

Privacy Vs. Technology In The Workplace

By David E. Canfield and Jason Paroff

28 July 2010

Forbes.com

Last month the [U.S. Supreme Court](#) issued a highly anticipated opinion, *City of Ontario, California v. Quon*, which sheds some light on an often overlooked, yet important, issue in many corporations today: technology and network use policies.

The case highlights the importance of using these policies to address a company's right to access information created and sent using work-issued technology in connection with an employee's expectation of privacy in the workplace. Taking into account this important decision, companies must create, implement and enforce these policies, ensuring employees are aware that their actions may be monitored.

Policy Creation

Experience has shown that typically a company's technology and network use policy--if one exists at all--is written by in-house or outside counsel who may not possess the intimate knowledge of the company's computer and network systems. As a result, sometimes these policies are too broad, discuss non-existent technology and can lead to confusion among employees and those whose job it is to enforce the policy. These generalized policies also further complicate the difficult task of responding to requests pertaining to litigation, investigations and regulatory compliance.

If counsel alone is not the best resource for policy development, who is? The CIO should be as involved from the beginning of the creation process as possible. Oftentimes, however, the CIO is more removed from the particulars of the computer systems, applications and technology than staff members such as system administrators might be. Thus, one solution is to form an internal working group, with input from legal, that includes IT managers and employees. This will allow the CIO to describe what is being monitored and why, which is extremely important in the development of effective use policies.

Implementation And Training

Simply creating a policy is not enough. There must also be employee training. The training can be online, in-person, through seminars, etc. Training should be conducted on an annual basis and/or when the policy is updated and must be documented thoroughly. If a court dispute over a policy ever does develop, taking these steps will demonstrate to the court that the company underwent significant efforts to ensure compliance with the policy.

The importance of clearly conveying the policy and training is highlighted by the [Supreme Court](#) in *Quon*. In this case, the City of Ontario created and implemented a "Computer Usage, Internet and E-Mail Policy." The City communicated this policy to all employees and had them sign a statement acknowledging they received and read the policy. However, this policy did not reference text messages directly, which was the communication at issue in the case. Regardless, the Supreme Court found the City clearly conveyed through an all-staff meeting that e-mail and text messages would receive similar treatment. The comments made at this meeting were also recorded in a memorandum and circulated to all employees. These documented steps helped overcome the employee's argument that text messages were not part of the policy and could not be monitored.

Follow The Policy And Keep It Updated

Once a policy is in place and employees are properly trained, companies must actually follow the policy. Companies must also acknowledge that the modern digital world is in constant flux, rendering the technology and network use policy sufficient for only a short period of time. The policy must be continually updated to reflect changes in company technology, equipment and evolutions in the outside digital world.

For example, an appropriate policy should now address such items as social media (e.g., Facebook, MySpace, Twitter, etc.) and [text messaging](#), which play an ever increasing role in the life of most

employees--both in and out of the workplace. The City of Ontario may have had an even stronger case if it updated its policy to reflect its adoption of pager and text messaging technology.

Testing the policy to ensure it continues to meet the needs of the company and accurately reflects what is happening in the company's technology environment is also important in terms of making routine updates. If the policy does not achieve the proper objectives, the policy was not constructed or explained well. Either way, action should be taken to update and modify the policy as needed to ensure its accuracy and scope.

Without a policy in place to address employee technology and network use, companies are exposing themselves to unnecessary risk. Experience has shown that many companies forego taking action on security-related items such as technology and network use policies, choosing instead to wait until something goes wrong. This invites disaster. It is far more difficult, time-consuming and expensive to implement corrective policies and engage in costly and sometimes embarrassing litigation, than it would have been had the company acted proactively.

David E. Canfield is a managing consultant in Kroll Ontrack's electronically stored information consulting group. He can be reached at dcanfield@krollontrack.com.

Jason Paroff is the senior director of computer forensics operations at Kroll Ontrack. He can be reached at jparoff@krollontrack.com.