NHMTA

NEW HAMPSHIRE MOTOR TRANSPORT ASSOCIATION

2014 Annual Directory

19 Henniker Street
P.O. Box 3898
Concord, NH 03302
Phone: 603-224-7337
Fax: 603-225-9361
www.nhmta.org

2013 Master Truck Driver Certification Winners

Kenneth Arnold, Wal-Mart Transportation; Anthony Cinquegrana, Wal-Mart Transportation; New Hampshire Department of Safety, Commissioner John J. Barthelmes; New Hampshire Governor, Maggie Hassan; Andrew Worster, Con-Way Freight; Lyle Stenersen, Wal-Mart Transportation; David Knowles, Ciardelli Fuel

WORKPLACE PRIVACY IN THE DIGITAL AGE

BY KEVIN HASKINS PretiFlaherty

Kevin Haskins

The modern workplace is defined by technology. Desktops, laptops, smartphones, tablets, and a bewildering array of applications and internet-based services—all of these are now ubiquitous features of the business world. It goes without saying, however, that technology is not unique to the workplace. More often than not, employees use this same technology for both business and personal purposes, bringing their personal lives into work and vice versa.

The blended use of technology for both professional and personal communication has had a significant impact on workplace privacy. Gone are the days when all an employer knew about an employee was what could be observed during the workweek and at the annual holiday party. Now, through technology, employers can monitor employees inside the workplace and out, and can delve into employees' backgrounds, internet usage, and email habits, among other things. Yet, notwithstanding these technological changes, employees continue to assume that they have some degree of privacy in their electronic communications.

This article explores several areas where workplace privacy in electronic communications is evolving with technology. These areas include: (1) monitoring employee internet usage, particularly social media; (2) monitoring employee email and similar electronic communications; and (3) developing and enforcing workplace technology policies.

I. INTERNET MONITORING

The internet provides incredible fodder for employers interested in learning about both the professional and personal lives of employees. Much of this information (and arguably the most tantalizing) can be found on social networking sites. Given the widespread use of social media—Facebook, for example, reported in August 2013 that one out of three people in the United States visits Facebook every day—this information is also readily available.

From a privacy perspective, the question for employers is: what restrictions are there on viewing or accessing online information about employees, particularly information gleaned from social networking sites? The answer depends in large part on how the employer gains access to the information. If an employer does not have authority to access an employee's social media information, it risks violating federal electronic communications law as well as running afoul of state invasion of privacy laws.

A. FEDERAL ELECTRONIC COMMUNICATIONS LAW AND STATE INVASION OF PRIVACY LAW

The most relevant federal law governing access to employee electronic communications is the Electronic Communications Privacy Act (ECPA). The ECPA actually contains two sections: the Wiretap Act and the Stored Communications Act (SCA). The Wiretap Act prohibits unauthorized, intentional "interception" of wire, oral or electronic communications, including email. The SCA, meanwhile, prohibits unauthorized access of electronically "stored" communications. However, an important exemption applies to companies that maintain their own electronic communications systems. For these companies, there is considerably more latitude to access electronic information that is transmitted or stored on their proprietary systems.

Invasion of privacy claims, on the other hand, are generally governed by state law. In New Hampshire, for example, the tort of invasion of privacy resulting from an intrusion upon a person's solitude or seclusion requires: (1) an intentional intrusion, physical or otherwise, upon a person's private affairs; and (2) the intrusion would be highly offensive to a reasonable person.

Over the last several years, there has been a proliferation of cases involving SCA and invasion of privacy claims arising from employers accessing employee social media information. For example, in *Ehling v. Monmouth-Ocean Hosp. Service Corp.*, a court found an employer was not liable under the SCA or state invasion of privacy laws when it "passively" obtained social media information about an employee from another employee. The plaintiff in this case, Deborah Ehling, was a registered nurse and paramedic who began working at Monmouth-Ocean Hospital (MONOC) in 2004. Ehling was also the president of a union, and in this capacity (and perhaps to the chagrin of management) she was "regularly involved in actions intended to protect MONOC employees," such as filing complaints with the EPA over MONOC's use of certain disinfectants and testifying in a wage and hour lawsuit of another coworker.

