Emerging Issues in Employee Monitoring

Brian Tretick
Ernst & Young

The following remarks were made to the forum of the 26th Annual International Conference on Privacy and Personal Data Protection, held on 14 to 16 September 2004, in Wroclaw, Poland. They were in the context of a panel on the balance between employer and employee rights and obligations in employee privacy, and were made by Brian Tretick from Ernst & Young's global privacy practice (see www.ey.com/privacy).

Employers are presented with an increasing array of employee communication channels that may be monitored for enforce corporate policies such as for:

- Workplace safety
- Acceptable use of corporate resources
- Workplaces free from harassment and hostile attitudes
- And productivity and performance measures.

We have heard that there is a history of monitoring the use of these communication channels, such legacy methods as:

- Telephone
- Email
- And Internet browsing.

However, new techniques encroaching on the workplace offer new challenges. They may have been provided by the employer as part of the corporate infrastructure, or they may have been brought in by the employees for personal use by an increasingly connected workforce. These technologies include the use of the following:

- Internet-enabled tools (in addition to browsers) such as an instant messaging applications that I am going to focus on. These also include media players and peer-to-peer (or P2P) software.
- Increasingly smart mobile telephones
- Blackberries, Treos, and other handheld computers that connect to the corporate infrastructure
- And interactive email, not just text, but with built-in scripting, forms, and other active content.

In general, it is the presence of these dual-use technologies, used for personal purposes and used for business purposes, which pose the most significant

challenges for employers: namely, monitoring the appropriate use of corporate resources and employee conduct without overstepping into personal affairs.

Instant messaging grew from personal use and has, for the last several years, begun to permeate the workplace. Initially, employees used instant messaging to keep connected with family and friends, then evolved to communicate with coworkers, customers, and other business associates. Companies have allowed the use of commercial instant messaging, like AOL, Yahoo, and MSN, and have even set up enterprise systems.

Instant messaging conversations may be personal, casual, and with little relation to work, or they could be communication about business transactions. Even a person's "Buddy List" –the others with whom the user is set up to chat–can be quite personal.

The challenge is faced when these communications are allowed over the corporate networks.

- Do you monitor them, or not?
- Under what conditions?
- And with what protections?

The Enron investigations discovered and ultimately made public millions of email messages—most were business, but others were about happy hours, vacations, and bowling scores.

Consider the more informal nature of the IM and it is clear that monitoring that form of communications would net traffic of a personal nature.

Other Internet-enabled applications that have invaded the workplace–such as media players, browser plug-ins and toolbars, interactive email and even peer-to-peer software–raise similar challenges. These connect to the web, and they often have built-in browsers, too. They flow through the same firewalls, proxy servers, and routers, and can leave their own trails in the network audit logs.

Employers should re-examine their workplace monitoring policies and practices in light of these techniques. Internet and email acceptable use policies written 10 years ago, at the dawn of Internet use, no longer cover all of the bases.

Employers should consider the following:

- Weigh the value and risk of monitoring these techniques
- Consider applying solutions that prevent inappropriate use, rather than monitoring all use
- Inform employees of the full scope of Internet monitoring taking place

- Update acceptable use policies to address these and emerging techniques
- Check your systems. Are they collecting as you describe? Do you have other unintended logs or records?
- If you offer enterprise solutions, such as instant messaging, yet still allow non-corporate tools, make it clear which channels are monitored
- Retain appropriate information for an appropriate timeframe, and protect those records from review, except under authorized conditions, such as an official investigation
- Consider how you will address the issue of data subject access on these records, and whether your systems and processes are adequate. Also, remember that there are 2 data subjects in an IM conversation, and the other parties may not be your employees.

I would like to conclude with this summary:

- New techniques, especially these dual-use communications techniques, pose increasing challenges to monitoring acceptable use of the Internet
- Employers are faced with the challenge of ensuring appropriate workplace behavior, while not excessively intruding into private lives
- Existing acceptable use and workplace monitoring policies are often outdated as to practices and may not sufficiently instruct employees, and even the IT staff who run the corporate Internet resources, on what will and will not be monitored.

Data Protection Officers should reassess their Internet monitoring practices and keep these policies current. And Data Protection Authorities should also consider guidance on this matter that extends to these new techniques.

I appreciate the opportunity to discuss this with you.
Thank you.