

EMPLOYEE PRIVACY – WHOSE INFORMATION IS IT ANYWAY?

Many employers believe that they have the right to control the conduct of their employees if that conduct might adversely impact the image or reputation of the company. With the rapid expansion of email and text messaging, the separation between business and personal lives of employees has become blurred. The explosion of information available on the internet, and the growing popularity of social websites such as Facebook and Twitter, has created conflicts between the employee's right of privacy and the employer's right to know information which might impact the business. As the technology changes at breakneck speed, lawmakers and courts are struggling to balance these competing interests in a number of areas.

1. Employee Background Checks

Many employers believe that conducting thorough background checks, including credit reports and criminal histories, is the best way to hire quality employees. There are strict statutory requirements imposed on the collection and use of this information, and some states have totally banned their use for employment purposes. The California Legislature has passed bills banning the use of credit reports and criminal histories for employment purposes during the past several years, only to see those bills vetoed by Governor Schwarzenegger. No one is quite sure how Governor Brown will react to these bills if they again are passed by the Legislature, but during his prior term Governor Brown rarely exercised the veto power and still holds the record for the lowest percentage of bills vetoed in the history of California. Efforts to ban the use of this information also are underway in Congress, although the recent shift in power may impact their passage.

Even if the use of credit reports and criminal histories is not banned entirely, their use is subject to scrutiny by administrative agencies and the courts if that use results in unlawful discrimination. The Equal Employment Opportunity Commission recently filed a federal court lawsuit against a major national company on the grounds that its use of backgrounds checks and credit reports resulted in the illegal exclusion of minority applicants. (*EEOC v. Kaplan*, Complaint filed 12/10.) Any employer who uses such information in making employment decisions should exercise caution and insure compliance with all statutory requirements.

2. Email and Text Messages

Many employers provide their employees with computers and/or cellphones for use in connection with the business. Some companies have policies governing personal use of those devices, and several courts have addressed the issue of employee privacy in the personal use of company email and text messages.

In *City of Ontario v. Quon*, police officers were provided with cellphones and advised that any personal usage would require reimbursement. Officer Quon paid for his personal use, but was disciplined after it was discovered that he was sending personal text messages and emails containing sexually explicit content. Quon sued for breach of privacy, claiming that the City had no right to look at his personal emails and text messages. Since the matter involved public employment, the lawsuit was analyzed under Fourth Amendment search and seizure standards requiring Quon to show (1) that he had an expectation of privacy in his personal messages and (2) that the governmental intrusion was unreasonable in scope. The Ninth Circuit Court of Appeals agreed with Quon on both counts, finding that the department's policy of making Quon pay for personal messages gave him

a reasonable expectation of privacy and that the departmental review of his personal messages was unreasonable. The United States Supreme Court agreed to hear the case, and many were hopeful that it would determine the issue of whether an employee has a constitutional right of privacy in personal email/texts sent on company equipment. The Supreme Court declined, stating that it is “uncertain how workplace norms will evolve” and that “the judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.” Instead, the Supreme Court reversed on very narrow grounds by simply *assuming* that Quon had an expectation of privacy and finding that the search was reasonable given the department’s need to review personal usage in order to recover reimbursement from Quon.

Lacking clear constitutional direction from the United States Supreme Court, courts are left to wrestle with the issue of employee privacy under state law. Two recent decisions addressing the issue of whether an employee has an expectation of privacy when using company equipment to communicate with a personal attorney reached different conclusions. In *Stengart v. Loving Care*, the New Jersey Supreme Court held that the employee had an expectation of privacy and did not waive the attorney-client privilege when she used a company computer to send email to her attorney through a personal web-based email account. The Court suggested that the result would have been the same if the employee had used the company email account because the employer’s policy acknowledged that occasional personal use of company email is permitted.

