Privacy at Work

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University

Recently I received an invitation to sign a petition:

> *Think the federal government threatens your privacy? It could be worse -- you could work for them.*
>
> *Federal agencies are increasingly monitoring their own employees using software that tracks keystrokes, takes screenshots, and even records Facebook and Twitter activity! This threatens employees' abilities to express political opinions and to work freely without fear of censure.*
>
> *These constitutional abuses came to light when scientists at the FDA, blowing the whistle on unethical drug review practices, found they were being spied on and intimidated. Now it's clear that other government agencies, including the TSA, extensively monitor their employees, down to their personal emails!*
>
> *How can we expect to live in a free, private society if even federal employees are systematically monitored? Join us in demanding [an] end to federal employee spying.*
>
> *PETITION TO THE FDA AND TSA: We all deserve the right to privacy, as is guaranteed in the Constitution. We demand that federal agencies adopt constitutional privacy practices and disclose to their employees the extent of monitoring.*

I was surprised at the naiveté of this petition.

In my classes on cyberlaw and information assurance management, we discuss the absolute right of employers to monitor, control or restrict the use of the employers' resources by employees. In the United States, the First Amendment of the Constitution is often misunderstood to grant absolute freedom of speech; however, it does not. There are several categories of speech that have been excluded from First-Amendment protection (e.g., sedition, incitement to violence, defamation, and obscenity) but in any case, that constitutional provision applies to governmental restriction of speech in the public sphere. There are many instances where employers – or even customers negotiating contracts with consultants – are perfectly justified in demanding restrictions on speech related to the work being conducted.

Any employer in the USA may define explicit regulations or policies affecting what employees may do with employer-owned communications resources. Typical privacy agreements explicitly state that employees agree to have any communications carried out using employer facilities (telephones, computers, faxes) potentially be monitored or restricted. Non-disclosure agreements provide frameworks to restrict revelation of proprietary or otherwise confidential aspects of an organisation's work. Security levels restrict communications among employees who have different degrees of access; access-control lists and other authorization schemes limit who may access which views of corporate data. Although there are restrictions on monitoring personal

conversations on corporate telephones, it is also possible and legally acceptable to promulgate regulations barring such calls or explicitly letting employees know that all communications using employer-owned equipment may or will be monitored.

An essential component of legality for all such restrictions is that there be no possibility of an expectation of privacy when using corporate resources. Even company cars may be searched legally as long as the policies are clear (privately owned cars may not be searched by employers). The yearly signature of a privacy policy by all employees is one way of ensuring that no one has an unfounded expectation of privacy in the workplace when using corporate tools; on computer systems, a good policy is to post the privacy (or lack-of-privacy) provisions for e-mail, Internet use, instant messaging, and application usage on the login screens for session and even on the start-up screens of applications.

On the other hand, if an employee makes a personal call on a personally owned mobile phone or personally owned computer that is not using corporate networks, normally those calls would be private according to the privacy policies of the organization. Note, however, that any use of the corporate Internet networks would instantly demolish any reasonable expectation of privacy if the policies made that clear.

For a summary of US rulings about privacy at work, see the article "Privacy at Work: What Are Your Rights?"< http://employment.findlaw.com/workplace-privacy/privacy-at-work-what-are-your-rights.html >. For a review of the European situation, see "European Court of Human Rights Expands Privacy Protections: Copland v. United Kingdom"< http://www.asil.org/insights070806.cfm > and "Personal Privacy in the Workplace: An EU Perspective"< http://mcguirewoods.com/Client-Resources/Alerts/2009/5/Personal-Privacy-in-the-Workplace-An-EU-Perspective.aspx >.

Please note that I am not an attorney and that the comments above are not legal advice. For legal advice, consult an attorney qualified in the appropriate area of the law and licensed to practice in your jurisdiction.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *