

You've Got Mail . . . And the Boss Knows:

A Survey by the Center for Business Ethics of Companies' Email and Internet Monitoring

W. MICHAEL HOFFMAN, LAURA P. HARTMAN, AND MARK ROWE

The use of email, the Internet, and corporate databases by individuals and companies is increasing exponentially, and has probably affected business more profoundly during the last few years than any other single phenomenon.¹ More than 50 million Americans connect to the Internet and use email at work. A U.S. Department of Commerce survey,² published in February 2002, shows that the proportion of employed persons aged 25 and over who use the Internet and/or email at work increased in just one year from 26.1 percent in August 2000 to 41.7 percent in September 2001. Whether they realize it or not, more and more of these employees are liable to have their Internet and email activities monitored by their employers. The Center for Business Ethics (CBE) at Bentley College, Waltham, MA, has conducted a survey of

Michael Hoffman is executive director of the Center for Business Ethics at Bentley College, Waltham, MA. Laura P. Hartman is Associate Vice President, Academic Affairs and Professor of Business Ethics at DePaul University, and a research fellow at the Center for Business Ethics. Mark Rowe is the senior research associate at the Center for Business Ethics.

The authors wish to pay grateful tribute to the valuable research and interviewing assistance provided by Yasam Tandogdu and Larissa Wilner, both graduate assistants at the Center for Business Ethics.

The Center for Business Ethics is also grateful for the support of the Ethics Officer Association and would like to thank its Sponsoring Partner corporations (and their interviewed representatives) for making this survey possible.

corporations that are Sponsoring Partners of the Ethics Officer Association (EOA). The survey was designed to discover the extent to which companies monitor their employees' use of the Internet and email, their reasons for doing so, and the means by which they go about it.

We have found that monitoring is commonplace, with nine out of every ten companies checking up on their employees' online activities while at work. Given the sensitive and somewhat controversial nature of the practice, it was surprising to discover how many companies monitor all the time, not just when something gives cause for concern. For the same reason, we were surprised at the nature of ethics officer involvement in the process. The majority of companies that responded to our survey seem to aspire to a system of responsible, sensitive, and appropriate monitoring. Nevertheless, we believe the survey has highlighted some issues that companies might want to revisit in the quest for best practices in this area.

BACKGROUND

Does New Technology Mean New Value Judgments? Employers have always gathered information about their employees. For instance, in the early 1900s Milton Hershey, of Hershey's Chocolate, used to tour Hershey, Pennsylvania, to see how well his employees maintained their homes. He hired detectives to spy on Hershey Park dwellers in order to learn who threw trash on its lawns. Henry Ford used to condition wages on his employees' good behavior *outside* the factory, maintaining a Sociological Department of 150 inspectors to keep tabs on them.

As the business world has become increasingly complex, and American society ever more litigious, employers have tended to regard employees as one of many potential sources of risk—at least, those employees whose conduct departs from the norm. This trend was intensified by the introduction, in 1991, of the Federal Sentencing Guidelines for Organizations (FSGOs).³ Imposing a mandatory system of heavy fines and rigorous probation conditions for organizations convicted of federal offences, the FSGOs caused employers to scrutinize employee activity closer than ever before.

Advances in technology have been dramatic, and have facilitated information gathering in ways that Hershey and Ford could never have imagined possible. From an ethical perspective, this does not mean that technology has created new value judgments; simply new ways to gather the information on which to base them. The manner in which employers collect information about employees may have changed far more than the values underlying the decision to do so, but there are some challenging issues that now confront us. In conducting our survey, we had in mind a number of issues, including the following:

- Managing employee and employer expectations.
- Distinguishing between work use and personal use of technology.
- Managing and measuring employee productivity and performance.
- Optimizing work/life balance.
- Balancing privacy interests.
- Managing risk and liability issues.
- Maintaining a virtual workplace.
- Responding to accessibility issues related to the “digital divide.”
- Protecting proprietary information.
- Operating flex-time.

In this article, we examine corporate monitoring of employees’ email and Internet usage in the context of some of these issues.

How Does Monitoring Work? Technological advances in information gathering have allowed monitoring that was never before possible. Worldwide sales of monitoring technology are estimated at \$140 million annually.⁴ One example of new technology is Raytheon’s *SilentRunner*, which allows firms to track everything that occurs on a network, including not only emails but also instant messaging—one of the new ways in which employees thought they had foiled email monitoring.⁵

The most prevalent Internet monitoring product in the United States is *Websense*, with 8.25 million users worldwide. While *Websense* merely *blocks* certain websites, *Websense Reporter*, an add-on, records all web accesses (not only attempted accesses blocked by *Websense*, but also all non-prohibited web surfing). Seventy percent of *Websense* customers install *Reporter*. *MIMESweeper*

is the most used email monitoring system in the United States with 6,000 corporate customers and over 6 million ultimate users worldwide. In a less publicized form of monitoring, SWS Security offers a product that allows managers to track the messages a worker receives on a portable paging device so that one could track whether the employee is being distracted by outside messages.