Ehling also had a Facebook account. Ehling used privacy settings on her account so that only her Facebook friends could see her Facebook wall. Although Ehling was Facebook friends with

many of her MONOC coworkers, she was not Facebook friends with any MONOC managers. One of Ehling's Facebook friends was a coworker named Tim Ronco. For some unknown reason, Ronco began taking screenshots of Ehling's Facebook wall and sharing them with a MONOC manager named Andrew Caruso. Although Ronco and Caruso did not work in the same division at MONOC, the two had become friends while working together at a previous job. Ronco apparently shared Ehling's posts on his own initiative—Caruso never asked Ronco for information about Ehling and never asked Ronco to keep him informed of Ehling's Facebook activity. At no time did Caruso have the passwords to either Ronco's or Ehling's Facebook account, or any other MONOC employee's account.

In June 2009, Ehling posted a comment to her Facebook wall about a shooting attack by a white supremacist at the Holocaust Museum in Washington, D.C. In her post, Ehling said she "blame[d] the DC paramedics" who had kept the attacker alive after he had been shot by guards. She also said the guards should "go to target practice." After management became aware of Ehling's post, MONOC suspended her with pay.

Ehling subsequently filed a complaint with the National Labor Relations Board (NLRB). However, the NLRB dismissed the complaint, finding no violation of the National Labor Relations Act and no privacy violation because Ehling's post was sent, unsolicited, to MONOC management.

Ehling then filed suit in federal court alleging a variety of claims, including claims arising under the SCA and invasion of privacy. MONOC moved to dismiss, but the court denied the motion, finding that the interplay between social media and privacy is still evolving and that, as a result, privacy claims must be examined on a case-by-case basis.

However, after the close of discovery, MONOC prevailed on summary judgment. With regard to the SCA claim, the first issue for the court was whether the SCA applies to non-public Facebook wall posts. Here, the court noted that the SCA essentially protects: "(1) electronic communications; (2) that are transmitted via an electronic communication service; (3) that are in electronic storage; and (4) that are not public." Private Facebook posts, the court concluded, meet all four criteria. Consequently, because Ehling had used privacy settings that restricted access to only her Facebook friends, her Facebook posts were covered by the SCA.

Having determined that the SCA covered Ehling's Facebook posts, the court next examined whether MONOC could avoid liability because it was "authorized" to view Ehling's posts. Here, the court found MONOC was authorized to do so: because Ronco was a Facebook friend he was authorized to view Ehling's Facebook posts and, because he was an authorized user, he was able to authorize MONOC to view any posts he could view.

As for the privacy claim, Ehling needed to prove that MONOC's access to her Facebook post: (1) intruded on the solitude or seclusion of her private affairs; and (2) the intrusion would highly offend a reasonable person. Here, the court found Ehling could not get past the first prong. The evidence did not show that MONOC gained access to Ehling's Facebook page by "logging into her account, logging into another employee's account, or asking another employee to log into Facebook." Rather, the evidence showed that MONOC was a "passive recipient" of information that "they did not seek out or ask for." In conclusion, the court found that while MONOC's access to Ehling's Facebook posts "may have been a violation of trust . . . it was not a violation of privacy."

In contrast to *Ehling*, the court in *Pietrylo v. Hillstone Restaurant Group* upheld a jury verdict finding that an employer violated the SCA when it accessed without permission a password-protected and invitation-only MySpace page. The plaintiff in this case, Brian Pietrylo, had created the MySpace page so that he and his coworkers could talk about their employment. As Pietrylo explained in his initial post, the purpose of the page was to "vent about any BS we deal with out [sic] work without any outside eyes spying in on us. . . . Let the shit talking begin."

Several managers obtained access to Pietrylo's MySpace page by asking for log-in credentials from one of the employees, Karen St. Jean, who had access to the page. After gaining access to the site, management terminated Pietrylo and explained that his termination was because of his operation of the MySpace page.

