SEYFARTH SHAW LLP ATTORNEYS

Seyfarth eDIGital

In this Issue

Employee Privacy in Personal Messages Transmitted on Company Servers

In this issue of Seyfarth eDIGital, Seyfarth Shaw's eDiscovery and Information Governance practice group newsletter, we will explore how employee use of company computers and mobile devices for personal use has impacted employee privacy in the workplace.

In recent years, employers have struggled with privacy issues arising from employee use of company equipment for personal purposes. Recent trends in online communication platforms, including social networking and professional networking sites, have only increased the ways in which employees may use company systems for personal use, blurring the lines between personal and work devices.

To address these issues, employers have implemented policies restricting personal use of company computers and devices. These policies vary, with some banning personal use altogether and others allowing limited or reasonable personal use. Employer policies also often include provisions in the policy which allow them to monitor employees' activities on company systems.

While a clear policy regarding acceptable use of company systems helps to define whether an employee's expectation of privacy is reasonable, the analysis often does not end there. Other factors, such as whether the company or the employee owns the device, and whether attorney-client communications are implicated, further complicate the issue of employee privacy in communications transmitted using company systems.

Employees' Reasonable Expectation of Privacy in Personal Communications

The issue of an employee's right to privacy often arises when an employer discovers the employees' purportedly private information during the course of an internal investigation, through routine monitoring, or in responding to discovery requests in litigation. In general, for an employee to have a valid invasion of privacy claim,

he or she must show that there was a reasonable expectation of privacy. In order for an employee to have a reasonable expectation of privacy, there must be: 1) a subjective expectation of privacy; 2) that is reasonable; 3) upon which an intrusion would be highly offensive to a reasonable person.

In evaluating employees' claims of privacy in the workplace, courts have considered whether the company had a policy in place regarding the use or monitoring of its network and systems. In *Thygeson v. U.S. Bancorp*, the court examined whether the plaintiff employee had a reasonable expectation of privacy where the company policy prohibited personal use of the computer and informed employees of the possibility of monitoring their activities.[1] As part of an internal investigation into the employee's performance, the company retrieved a listing of the internet sites he visited and reviewed emails stored in a network folder labeled "personal."[2] The court found that any expectation of privacy the employee may have had was unreasonable in light of the company's IT policy and the fact that the files were stored on the company's network.[3]

The increased use of company provided mobile devices and systems which are frequently used by employees for personal communications complicates the privacy analysis and has led to increased uncertainty regarding the scope and nature of permissible employer monitoring. Many practitioners believed that the Supreme Court's opinion last summer in *City of Ontario, California v. Quon* would provide some finality and clarity to the issue of permissible monitoring of employee communications on work related systems. [4]

City of Ontario, California v. Quon

The *Quon* case involved a police officer, whose text-capable pager was provided for him by his employer, the City of Ontario. The City's written internet and email policy stated that it had the "right to monitor and log all network activity including email and Internet use, with or without notice," and that employees had "no expectations of privacy or confidentiality" when using devices. Officers were routinely exceeding the monthly allotment of text messages, and in the course of a police department investigation of personal pager use, officer Quon was found to have sent several sexually explicit personal text messages with the City-issued pager device. Quon sued the City of Ontario claiming, among other things, that his Fourth Amendment right against unreasonable search and seizure had been violated.

The Supreme Court opined that even if Quon had a reasonable expectation of privacy in his messages, the search was reasonable, and there had been no Fourth Amendment violation. The Court first found that there was a documented technology policy that clearly explained the limited expectation of privacy employees should have in City-provided devices.[5] Second, the Court held that the City had "a legitimate work-related" reason to review the messaging content.[6] The justices reasoned that a "non-investigatory, work-related purpose," such as a review of the text messaging plan, or the investigation of work-related misconduct would both be "regarded as reasonable and normal in the private-employer context," [7] and that the City's search "was not excessively intrusive" in light of the purpose, i.e., making sure that the City taxpayers were not paying for extensive personal text messaging. [8]

While the Court limited the *Quon* holding to public employees and to the facts of the particular dispute, the two factors considered in the opinion provide some guidance to private sector employers contemplating searches of employee communications. A clearly defined and written technology usage policy, and a legitimate purpose for monitoring or investigation should be every employer's starting point when considering the boundaries of monitoring or reviewing employee communications.

Key Takeaways and Considerations for Implementing a "Personal Use" Policy

Implementing a policy prohibiting personal use of company IT systems and notifying employees that their activities may be monitored does not in and of itself provide a blanket license to search employees' activities and files. The presence or absence of such a policy, and its provisions, is just one factor the court will take into account in analyzing whether an employee has a right to privacy in his or her personal communications transmitted on company servers. In addition to the policy, courts will generally take the following factors into consideration:

- Type of notice to employees regarding personal use and potential monitoring, including whether the notice was written and acknowledged by the employee;
- The frequency of the notice given to the employee (e.g., daily startup screen notice);

- Whether the policies regarding use and monitoring are implemented and enforced;
- Type of monitoring that occurs (e.g., internet site history vs. content);
- Any precautions or measures the employee put in place to protect her information, such as using personal email accounts or password protection;
- Whether the company or the employee owns the computer or mobile device;
- Local statutes and regulations regarding employee email and internet access monitoring;[9] and
- The reason for monitoring the employees' email and/or internet usage.

The decision to monitor an employee's email or internet usage should be made in consultation with counsel. The circumstances will vary case-by-case and may require additional considerations of other issues, such as attorney-client communications. The discovery of an employee's attorney-client communications on company systems and the potential for a waiver of privilege will be discussed in the next issue of Seyfarth eDIGital.

Please contact the member's of Seyfarth's eDiscovery and Information Governance practice group with any questions related to this newsletter.

---

[1] No. CV-03-467-ST, 2004 WL 2066746 (D. Or. Sept. 15, 2004).
[2] *Id.* at *3.
[3] *Id.* at *21.
[4] 130 S. Ct. 2619 (2010).
[5] *Id*. at 2629.
[6] *Id*. at 2632-33.
[7] *Id*. at 2633.
[8] *Id*.
[9] Some states, including Delaware and Connecticut, have specific requirements for monitoring employee email and internet access, and may impose penalties for violations. *See* DEL. CODE. ANN. tit. 19, § 705 (2010); CONN. GEN. STAT. ANN. § 31-48d (West 2011).

SEYFARTH ATTORNEYS SHAW LLP

Breadth. Depth. **Results.**

www.seyfarth.com