Why Monitor Email and Internet Usage? There are numerous arguments that support the choice of a firm to monitor. Since the current research surveyed members of the Ethics Officer Association, we sought to determine attitudes and practices related to monitoring at those firms in particular that may be more acutely aware of the ethical challenges to monitoring. Recent research has found that monitoring serves a number of purposes for a firm. Consider the following:

- a) Managing the workplace.
 - Ensuring compliance with affirmative action.
 - Administering workplace benefits.
 - Placing workers in appropriate positions.
- b) Ensuring effective, productive performance.
 - Preventing loss of productivity to inappropriate technology use. Calculations have been made as to the cost of productivity lost as a result of employees spending work time on the Internet for non-business reasons. One study calculates that if 50 users spend 3 hours per week on recreational surfing during work hours, the cost to the organization is \$3,322.50 per week in lost salary expenses; this is \$172,770 per year.⁶
 - 13 percent of employees spend over two hours a day surfing non-business sites.⁷
 - A recent survey in the U.K. reports that, of the workers surveyed:
 - 53 percent behave “immorally” in email.
 - 38 percent have used email in the pursuit of political gain within their company, at the expense of others.
 - 30 percent admit to having sent racist, pornographic, sexist, or otherwise discriminatory emails while at work.⁸
- c) Protecting information and guarding against theft.
- d) Protecting investment in equipment and bandwidth.

- e) Protecting against legal liability, including possible
 - perceptions of hostile environments;
 - violations of software licensing laws;
 - violations regarding proprietary information or trade secrets;
 - inappropriate gathering of competitive intelligence;
 - financial fraud;
 - theft;
 - defamation/libel;
 - discrimination.
- f) Maintaining corporate records (including email, voicemail, etc.).
- g) Investigating *some* personal areas—consider Infoseek executive Patrick Naughton’s pursuit of a tryst with an FBI agent posing as a 13-year-old girl in a chat room.

These purposes do not appear unreasonable. Nevertheless, there may be a number of reasons to limit monitoring and we will explore these arguments below.

How Far Should Monitoring Go?

Notwithstanding a number of persuasive justifications for monitoring in the workplace, there remain several reasons to limit monitoring. Below, we set out a number of them.

- Monitoring may create a suspicious and hostile workplace.
- Monitoring constrains effective performance (employees claim that lack of privacy may prevent “flow”).
- It may be important to conduct *some* personal business at the office, when necessary.
- Monitoring causes increased workplace stress and pressure, negatively affecting individual and, by extension, company performance.
- Employees claim that monitoring is inherently an invasion of privacy.
- Monitoring does not always allow for workers to review and correct misinformation in collected data.
- Monitoring constrains the right to autonomy and freedom of expression.
- Monitoring intrudes upon one’s right to privacy of thought (*“I use a company pen; does that mean the firm has a right to read my letter to my spouse?”*)

There is some force in these arguments, yet some counter-arguments might also be made.

For instance, it is arguable that monitoring is less likely to be a cause than a symptom of a suspicious and hostile work environment. We have anecdotal evidence of monitoring that is carried out without breeding suspicion and hostility. If the management of a company is respectful of the employees, manages their expectations realistically, and is frank about the company's objectives, it is more likely to cultivate an atmosphere of trust and transparency. Then, the employees are more likely to view the monitoring process as serving a business need than as a sinister intrusion. A 2001 survey found that 75 percent of employees thought it was acceptable for companies to implement email and Internet monitoring if the employees were notified in advance.⁹

Secondly, it is clear from our interviews that many companies recognize that changing work patterns and lifestyles make it not only appropriate but also necessary for some personal affairs to be dealt with from the workplace. It is incumbent upon employers to let employees know that this is acknowledged, at the same time giving the best indication of what is, and is not, acceptable.

In the American Management Association's 2001 survey, more than two-thirds reported that they engaged in monitoring as a result of their concerns for legal liability. Given the courts' focus in many cases on employer response to claims of sexual harassment or unethical behavior, among other complaints, firms believe that they need a way to uncover these inappropriate activities. More than 10 percent of firms have reported receiving a subpoena for employee email and one-third of the largest firms report firing employees for inappropriate email.¹⁰ Without monitoring, how would they know what occurs? Moreover, as courts maintain in many cases the standard of whether the employer "knew or should have known" of wrongdoing, the state of the art definition of "should have known" becomes all the more vital. If most firms use monitoring technology to uncover this wrongdoing, the definition of "*should have known*" will begin to include an expectation of monitoring.

Survey Methodology

The survey was conducted over the spring and summer of 2002. It was designed in two parts. The first part sought quantitative data

and involved a questionnaire with 18 questions submitted to 192 corporations that are EOA sponsoring partners. The second part of the survey was qualitative in nature and necessitated telephone interviews with a sample of corporate ethics officers and senior managers.

The first four questions in the questionnaire were concerned with the existence and communication of any policies that companies might have adopted in relation to the monitoring of email and Internet usage. Questions 5–7 were designed to investigate the degree of permissibility of personal usage by employees of companies' electronic systems. The final 11 questions dealt with the motives and methods of corporate monitoring, and the responsibilities and safeguards attaching to such activity. In answering some questions, respondents were invited to indicate more than one category (if appropriate) and this should be borne in mind when viewing some of the figures. The survey was emailed to the chief ethics officer of each sponsoring partner company in spring 2002. Respondents were given the option of completing and returning the questionnaire electronically or, alternatively, printing out and mailing back a hard copy. The response rate was 54 percent, with all data received back by July 2002.

Ten interviewees were selected for follow-up questions in order to provide data of a more qualitative nature. Selections were made on the basis of interviewees' reputations and experience, and in such a way that a variety of industries were represented. In July 2002 we spoke to ethics officers and senior managers employed in the following sectors: accounting; aviation; defense; energy; insurance; paper; and telecommunications. Interviewees were asked seven pro forma questions to elicit detailed comments on specific areas of particular interest or concern.

