The right corporate policy: E-mail and Internet monitoring

by [John Kador](http://search.techrepublic.com.com/search/John%20Kador.html) | May 12, 2000 7:00:00 AM

**Tags:** [John Kador](http://search.techrepublic.com.com/search/John%20Kador.html)

**Takeaway:** If you've decided to monitor company Internet and e-mail use, what are the legal challenges you'll face? Why do such practices appeal to businesses? What are some of the software tools available? Read on to find out more about Internet content management.

Few employees are aware that everything they do on the network leaves fingerprints. Internet content management tools now enable security administrators to monitor not only every Web site browsed by every employee, but every e-mail message that they send or receive.  
  
With a few clicks, the administrator can open a window and see the senders, recipients, and subject headings of each message, as well as the URL of every Web site browsed and the duration of the visit.  
  
Using such software, Andrew Quinn, a systems manager at Ritvik Toys, has learned more about his fellow employees than he ever wanted to know. He found that one co-worker has a penchant for herbal remedies, another likes jokes about women drivers, and another checks the lottery numbers each morning.  
  
Managers give a variety of reasons for installing such software. Most are trying to prevent gross abuse by workers who gamble online, browse pornography, or run private businesses on company time.  
  
Some want to prevent loss of intellectual property, while a few are concerned about employees sending harassing messages. Others are on the lookout for oversized e-mail attachments that clog networks. Still others seek to dissuade employees from using their systems for personal activities.  
  
Whatever your reason, once you’re onboard the monitoring ship, you need to know the right steps to take in order to keep your employees happy and your business intact.  
In [“Internet content management: A necessary evil,”](http://www.techrepublic.com/article.jhtml?id=r00520000502kad01.htm) our first article on Internet and e-mail monitoring, we examined some of the reasons businesses give for such practices. In this article, we discuss acceptable Internet usage policies, potential legal challenges to Internet and e-mail monitoring, and some of the software tools businesses use.

**Protecting your business**  
The first step in protecting yourself is distributing an acceptable Internet usage policy (AUP).  
  
Most companies believe that a certain level of recreational Web use is acceptable. Within that definition, however, most AUPs exclude sites that offer pornography, gambling, and a few other carefully selected content areas. A sound policy clearly states that libelous, sexually explicit, or defamatory material may not be displayed or distributed at work.  
  
It also makes employees responsible for protecting copyright, software licenses, and intellectual property. Finally, it makes explicit how the policy is enforced—via monitoring software, for example—and outlines the steps that will be taken if the policy is violated. For most cases, the existence of a policy alone will deter the recurrence of breaches of security.  
  
The ethos of monitoring does not sit well with many IT managers, who are trained to provide service, not deny its use. Others say that, like telephone use at work, some non-work-related Web activities might just have to be tolerated.  
  
It’s perhaps too much to expect that every employee is always 100 percent aligned with the work experience. The issue is how much tolerance is reasonable.  
  
A good example of a company that is navigating this high-wire dance is [Kinko's](http://www.kinkos.com/), which rents out computers at its 900 copy centers in the United States. Kinko's uses [SurfWatch](http://www.surfwatch.com/products/swwork.html) software on the computers it makes available to the public, but it doesn’t use the monitoring software internally.  
  
Kinko's is not concerned with productivity, bandwidth, or liability with its own employees, says Brian Gerk, technical development manager at the company's Ventura, CA.-based headquarters.  
  
"I'm more concerned with what our customers see and what they're exposed to," he said. The company's standard human resources policy includes computer usage and the section regarding appropriate behavior in the workplace applies to computers as well.  
Every organization has its own protocols, but most organizations are interested in tripping an alarm when the monitoring software detects the following situations:

1. Messages with .exe attachments, which might contain a virus.
2. Any attachments such as animated movies larger than a couple of megabytes, which can clog the network.
3. Subject lines with the designation Fwd or Re appearing several times in one message, which are likely to indicate forwarded jokes and back-and-forth chats.
4. Scores of messages sent in one day by a single employee to people outside the office, which can overload the system and suggest the sender is not attending to the company’s interests.
5. Headlines with phrases like “Job Hunt” or “Resume Enclosed,” which might reveal an employee looking for another job.
6. Words such as “confidential” or “proprietary,” which suggest the loss of intellectual property.
7. Racial slurs or words such as “sex” and “babe,” since ethnic comments and off-color jokes can establish a hostile work environment and lead to lawsuits.

**Legal challenges**  
From time to time, employees challenge the rights of companies to monitor workers’ e-mail, but the challenges don’t get very far. The more companies disclose what they are doing, the easier the monitoring pill goes down.  
  
Undisclosed observation seems to upset workers the most, according to the [American Civil Liberties Union's](http://www.aclu.org/) Workplace Rights Project.  
  
“Workers get extremely upset when they find out they are being spied on," said Jeremy Gruber, Legal Director of the ACLU's Workplace Rights Project.  
  
“There are a couple of downsides to monitoring in the workplace," agrees Beth Givens, Director of the [Privacy Rights Clearinghouse Project](http://www.privacyrights.org/) in San Diego. “If monitoring is done secretly, without there being a written privacy policy, the employer faces the risk of privacy-related lawsuits. Even though the vast majority of such lawsuits have been decided on the side of the employer, lawsuits cost employers a lot of money and time.”  
  
If a company decides to take action based on monitoring, it’s better if there is probable cause. “If the monitoring is random or ongoing, rather than based upon 'individualized suspicion,' the employer risks creating the perception that they do not trust their employees. That could result in a morale problem,” says Givens.  
Has monitoring become a necessity or are businesses that use these types of tools invading a worker’s privacy? Does your business use monitoring software? Has your company decided not to? Post a comment below or send us an [e-mail](mailto:cio@techrepublic.com?subject=Monitoring).  
**Monitoring tools**  
Here are a few companies that provide monitoring software:  
  
[Aspeon Software Inc.](http://www.aspeonsoftware.com/)  
*Exchange Plus*  
  
[Content Technologies Inc.](http://www.mimesweeper.com/)   
*MailSweeper*  
  
[Elron Software Inc.](http://www.elronsoftware.com/)   
*Elron CommandView Message Inspector*  
  
[Marshal Software](http://www.marshalsoftware.com/)   
*MailMarshal*  
  
[SRA International Inc.](http://www.sra.com/)   
*Assentor*  
  
[SurfWatch Software](http://www.surfwatch.com/products/swwork.html)   
*SurfWatch*  
  
[Symantec Corp.](http://www.symantec.com/)   
*MailGear*  
  
[Trend Micro Inc.](http://www.antivirus.com/)  
*ScanMail*  
  
[Tumbleweed Communications Corp.](http://www.tumbleweed.com/)  
*WorldSecure Mail*

John Kador is an independent business writer in Geneva, IL.