities. Inform employees that they may be monitored, since the key privacy issue is typically whether an employee had a "reasonable expectation" of privacy. Monitoring could be limited to such legitimate business reasons as increasing productivity, aiding in quick responses to emergencies and improving the efficiency and timeliness of driving routes. Consider permitting employees to shut down monitors during meal breaks and other off-the-clock times. In addition, access to any information provided by tracking devices should be limited to those on a need-to-know basis. Finally, be aware of how the monitoring may be perceived, especially in connection with federal labor laws.

Employers should develop a written policy on GPS use, which should address such issues as:

- Notice of GPS tracking technology
- Access to data
- Shutdown of GPS unit during breaks/off duty
- Employer's right to monitor employee locations during working hours for business purposes
- Right to discipline employees based on location monitoring
- Method for collecting GPS data, and how you will store it and keep it secure

Video Camera Surveillance

Employers may have several reasons for wanting to use video surveillance cameras in the workplace. Cameras may be useful for preventing theft, monitoring employee performance to guarantee customer satisfaction, training, and investigation of sexual harassment or other suspected criminal wrongdoing by particular employees. When cameras are used in private areas (such as bathrooms) and/or without the knowledge and consent of the employees being observed, liability may result.

Workplace video surveillance in open or common areas is generally permissible. This is based on the notion that employees do not have a reasonable expectation of privacy in those places. Examples of areas that are "common" or "open" are:

- hallways
- lobbies
- employee cafeterias
- open offices
- warehouses
- any areas open to the public

Courts have generally held that video surveillance of these areas is legal regardless of whether the

surveillance is conducted with a visible or a hidden camera, and regardless of whether notice is given to employees.

On the other hand, courts have held that placing surveillance cameras in areas in which employees have a reasonable expectation of privacy without informing employees of the presence of these cameras can constitute a violation of employees' privacy rights. Workplace areas in which employees are deemed to have a reasonable expectation of privacy with regard to video surveillance include:

- employee dressing rooms
- bathrooms
- desks
- lockers

Employers are encouraged to consider carefully their need for video surveillance. Depending on the particular situation and corporate culture, employers will need to determine whether invisible cameras or open cameras should be used, taking into account issues such as legality, effectiveness, and employee morale. Also, employers should evaluate whether they want to put employees on prior notice that they may be monitored by video surveillance.

REMAINING UNCERTAINTIES

As noted, the area of employee privacy in workplace technology is constantly evolving and developing as courts begin to grapple with and address these issues directly. Though a well-drafted technology use policy is an important step towards protecting the employer's interest, it remains unclear where courts will draw the line between a "necessarily strict" and "unnecessarily broad" policy.

In a recent complaint filed by the National Labor Relation Board's (NLRB) Hartford, Connecticut office, the NLRB alleges that the American Medical Response of Connecticut, Inc. violated the National Labor Relations Act (NLRA) by terminating an employee for posting negative comments about her supervisor on her Facebook profile.[39] The employer has a social media policy that prohibits employees from disparaging supervisors in social media posts, even while off-duty and off-site on a personal computer and internet source. However, the policy does not include a statement that it would not be construed or applied in a manner that interferes with employees' rights under the NLRA. A NLRB investigation found that the employee's Facebook postings constituted protected activity and that the company's social media policy was overly broad. The NLRB's complaint alleges that application of the policy unlawfully interfered with the employee's right under Section 7 of the NLRA to engage in protected concerted activity, such as communicating with coworkers about the terms and conditions of employment.

Though the current law holds that a work policy which prohibits all criticism of an employer is presumed invalid, it has also been found that employers do not violate the NLRA by disciplining employees whose commentary rises to the level of disparagement or disloyalty. Due to the uncertainty surrounding this type of social media policy, employers should take caution before taking an adverse action against an employee for negative postings on a social networking website. At a minimum, employers should re-evaluate their current social media policies (or create one if one does not exist) and determine whether it would be appropriate to include an assurance that the policy will not be construed or applied in a manner that interferes with employees' rights under Section 7 of the NLRA.

---

[1] The author wishes to thank Kaitlyn Millerick, a Northeastern University co-op student, for

her invaluable assistance in the research and preparation of this article.

[2] Mass. Gen. Laws ch. 214, § 1B.

[3] Mass. Practice Series, vol. 45, Employment Law, § 7.1.

[4] *City of Ontario, Cal. v. Quon*, 130 S.Ct. 2619 (2010).

[5] *Id*. at 2630.

[6] *Id*. at 2623.

[7] *Id.* at 2624.

[8] *Id.* at 2629.

[9] *Id.*

[10] 18 U.S.C. § 2701(a).

[11] *Quon v. Arch Wireless Operating Co., Inc. et al.*, 529 F.3d 892, 899 (9th Cir. 2008), overruled by *Quon v. City of Ontario, Cal.*, 130 S.Ct. 2619 (2010).

[12] 18 U.S.C. § 2702(a).

[13] 18 U.S.C. § 2702(b)(3).

[14] *Bohach v. City of Reno*, 932 F.Supp. 1232 (D. Nev. 1996).

[15] *Id.* at 1236.

[16] *Fraser v. Nationwide Mutual Ins. Co.*, 352 F.3d 107 (3rd Cir. 2004).

[17] *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp.2d 548 (S.D.N.Y. 2008).

[18] *Pietrylo v. Hillstone Restaurant Group d/b/a Houston's*, 2009 WL 3128420 (D.N.J. Sept. 25, 2009).

[19] *Crispin v. Audigier, Inc.*, 2010 WL 2293238 (C.D. Cal. May 26, 2010).

[20] *Romano v. Steelcase, Inc.*, 2010 WL 3703242 (N.Y. Sup. Sept. 21, 2010).

[21] *Equal Employment Opportunity Commission v. Simply Storage Management, LLC et al.*, 2010 WL 3446105 (S.D. Ind. May 11, 2010).

[22] *McMillen v. Hummingbird Speedway, Inc. et al.*, No. 113-2010 CD (PA Sept. 9, 2010).

[23] 18 U.S.C. § 2701(c)(2).

[24] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 880 (9th Cir. 2002).

[25] *Pietrylo*, *supra* note 6.

[26] *Garrity v. John Hancock Mutual Life Ins. Co.*, 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002).

[27] *Doe v. XYC Corp.*, 382 N.J. Super. 122 (2005).

[28] *TBG Ins. Services Corp. v. The Superior Court,* 96 Cal.App.4th 443 (Cal. App. Ct. 2002).

[29] *Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300 (2010).

[30] *Nat'l Economic Research Associates, Inc. v. Evans*, 2006 WL 2440008 (Mass. Super. Aug. 3, 2006).

[31] *Id.* at *5.

[32] *Scott v. Beth Israel Medical Center, Inc.*, 2007 WL 3053351 (N.Y. Sup. Oct. 17, 2007).

[33] *Elgin v. St. Louis Coca-Cola Bottling Co.*, 2005 WL 3050633 (E.D. Miss. Nov. 14, 2005).

[34] *Id.* at *4.

[35] *Id.*

[36] C.G.S.A. § 31-48d.

[37] *Id.* at § 31-48d(a)(3).

[38] *Vitka v. City of Bridgeport et al.*, 2007 WL 4801298 (Conn. Super. Dec. 31, 2007).

[39] National Labor Relations Board news release (November 2, 2010), http://www.nlrb.gov/About_Us/news_room/ (last visited on November 4, 2010).