SURVEY FINDINGS

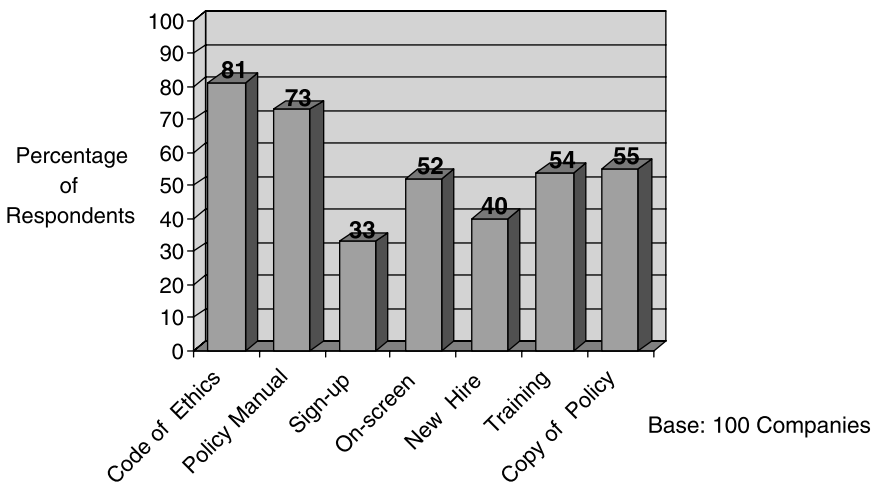
Monitoring Policy

Unsurprisingly, all of the 103 companies responding to the survey provide their employees with access to email, the Internet, or other communication technology. Monitoring employees' usage of such technology is widespread, with 92 percent of companies that

responded to the survey confirming that they do monitor use of email, Internet, and other technology.* All of the firms surveyed who engage in monitoring maintain a policy in this regard. Only one company responding to the survey does not tell employees that their use of email, the Internet, or other technology is subject to scrutiny.

Companies use various communications tools, often in combination, to notify employees of the monitoring policy. Incorporating a clause in the company's code of ethics/business conduct is the route most frequently taken, although almost as many companies publish a separate manual containing details of the policy. Other methods adopted by respondents include notifying employees of the monitoring policy while they are actually using the technology—for example, by means of “pop-ups” that appear on the screen—or in the course of orientation or ongoing training programs. Figure 1 shows the prevalence among survey respondents of various means of communicating the company policy on monitoring. The question

FIGURE 1 Notification of Monitoring Policy to Employees



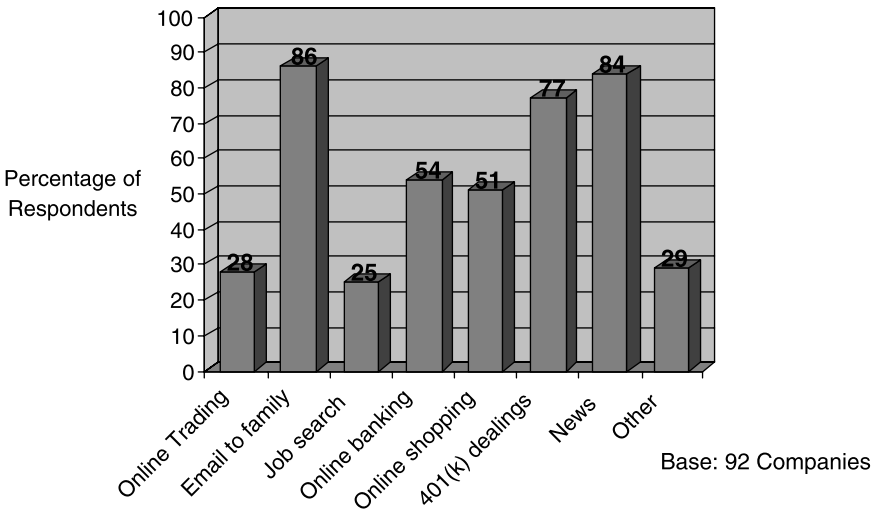
* It is possible that the percentage of companies that engage in monitoring is even higher than 92 percent. In their responses to our question on frequency of monitoring (see following section “How Often Do Companies Monitor?”), only 2 out of 102 companies said they “never monitor.” This may be a discrepancy explained by a few inconsistent answers but we felt it worthy of mention.

asked was, "How does your company communicate the email, Internet monitoring or technology usage policy to employees? (Check all that apply)."

Should Email and the Internet Be Treated Differently? The survey explored whether companies draw a distinction between monitoring employee email and monitoring Internet usage. The majority of those company executives whom we interviewed made no such distinction. One vice president explained his company's rationale: "We tell employees up front that our systems and our hardware are proprietary. There's no expectation of privacy and, depending on the situation, we will monitor activity and take action." Although seeing no ethical distinction in principle between monitoring email and Internet usage, one manager told us that her firm was sensitive to the fact that employees have less control over what types of electronic mail they receive than over the websites they access. She did see an ethical issue if "reading" email content is included in the monitoring of emails, saying, "Our corporate policy on access to this information is rather strict and requires a real business need to obtain such information [the content of emails]."