Pietrylo filed suit alleging claims under the SCA and state privacy law, among other things. The jury found against Pietrylo on his invasion of privacy claim, finding that he had no reasonable expectation of privacy in the MySpace page. However, the jury found in favor of Pietrylo on his SCA claim, finding that management had intentionally accessed the MySpace page without authorization.

Management appealed the jury verdict, but the court affirmed based on the testimony St. Jean provided at trial. St. Jean testified that she provided her log-in credentials only because she worked directly under her managers and felt that she "probably would have gotten in trouble" had she not provided the information. Had another coworker asked the information, St. Jean testified that she would not have given it.

Based on St. Jean's testimony, the court concluded that a jury reasonably could have inferred that St. Jean's "authorization" was coerced or provided under pressure. In consequence, the jury had a reasonable basis to conclude that the managers' access to the MySpace page was not authorized under the SCA.

B. ANTI-DISCRIMINATION LAWS

Employers should keep in mind, however, that even if access to an employee's social media information is authorized—for example, the information may be publicly available—restrictions may still apply to how specific content is used. The chief restrictions here are federal and state anti-discrimination laws. Thus, even if an employer's access to an employee's social media page fails to give rise to a "privacy" claim under the SCA or state privacy laws, the employee may still have a discrimination claim if the employer learns of an employee's protected status online and then uses this information in making an adverse employment decision.

II. ACCESSING EMPLOYEE EMAIL, TEXT MESSAGES, AND TELEPHONE CALLS

Employers have legitimate reasons for wanting to view emails and similar electronic communications sent by employees. For example, employee use of electronic media may lead to inadvertent (or intentional) disclosures of confidential information or trade secrets. Employers may also want to monitor email and similar communications to ensure that employees are actually doing their work and not spending excessive amounts of time on personal matters or sending out solicitations or "spam" that clog resources and distract others.

Although employers have considerable discretion to monitor and access electronic communications such as email, employers do not have unfettered access. Again, the primary restrictions are the ECPA, including both the Wiretap Act and the SCA (and state corollaries), as well as state invasion of privacy laws.

A. EMAIL FROM PROFESSIONAL ACCOUNTS

Employers have the greatest degree of discretion when monitoring employee email that is sent or received on employer-provided accounts. This is because the ECPA generally exempts communications related to the "normal course of business" as well as those that are transmitted or stored on proprietary communications systems. As a result, monitoring email from an employer-provided professional account is generally permissible.

Furthermore, because employer-provided accounts are proprietary and belong to the employer, employees generally have no reasonable expectation of privacy in information that is transmitted on such accounts. In fact, cases have held that employees do not have a reasonable expectation of privacy in employer-provided accounts even when employers have promised it.

In *Smyth v. Pillsbury Co.*, which was one of the first cases to address email privacy in the workplace, the plaintiff sued his employer for invasion of privacy after he was terminated for sending inappropriate and threatening comments to a supervisor through Pillsbury's email system. Pillsbury had previously told all of its employees that email communications were private and would not be used as grounds for termination or discipline. Nonetheless, Pillsbury intercepted Smyth's emails and terminated him. Ultimately, the court denied Smyth's claim, finding there is no "reasonable expectation of privacy in email communications voluntarily made by an employee to his supervisor over the company email system notwithstanding any assurances that such communications would not be intercepted by management."

Although it is generally presumed that employees have no reasonable expectation of privacy in email accounts provided by their employer, employers may strengthen this presumption by adopting policies that expressly deny any right of privacy in employer-provided accounts.

B. EMAIL FROM PERSONAL ACCOUNTS

Questions arise when employees access personal email accounts (*e.g.* Gmail, Hotmail, Yahoo, etc.) through employer-provided networks. Increasingly, employees are resorting to these accounts for their personal correspondence and using their work accounts strictly for work email. The question, of course, is whether employees have a reasonable expectation of privacy when using these personal email accounts, even when they are used during work.

As with email sent from professional accounts, there is growing consensus that employers may monitor email sent or received from personal accounts—*provided the emails are sent and received over the employer's network.* Again, the key here is the exemption in ECPA, which allows employers to monitor traffic over its proprietary electronic communications systems. Employers may also dispel any reasonable expectation of privacy that employees might have in email sent from personal accounts by expressly stating in a policy that all email sent over the employer's network, including email from personal accounts, is subject to monitoring.