In *Holmes v. Petrovich*, the California Court of Appeals reached the opposite conclusion on breach of privacy claims arising from the employer’s retrieval and use of employee emails sent to her attorney through a company computer. Even though the employee attempted to delete the emails from the system after sending them, the Court held that the employee’s communications with her attorney were not protected because the company policy specifically stated (1) that the company owned the computers, (2) that the computers may not be used for personal business, (3) that the company monitored the computer for compliance and (4) that the employee had no expectation of privacy in anything sent on company computers. The Court concluded:

The emails sent via company computer under the circumstances of this case were akin to consulting her lawyer in her employer’s conference room, in a loud voice, with the door open, so that any reasonable person would expect that the discussion of her complaints about her employer would be overheard by him.

While the issue of employee privacy with respect to email or texts sent on company equipment is not resolved, it is critical for employers wishing to exercise control over employee communications to adopt and enforce policies stating: (1) that the company owns all computers and phones provided to employees, (2) that the company computers and phones are not to be used for personal purposes, (3) that the company has the right to monitor employee use of company computers and phones, and (4) that the employee has no expectation of privacy in the use of company computers and phones. Strong policies will provide the most protection to employers who are faced with issues relating to employee use or abuse of email and texting.

3. Social Media

The increasing popularity of social media is creating a host of new problems for employers. Facebook currently has more than 1/2 billion users, while Twitter has more than 100 million followers. It would be incorrect to assume that those involved in social media are primarily young

or unemployed, as 60% of Facebook and Twitter users are 35 years of age or older. There is no doubt that social media activity occurs during working hours, and on workplace equipment.

By statute, California employers are prohibited from disciplining employees for lawful off-duty conduct. There is an obvious tension between this respect for employee privacy and the desire of employers to prevent online behavior which might expose the company to ridicule or liability. On one extreme, workers at a Domino's Pizza created a YouTube video in which they engaged in unsanitary acts with food while wearing company uniforms. After considerable detective work, Domino's identified the employees and fired them. The employees had no basis for a claim because the conduct directly related to their job and violated food safety laws.

On the other extreme, employees who were fired for engaging in online conversations about working conditions on a private website using personal computers recovered a damage award for breach of privacy. The employer discovered the private chat group when a manager overheard employees talking about it and demanded the password. Based on the manager's conduct, the jury awarded compensatory and punitive damages against the employer.

Between these extremes is the case of a female firefighter who placed nude photos of herself with firefighting gear on her private MySpace page. At some point the privacy settings were changed to permit public viewing of her MySpace page, at which time her employer saw the photos and reprimanded her. She reacted badly to the reprimand, and was fired for insubordination. Her claims were rejected because the termination was not the result of her online conduct, but instead was the result of her insubordination.

In addition to the statutory prohibition against disciplining employees for lawful off-duty conduct, employers are precluded by Section 7 of the National Labor Relations Act (NLRA) from restricting employee communications concerning working conditions. The National Labor Relations Board (NLRB) recently filed an action against a company which had a written policy prohibiting derogatory comments concerning the employer and which used that policy to fire an employee for engaging in a Facebook chat with fellow employees concerning her supervisor. The NLRB issued a news release to publicize its prosecution of the case, a highly unusual event which suggests the importance it attaches to employer conduct which restricts concerted activity by employees. Section 7 applies with equal force to non-union employers, and applies to employee communications through social media in the same manner that it applies to conversations around the water cooler.

The resolution of cases involving social media involves a balancing act between the employee's right of privacy and the employer's right to control activity which might impact the business. A critical component in this analysis is the existence and enforcement of employer policies regarding: (1) access and use of social media during working hours and on company equipment; (2) warnings against online conduct which is harassing, defamatory or offensive and which could create liability if committed in the workplace; and (3) warnings against disclosure or use of confidential company information.

4. Conclusion

The tension between the employee's right of privacy and employer's desire to control conduct which might impact the business will increase as technology continues to blur the line between work life and home life. The laws in this area are changing rapidly, and employers are advised to stay abreast of new legislation and court decisions. In addition, employers are strongly encouraged to implement and enforce clear policies with regard to employee conduct and the use of company equipment.