Some companies do, however, see a difference in principle between monitoring employee email and monitoring their use of the Internet. The director of legal compliance and business ethics at one corporation observed, "The monitoring of employee email has a greater propensity to surface employee concerns regarding privacy. Email, like the telephone, is a tool that is used for both business and personal reasons. Unlike the Internet, email affords the user the ability to communicate with others on matters that are personal and private. The Internet is simply an information gathering tool." However, this approach appears not to take into account problems that might arise as a result of employees joining Internet chat rooms or engaging in instant messaging while at work.

"Reasonable" Personal Usage The same percentage of respondent companies that engages in monitoring (92 percent) also allows "reasonable" personal usage of their electronic systems. Of course, this begs the question as to what reasonable use is. Only 42 percent of responding companies define "reasonable personal usage" in their policies, which means a majority of companies offer employees no guidance. One company takes away the problem entirely, at least

FIGURE 2 What Is Considered “Reasonable Use”?

where email is concerned, since it stipulates to employees that email is to be used only for company business. Figure 2 shows a range of employee activities permitted by those companies that do attempt to define reasonable email and Internet usage. There is consensus in several areas, with similar percentages of respondents (around 80 percent) giving approval to email contact with family, keeping abreast of news, and dealing with 401(k) matters. Some companies do not even mind usage such as research and communications as part of a job search, although three-quarters of our respondents do not think that this is a reasonable use of company facilities.

However companies define reasonable usage of email and the Internet, many draw an analogy with personal telephone calls. “For email,” one manager commented, “usage would be comparable to personal telephone usage. That’s to say a quick call to a family member or friend, some personal business needs, a call to your insurance agency or telephone company.” Her company’s policy on Internet usage is similar, allowing “incidental and occasional” usage.

A recurring theme in responses to the survey was that an employee’s use of email and the Internet should never compromise his or her ability to do their job, nor conflict with any of their

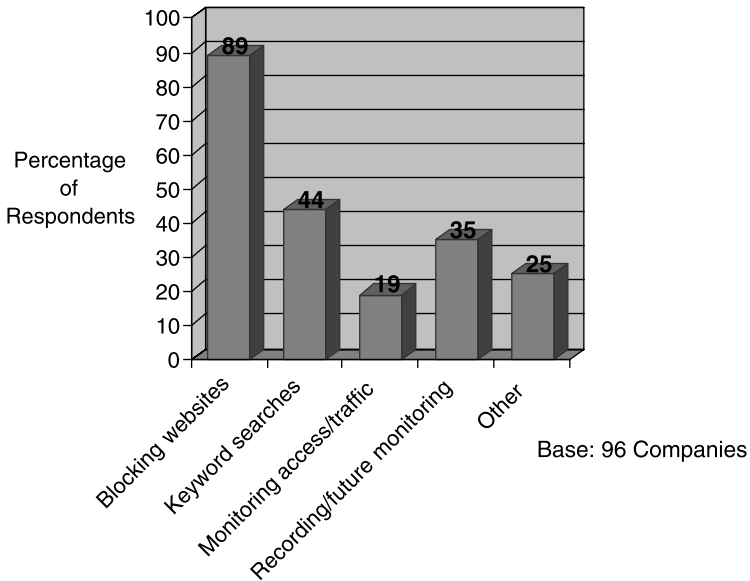
employer's business activities. The survey suggests, therefore, that the key criteria for determining reasonableness of personal use of email and the Internet are individual performance, productivity, and the safeguarding of company interests. In the section "Monitoring and Discipline" we will look at attitudes and practices in situations where performance or conflict issues do arise, and the employer considers it appropriate to take action.

Monitoring Methods

Monitoring in the workplace can take several forms and occurs for numerous reasons. Privacy scholar Colin Bennett identifies several types of surveillance that can specifically impact workers.¹¹ The first is surveillance by "glitch," where information is uncovered by mistake. In the workplace, a glitch could occur when a technician checks to see if a computer's hard drive has been erased by the previous users for use by someone else. That technician might notice inappropriate content on that hard drive. In another example of a glitch or mistake, an employee's salacious email could, through inattention to predictive text in the address box, be sent to an unintended recipient who reports the matter. These glitches may uncover violations of a usage policy even when no systematic monitoring is being conducted.

Bennett's second form of surveillance is "surveillance by default." This is where the default setting is to monitor, where all information that is sent through a system is caught and catalogued. In the context of this survey, surveillance by default occurs when all employees' email and Internet usage is monitored all of the time, whether there is a good reason or particular purpose or not. The American Management Association reports that 75 percent of firms surveyed in 2001 regularly record their employees' email transmissions as a default setting.¹²

A third form of monitoring is "surveillance by design," where the entire purpose of the technology is to collect information, and, generally, the user is aware of this purpose. One means of surveillance by design is when firms conduct either random or periodic keyword searches of email or other transmissions. One-quarter of firms surveyed by the American Management Association reported that they performed keyword searches, generally seeking sexual or scatological language to protect themselves from later liability.¹³ This

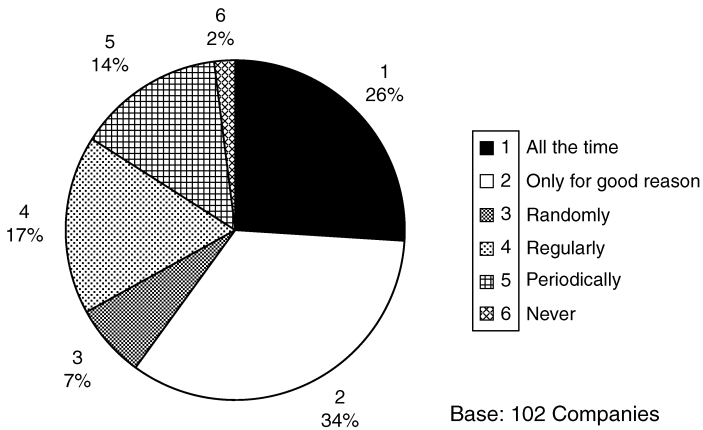
FIGURE 3 Which Methods Are Used?

illustrates the point made earlier about companies viewing employees, in one sense, as a risk element in their business.