That being said, courts have found that employees continue to have privacy rights in email from personal accounts in at least two situations. First, courts have found that employees continue to have an expectation of privacy in personal email accounts themselves. As a result, even if an employer has a technology policy that purports to authorize access to personal email accounts, employers who access those accounts without authorization may be liable under the SCA and state privacy laws.

For example, in *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, a gym maintained a policy stating that employees had no right of privacy in matter stored in or created on the company's network, including the "use of personal email accounts on company equipment." The policy also notified employees that computer usage was subject to monitoring at any time and without notice.

The employee, who was a fitness instructor at the gym, left to start a competing fitness facility in the same town. After the employee left, the gym's owner apparently accessed the employee's Hotmail and Gmail accounts by using the usernames and passwords that were stored on the gym's computer, and then printed several emails that contained information about the employee's efforts to open the competing facility. Using these emails as evidence, the gym then sued the employee to enforce a non-competition agreement.

The non-competition agreement was found to be unenforceable. However, that did not end the matter. Instead, the employee then removed the lawsuit to federal court and alleged that the gym's unauthorized access of his personal email accounts violated the SCA. In defense of this claim, the gym argued that the employee had waived all right to privacy in his personal email account because he had received the gym's technology policy. The court, however, disagreed and found that the gym's technology policy only applied to the company's equipment and any emails composed or transmitted on that system. The policy did not go so far as to encompass emails stored, created, or transmitted on outside systems not belonging to the gym.

The second situation where employees may continue to have an expectation of privacy in emails sent or received from personal accounts involves privileged communications with attorneys. For example, in *Stengart v. Loving Care Agency, Inc.*, an employee named Marina Stengart sued her employer, Loving Care Agency, claiming that a hostile work environment had led to her constructive discharge. In the course of discovery, Loving Care searched her company-issued laptop and discovered she had used it to access her personal Yahoo email account for purposes of corresponding with her attorney. Loving Care was able to retrieve from the laptop copies of those emails.

Stengart demanded that Loving Care turn over the emails, which she considered to be privileged. Loving Care refused, however, claiming that it had a right to access the emails under its technology policy, which reserved the "right to review, audit, intercept, access, and disclose all matters on the company's media systems and services at any time, with or without notice." The policy also stated that although "occasional personal use" of email was permitted, the "principal purpose of electronic mail is for company business communications."

The New Jersey Supreme Court ultimately held that Stengart could reasonably expect that email communications with her attorney through her personal account would remain private, and that using the company's laptop to send the communications did not waive the privilege. In reaching this conclusion, the court noted that the technology policy did not define what the company's "media systems" were, nor did it explicitly mention personal email accounts. As a result, the policy did not effectively put employees on notice that messages sent on a password-protected web-based account were covered by the policy. In addition, the court noted that Stengart had taken steps to protect her correspondence with her attorney: she had used a password-protected personal email account instead of her work account. In the court's view, this established a "subjective expectation of privacy in messages to and from her lawyer discussing the subject of a future suit."

It is unclear at this time whether courts in New Hampshire would follow New Jersey's lead in *Stengart*. Although New Hampshire courts have found that email communications with counsel may be privileged under the attorney-client privilege,

they have also found the privilege may be waived by disclosure to third-parties. Consequently, it remains an open question as to whether New Hampshire courts would find the privilege waived where an employee's email to counsel from a personal account is "disclosed" to the employer by virtue of the fact that the email was sent over the employer's network.

C. EMPLOYEE TEXT MESSAGES

In *City of Ontario v. Quon*, the U.S. Supreme Court found that the City of Ontario, California did not violate a SWAT officer's right to privacy in text messages sent to and from a City-issued pager. The City provided pagers to officers with an allotment of 25,000 characters per month, after which overage charges applied. When the City first issued the pagers, it informed officers that it considered pager messages to be email and that the messages "would fall under the City's policy as public information and [were] eligible for auditing" overages. However, in practice, the City did not routinely monitor messages and verbally told officers that messages would not be audited if the officers simply paid any overages.

The officer in this case, Jeff Quon, often exceeded his character limit but always paid for his overages. However, after receiving complaints that too many officers were exceeding their limits, the chief of police ordered Quon's supervisor to obtain transcripts of text messages sent by employees with overages, including Quon. Quon's messages included many sexually explicit messages. After learning that the City had read his text messages, Quon sued alleging that the City had violated his privacy rights under the Fourth Amendment.

The Supreme Court dodged the question of whether Quon had a reasonable expectation of privacy in the text messages he sent from his pager. Rather, the Supreme Court found that even if Quon had such an expectation of privacy, the City did not violate his Fourth Amendment rights by obtaining the texts because the search was reasonable.

Although *Quon* arose under the Fourth Amendment, which generally does not apply to employers in the private sector context, the Court's holding in *Quon* nonetheless has the potential to impact state common law privacy claims. This is because *Quon* confirms that even if an employee has a reasonable expectation of privacy in electronic communications, an employer may still be able to search or review those communications provided its actions are reasonable under the circumstances.

D. EMPLOYEE TELEPHONE CALLS

The federal Wiretap Act and state corollaries prohibit unauthorized interception of oral communications. Consent in this area is very fact specific. For example, although a technology policy may explain that employees have no expectation of privacy in telephone calls and that calls are monitored, such a policy may not be enough if an employee is able to maintain that he or she did not receive the policy or was not aware of it. In addition, although an exemption exists under federal law for calls made "in the ordinary course of business," this only covers business telephone calls, not personal telephone calls.

III. WORKPLACE TECHNOLOGY POLICIES

In *City of Ontario v. Quon*, the Supreme Court emphasized the importance of technology in employees' lives, observing that "cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." In light of this importance, the Court noted that written policies, and the operational context in which they are applied, are critical to determining the reasonable expectation of privacy in electronic communications. In the Court's words, "employer policies concerning [monitoring of electronic] communications . . . shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated."

Clearly, workplace technology policies are essential tools for defining the scope of privacy in electronic communications. In preparing and enforcing technology policies, however, employers should be mindful of two potential pitfalls: (A) overbroad technology policies; and (B) discriminatory enforcement of technology policies.

A. OVERBROAD TECHNOLOGY POLICIES

Recently, the National Labor Relations Board (NLRB) has scrutinized employer technology policies to ensure that such policies do not unreasonably "chill" the rights of employees to exercise their rights under the National Labor Relations Act (NLRA).

For example, in May 2012, the Acting General Counsel of the NLRB released a memorandum detailing seven cases in which it had examined technology policies governing the use of social media. In six of the cases, the NLRB found the policies were overbroad. Many of these policies contained provisions that,

on their face, would appear to be innocuous. For example, the NLRB found that a provision instructing that "offensive, demeaning, abusive or inappropriate remarks are as out of place online as they are offline" was unlawful, because it proscribed a "broad spectrum of communications that would include protected criticisms of the Employer's labor policies or treatment of employees." In only one case was a policy determined, with revisions, to be lawful under the NLRA. This policy was upheld because, unlike those in the other six cases, it was not ambiguous and could not be reasonably interpreted by employees as prohibiting protected activity. The NLRB found the policy was not ambiguous because it provided specific examples of prohibited conduct.

More recently, in *UPMC et al. v. SEIU Healthcare Pennsylvania*, the NLRB reviewed a number of technology policies maintained by a group of hospitals. The policies included a non-solicitation policy, an electronic mail policy, and an acceptable use of information technology policy. The SEIU claimed that the policies were facially overbroad because they restricted the rights of employees to communicate about the terms and conditions of employment.

The NLRB found that the non-solicitation policy was lawful because it prohibited all solicitation, regardless of nature, and therefore did not single out collective activity. However, the NLRB found the electronic email policy was overbroad because it allowed some non-work use of the email system and banned only communications that were "disruptive," "offensive," or "harmful to morale." Because the policy banned only some non-work use and was ambiguous about which specific acts were prohibited, the NLRB found the policy could reasonably be construed by employees to prohibit protected activity. Similarly, the NLRB found the acceptable use policy unlawful because although it allowed "de minimis" personal use of company equipment, it was ambiguous as to what activities were acceptable.