Much of the monitoring that occurs today in American firms is surveillance by *design* or *default*. For instance, an email program that systematically sorts and saves all email that uses certain terms (such as those used in a job search or those terms that might be considered sexual harassment) would constitute surveillance by default. Some programs are designed to record email and Internet traffic for later monitoring as necessary. A monitoring program that tracks Internet accesses and blocks inappropriate websites would be surveillance by design. Figure 3 shows the relative usages of different monitoring techniques by 96 of the companies responding to our survey.

How Often Do Companies Monitor? In our interviews the overwhelming majority of executives said that monitoring was conducted in their companies in response to particular concerns or allegations that came to management's attention. However, this is not in line with the survey results. Instead, 64 percent of companies responding report that they either monitor all of the time

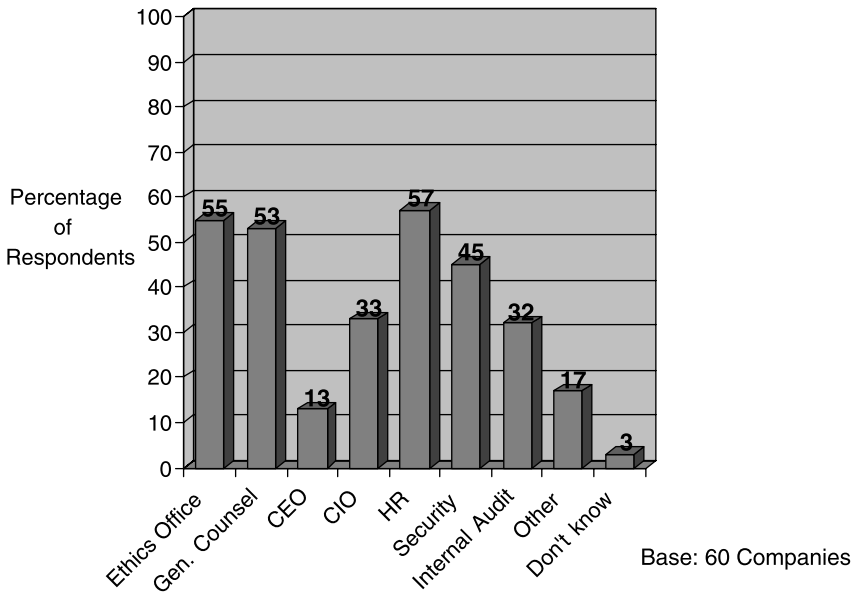
FIGURE 4 Frequency of Monitoring



(26 percent), or utilize “random,” “regular,” or “periodic” monitoring (38 percent). Thirty-four percent of companies monitor “only for good reason.” The latter figure is surprisingly low when compared to the interview responses. The breakdown is shown in Figure 4.

Monitoring for Due Cause If a company has adopted a policy of monitoring where it considers there is good reason to do so, how does it decide when and whom to monitor? According to the survey respondents, the decision might be taken by a variety of individuals or departments, but most commonly it is the ethics officer, the general counsel, or a senior member of the human resources department who will sanction the monitoring (see Figure 5).

As we have observed, monitoring is often undertaken to address a particular problem or complaint that has come to management’s attention. The treatment of email and the Internet may, however, be different. One company’s chief ethics officer describes a procedure that is fairly typical in relation to email monitoring: “Upon receipt of an allegation of misconduct, the receiving party (Legal Compliance and Business Ethics, management, HR, corporate security, etc.) evaluates the information provided, to determine if there is enough substance to warrant an investigation or monitoring. Once the decision is made to move forward, the employee is informed of the allegation and that their email account will be searched.”

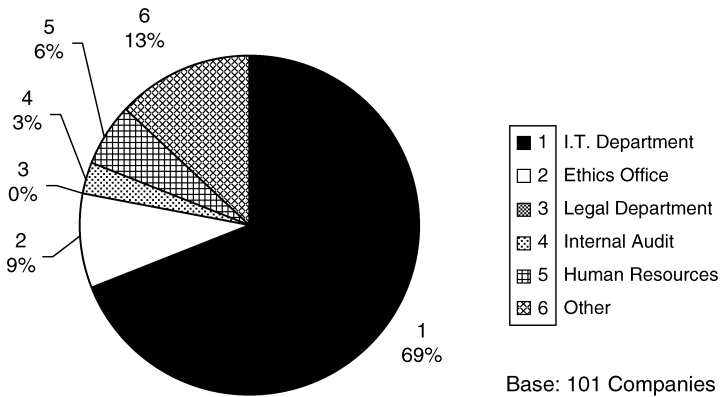
FIGURE 5 Who Determines There Is Good Reason for Monitoring?

The same executive says of Internet monitoring: “Employee use of the Internet is tracked regularly in terms of sites visited and the time a particular site was accessed. Additionally, by means of a firewall, sites deemed inappropriate by the company (e.g., sexually explicit content, games, gambling sites) are filtered and access is denied.”