At the same time (and to the relief of employers), the NLRB has also recently stated that employees do not have an automatic right to use an employer's electronic communication system for purposes of engaging in activity protected under the NLRA. In *Register Guard*, the NLRB noted that the company's electronic communications system, including its email system, was the company's property. In consequence, because the company had the legal right to bar non-work uses of its systems, the company's policy prohibiting use of the system for "non-job-related solicitations" was facially valid.

B. DISCRIMINATORY ENFORCEMENT

In *Register Guard*, discussed briefly above, the NLRB found that a company's technology policy was not facially overbroad where it restricted "non-job-related solicitations." However, in the same case, the D.C. Circuit Court of Appeals (which heard the case upon appeal) found that the company nevertheless enforced the policy in a discriminatory manner. At issue in the case were three emails sent by an employee to her co-workers relating to work and the local union. One email asked co-workers to wear a certain color in support of union negotiations; a second email asked co-workers to assist with the union's upcoming parade; and a third corrected an earlier email from a co-worker about a union rally. The company disciplined the employee for improper use of the employer's email system for "union business."

As for the company's technology policy, it stated that the company's communication systems were owned by the company for purposes of conducting company business. It also prohibited the use of the system to "solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations." In practice, the company allowed many non-business emails to be sent on its communications system, including personal emails as well as solicitations for social events and pet services. Apparently, no discipline had ever resulted from these mailings.

The court found that the company improperly disciplined the employee for sending one of the emails because the email was not a solicitation. In addition, the court found there was insufficient evidence to support the conclusion that the remaining two emails violated the company's policy prohibiting "non-job-related solicitations." The court noted that the policy made no distinction between solicitations by groups as opposed to individuals and therefore purported to prohibit all non-job-related solicitations. Moreover, the reason given to the employee for her discipline focused on the union-related content of her emails. Finally, the court noted that no other employees had been disciplined for violating the policy, even though employees had clearly breached it in the past. Thus, the court found there was evidence that the company disciplined the employee based on her union activity.

In light of *Register Guard*, then, employers must ensure that they do not apply their technology policies in a discriminatory manner. Employers that selectively enforce their technology policies against employees for exercising statutory rights run the risk of violating the NLRA and state labor laws.

IV. CONCLUSION

As technology continues to evolve so, too, are the laws and practices surrounding workplace privacy in electronic communications. Navigating workplace privacy in the digital age presents a number of challenges to employers. There are few bright line rules and very often the determination of whether a reasonable expectation of privacy exists in an electronic communication depends on specific facts.

For employers, one of the best strategies for dealing with this evolving area is to maintain a technology use policy that clearly and explicitly explains the purpose and uses of its electronic communications system, as well as the privacy rights employees can expect to have with respect to communications sent or received on the system. Although there is no "one-size-fits-all" approach for developing such a policy, employers should consider the following objectives:

- Provide clarity to employees and explain that the company's electronic communications system and related equipment are owned by the company;
- Explain the company's rights, as owner of the system, to monitor, search, access and read information on the system and the related equipment;
- Make clear that employees have no expectation of privacy in information created, transmitted, received, or stored on the system or any device/equipment provided by the company;
- With respect to email, be clear that there is no expectation of privacy in emails sent or received from a personal email account via the company's electronic communications system;
- Given that employees will almost certainly use the system for some "personal use," acknowledge that "limited" personal use is allowed, subject to the other provisions of the policy;
- When possible, provide specific examples of the conduct prohibited under the policy;
- Strive to eliminate ambiguity in provisions that could be construed as limiting the rights of employees to engage in protected activity;
- As a savings clause, consider adopting a general statement providing that nothing in the policy should be construed as limiting employee rights under the NLRA and state labor laws;
- Make sure the policy is written and distributed to all employees, and ensure that the policy is implemented as written (i.e. no "verbal" alterations).