Referring to his company’s practice of monitoring employees’ Internet usage on a random basis, a vice president of ethics and compliance explains, “We look at the top ten sites at a [company] location, and when we see something unusual popping up, or something that has a lot of usage but doesn’t have a clear business purpose, the people doing the monitoring would go in and take a look at it.”

Responsibility for Monitoring So who actually does the work of checking on their co-workers’ email and Internet usage? In the overwhelming majority of companies that responded to our survey, this is the responsibility of the IT department. Figure 6 demonstrates that respondent companies delegate this responsibility in different ways and, interestingly, the ethics office is responsible in only

FIGURE 6 Who Is Responsible for Monitoring?

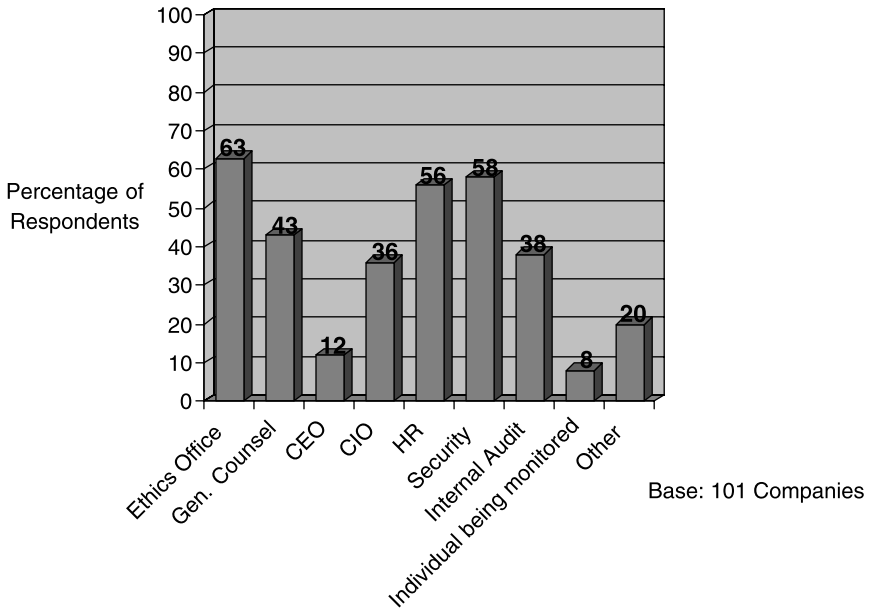


9 percent of cases. That is not to say that the ethics officers do not become involved in the monitoring process. In the following sections we explore the extent to which this happens.

Monitoring the Monitors: How Is the Process Overseen? We have already alluded to the fact that monitoring employees’ email and Internet usage necessarily involves an impingement on employees’ privacy, to a greater or lesser degree. Even if employees accept that monitoring is necessary, it is critical that the process is carried out in a responsible and professional manner, and that information about employees does not fall into the wrong hands. In addition to the privacy issue, the fact that monitoring can lead to disciplinary action, including dismissal, would lead one to expect universal acceptance of the need for oversight and guidance of the monitoring process to prevent abuses. To our surprise, this appears not to be the case, as 25 percent of companies surveyed do not have in place procedures to ensure that the monitoring process is not subject to abuse. Furthermore, only 57 percent of companies responding to the survey have written guidelines, policies, or procedures to direct the monitoring process.

Given the potentially sensitive nature of the information collected about employees, it is perhaps also surprising that only 36 percent of companies in the survey require the monitoring department or person to sign a confidentiality agreement.

FIGURE 7 Who Has Access to Information Collected Through Monitoring?



An essential requirement of any effective monitoring process is that relevant information needs to reach those people in the company who have a legitimate need to know it. As one might expect, different companies have different “need to know” criteria and they disseminate information gathered through monitoring to various individuals and corporate functions. It is perhaps not surprising that the largest consumers of such information are ethics officers, with 63 percent of companies allowing their ethics office access to the monitoring data. Security and human resources departments are not far behind, followed by legal departments (see Figure 7).

Ethics Office Involvement An organization’s greatest source of knowledge about the ethical implications of monitoring is usually its ethics office (if it has one), and one would therefore expect the ethics office to have significant involvement in the monitoring process. Our survey sought to discover the extent to which this is true in practice.

We asked each company whether the monitoring process and the information thereby collected are overseen, implemented, and reviewed by its ethics office. The results were surprising. Only 43 out of 98 companies responding to this question (44 percent) involved their ethics offices in this way. We sought to clarify the situation in our interviews. When asked whether his company's ethics officer was involved in overseeing the monitoring of employee email and Internet usage, one corporate director of ethics and compliance was quite categorical, responding, "Frankly, no. It's more of an IT or Security responsibility." When asked whether he thought his office *should* be involved, he said, "I get involved where there are complaints that come to our ethics [help] line." Two other interviewees took a similar line, explaining that they became involved only if contacted directly with a complaint or allegation that warranted investigation. It appeared they did not otherwise see a role for the ethics office in the monitoring process.

At other companies, the degree of involvement of the ethics office appears to be greater. One director of ethics and compliance said, "I'm not part of the initial group that would be notified personally. That would be legal and HR. But those [ethics] incidents are reported in our working group, where Legal, HR and I meet on a monthly basis; I chair the group. In some cases, where an incident is reported through the helpline, of course I'm notified then."

While not getting involved in specific cases, a vice president to whom we spoke said that the ethics office at his company was involved in setting up the procedure for oversight of monitoring and determining the checkpoints along the way. He elaborated: "We were involved in setting up the procedures so that all the right people [are involved] before they go in specifically to open up an employee's file and look at all of their data and systems and email and Internet usage. There are several people who have to be involved: an attorney, someone from Human Resources, someone from the management team. And if they follow that protocol, then we're sure that we're treating people properly. And then . . . I oversee every disciplinary action."

Monitoring and Discipline The executives and managers interviewed were asked about their respective company's experience of email and Internet monitoring leading to disciplinary action against employees. The ten interviewees all knew of instances where this

had happened, with employees being subject to a range of sanctions, from verbal warning to termination, depending on the circumstances. In all cases, employees were left in no doubt that abuse of company email, Internet, and other technology was viewed very seriously.

In most cases we found that discipline is handled by the human resources department in conjunction with line management. In the majority of cases, ethics office involvement is in an advisory capacity only. None of our interviewees had figures for disciplinary action in relation to email and Internet abuses.

Is Monitoring Ethical?

Our survey asked companies whether they believe it is ethical for them to monitor, read, or review employee email and/or Internet usage. Unsurprisingly, none thought monitoring was unethical. Fifty-seven percent gave an unqualified “yes” while the remaining 43 percent were prepared to support monitoring “only for good reason.”

Changing Times, Changing Expectations

Several of the company representatives we interviewed had interesting observations on how changes in working practices and the work environment had affected their companies' approaches to the monitoring of employee email and Internet usage. One felt that “our previous policies, which did not contemplate reasonable personal use, and which were written at different times and in different styles, and not comprising a unified policy framework, really were not serving us well. . . . So this move [policy change] by us is a recognition that we want to create our policy in a manner that is aligned with the behavior that we are prepared to tolerate . . . and to make sure that some important values that we believe in are fully carried out with this policy.”

Commenting on his company's change of policy to allow certain personal usage of company email and the Internet, another executive explained that it formally recognized what was happening anyway, but also acknowledged that as working hours had increased it was only reasonable to allow employees to take care of certain personal affairs such as online banking and bill-paying.

One manager of a global corporation highlighted geographical limitations on their monitoring policy, explaining that, in Europe, European Union regulations prevented the corporation from filtering and monitoring email and Internet usage to the full extent permissible in the United States. This is evidence of the difference between European and American attitudes to employee monitoring of technology use.

Summary of Survey Findings

A general sense that email and Internet monitoring is extremely widespread in corporate America has been affirmed by the finding that it is carried out by 92 percent of the corporations responding to our survey. Only one of these companies does not notify its employees that their use of email, the Internet, and other electronic media may be monitored. We can envisage no ethical justification for such a policy. About 4 out of every 5 companies that do notify their employees of the possibility of monitoring commonly publicize the fact in their ethics code and/or other manuals. It surprises us that only half of our respondents consider this an issue to be covered in training sessions.

Although all of our respondent corporations had adopted some kind of monitoring policy, it is worth noting one commentator's observation that despite—or possibly because of—the rapid expansion in the use of email and the Internet, most companies have not addressed the associated legal issues in a formal policy statement.¹⁴ Note that, although we asked corporations about their adoption of monitoring policies, it was not our aim in this survey to examine the details of such policies.

Only one out of the ten executives we interviewed made an ethical distinction between monitoring employees' email usage and monitoring Internet usage. His distinction was based on his view that monitoring email is more likely to raise employee privacy concerns. We believe such concerns are legitimate and important, recognizing the controversial nature of the privacy issue and the case for limits on monitoring.

Almost all companies participating in the survey (92 percent) allow their employees reasonable personal usage of their electronic systems, yet fewer than half actually define what they consider reasonable. More than three-quarters of those companies that do

attempt such a definition have no difficulty with emails to family members, occasional visits to news websites, and attending to retirement plan issues. Other activities are also permissible at some firms, albeit at only half or less of the respondent firms. Our interview questions elicited a recurring analogy with personal telephone calls. As with use of the telephone, employers do not want work patterns, productivity, or performance to be disrupted; and where that starts to happen is the point at which most employers draw the line on personal usage. Another major consideration for employers, apart from misuse of company time, is the protection of corporate interests. By certain kinds of personal usage of email and the Internet, employees can put themselves into conflict with the legitimate interests of their employers. Our interviews revealed that employers' greatest concerns in this area pertain to minimizing corporate risk exposure.

Some might find it surprising, if not alarming, that two-thirds of companies in our survey that monitor employees' email and Internet usage do not characterize their monitoring activities as "only for good reason." This is not to suggest that they do not have legitimate concerns that they are addressing, but it does seem to imply that the majority of companies do not consider it necessary to have suspicions, allegations, or complaints before monitoring.

Perhaps the most surprising discoveries of our survey were in the area of monitoring oversight. In the face of what is evidently an emotive issue, having ramifications in such sensitive areas as privacy, discipline, fiduciary relationships, and career progression—and having the potential to affect livelihoods very significantly—one might expect that great care is being taken by employers to prevent abuses and errors. In very many corporations we are sure that this is the case. Nevertheless, attention should be paid to the following statistics:

- A quarter of the companies in our survey admitted that they do not have in place any procedures or safeguards to ensure that the monitoring process is not abused.
- Nearly half do not have written guidelines, policies, or procedures by way of monitoring guidance.
- Two-thirds of respondents do not require the monitoring department or person to sign a confidentiality agreement.

Another surprising revelation was that less than half (44 percent) of the companies we surveyed involved their ethics office as a

matter of course in the monitoring process, by way of oversight, implementation, or case review. When we sought clarification, we found that several ethics officers among our interviewees regarded their involvement as being restricted to cases in which an allegation or complaint is made to them directly. Other companies appear to retain ethics officers in more of a consultative or advisory capacity; for example, in helping an HR manager to determine appropriate disciplinary action. It seems rare, however, for companies to involve their ethics officer throughout the monitoring process.

Like many aspects of business practice, email and Internet monitoring appears to be evolving. There was recognition of this by a number of our interviewees who explained that their respective companies had reviewed their monitoring policies and revised them. Their concern was to ensure that the policies are aligned with altered perceptions and expectations concerning acceptable conduct by employees.

CONCLUSION

Perhaps the most effective means by which to achieve legitimate objectives of monitoring, while remaining sensitive to the valid concerns of employees, is to strive toward a balance that is respectful of both purposes. This balance would safeguard individual dignity and also hold individuals accountable for the satisfaction of their particular roles in the organization. Notwithstanding the impact on personal rights, as well as management objectives, the achievement of this balance is not without significant rewards for the organization as a whole. The Centre for Innovation in Management (CIM), in conjunction with the Schulich School of Business, has recently published the results of a research project examining the link between high trust stakeholder relationships and business value creation.¹⁵ Ann Svendsen, CIM executive director, concludes that “trust, a cooperative spirit and shared understanding between a company and its stakeholders create greater coherence of action, better knowledge sharing, lower transaction costs, lower turnover rates and organizational stability. In the bigger picture, social capital appears to minimize shareholder risk, promote innovation, enhance reputation and deepen brand loyalty.”

A monitoring program developed according to the mission and values of the organization (i.e., with integrity), then implemented in

a manner that remains accountable to the affected employees, approaches that balance. In line with other survey findings, critical program elements would include adequate notice of the intent to monitor, including the form of monitoring, its frequency, and the purpose of the monitoring. Additionally, in order to be respectful of the balance between personal and professional interests, the employer should offer a means by which the employee can control the monitoring in order to create personal boundaries. Finally, monitoring should be connected to some specific legitimate business purpose, which will help the organization to create the most effective and least impactful program possible.

The survey evidences the broad impact of monitoring technology on our workplace decisions and environment. However, it also presents some relatively distressing data surrounding the responsibility for the implementation of monitoring—25 percent are lacking in policies designed to prevent abuse and almost 50 percent fail to have in place relevant policies and procedures. Where advances in technology allow us the ability to explore new activities of any type, it is critical that we also explore the ethical implications of, and accountability for, “pushing the envelope.” Technological growth is only responsible where we also continue to maintain and develop our ethical awareness and we respect underlying organizational values. Therefore, when faced with innovative technology in the workplace, perhaps the response with the most integrity is the one that preserves appropriate traditional values while remaining open to exploring new ones.

NOTES

1. David Farrington, Foreword to *Employee Use of the Internet and E-Mail: A Model Corporate Policy*, ed. David M. Doubilet and Vincent I. Polley (American Bar Association, 2002).

2. U.S. Department of Commerce, Economics and Statistics Administration and National Telecommunications and Information Administration, “A Nation Online: How Americans Are Expanding Their Use of the Internet” (February 2002).

3. United States Sentencing Commission, *Guidelines Manual*, Chapter 8 (Washington, D.C., 1991).

4. Andrew Schulman, “One-third of U.S. Online Workforce under Internet/Email Surveillance,” *Workforce Surveillance Project* (Privacy

Foundation, July 9, 2001). http://www.privacyfoundation.org/workplace/business/biz_show.asp?id=70&ac.

5. Jeffrey Brenner, "Privacy at Work? Be Serious," *Wired Magazine*. <http://www.wired.com/news/business/0,1367,42029,00.html> (accessed 2/26/02).

6. Elron Software, "Guide to Internet Usage and Policy," p. 12 (2003). http://www.elronsoftware.com/pdf/IUP_Guide.pdf (accessed 5/20/03).

7. Alan Cohen, "Worker Watchers," *Fortune/CNET Technology Review* (summer 2001), 70, 76.

8. Institute for Global Ethics, "U.K. survey finds many workers are misusing email," *Newsline* 5(10) (3/11/02).

9. Elron Software, "The Year 2001 Corporate Web and Email Usage Study," p. 8. <http://www.elronsoftware.com/pdf/NFOReport.pdf> (accessed 5/21/03).

10. Dana Hawkins, "Lawsuits Spur Rise in Employee Monitoring," *U.S. News & World Reports*, August 13, 2001.

11. Colin Bennett, "Cookies, Web bugs, Webcams and Cue Cats: Patterns of Surveillance on the World Wide Web," *Ethics and Information Technology* 3 (2001), 197-210.

12. Hawkins, *Lawsuits Spur Rise*.

13. Ibid.

14. Farrington, "Foreword."

15. Ann C. Svendsen, Robert G. Boutilier, Robert M. Abbott, and David Wheeler, *Measuring the Business Value of Stakeholder Relationships*, Part 1 (Toronto: Canadian Institute of Chartered Accountants, 2001).

