

Monitoring Employee Internet Usage

John Gorman

Do employers know where their employees are going when they are provided with Internet and World Wide Web access? Should they know? Or is that a breach of privacy issue? Exploring this sensitive area is a former consultant for a software company, who is completing his MBA at London Business School.

A study called "Maximising the Internet" has just been produced for *CIO Magazine*. The publication commissioned the study, subtitled "Policies, Procedures, and Best Practices," as a comprehensive overview of the realities of managing Internet usage within corporations. Some of the biggest areas of study were usage rules, monitoring policies and security and legal considerations. A key finding within the report concerned employee productivity and how and where employees spend their time when they use the Internet and World Wide Web at work.

This brings me to the central theme of this article. Is it ethical for corporations to monitor every move an employee makes while using his or her computer at work, and can they eventually fire someone if they feel this person's actions, while on their computer, are not in line with the corporation's policies? At the heart of this is the advent of technology that allows corporations to know exactly where an employee goes on the Internet, how much time they spend there, what information employees send and receive from News Groups, and what is being said in their E-mails. Is this "Big Brother" gone techno, or do these companies have every right to watch their employees, since, after all, they pay the salaries?

These products go by such names as LittleBrother Pro, ON Guard, and Cyber Patrol. In one corner of this argument are those who claim that corporations have every right to watch and monitor their employees. They do it now in manufacturing plants, hospital wings, supermarket aisles, and office buildings throughout the world. What's the difference if technology is used? On the other

side are those privacy advocates and personal freedom groups who ask when enough is enough. You may pay the salary of an employee, but you don't own his or her life.

At the heart of the issue seems to be the aspect of an employee's productivity. A recent survey by a consultant Robert Half International Inc. showed that more than half of the executives polled said time spent accessing the Internet for non-business purposes is undermining their employees' effectiveness on the job. Analysis of Web sites which contain sports or pornography showed numerous hits during weekday business hours. At Black and Decker Corp. in the United States, for example, monitoring showed that only 23% of the computer traffic going across the company's Internet connection was business related. The scary part of this example is the fact that Black and Decker were able to track the exact percentages along with who were the parties conducting both the business and non-business usage.

The monitoring is aimed at preventing workers from frittering away hours in planning vacations, shopping for cars, or checking the latest sports scores on company time. At some companies managers who suspect an employee is wasting too much time on the Internet are seeking confirmation from Web monitoring logs. To date, there are employees who have been fired because of improper usage. Specific corporate policies regarding the Internet and computer usage are now in vogue all over the world, and certain companies have even developed systems that post messages directly to an employee's computer screen stating that all usage should be for business purposes only and all activity is

monitored. It is obvious that "surfing" the Internet is a problem within corporations all over the world, but the ethical debate hinges on the monitoring, privacy and trust issues.

Arguments for Internet monitoring

Proponents of a policy of monitoring employee use of the Internet cite various reasons for their position. First and foremost, the level of productivity of an employee who spends a lot of time on the Internet inevitably diminishes. Next, there are the legal aspects of allowing employees to pass and retrieve information from the vast reaches of the World Wide Web without the knowledge of management. Thirdly, there is concern about aspects of company policies regarding espionage, security and private company information. These policies, without proper monitoring, would be useless.

Finally, there is concern about the exposure of critical information systems to deadly computer viruses. The argument for preventing exposure to harmful computer viruses stems from the fact that companies are secure in the idea that all of their information systems have been thoroughly checked for such problems. Yet, once an employee ventures beyond the borders of the company's infrastructure and programmes it is very simple for them to pick up a virus from some unknown place out on the "Information Frontier." Once this occurs, unbeknownst to the user they can expose a company's entire computer network to wholesale problems and as a consequence major financial costs. The argument follows that through programmes of monitoring or blockage of employee usage, companies reduce the risk of this event ever occurring.

The argument on the legal front takes into account the fact that employees, as representatives of a company, are open to lawsuits when information they retrieve or send out is deemed to be inappropriate. For example, an employee posts a message regarding a competitor's product on a USENET newsgroup or bulletin board. This instantly reaches millions of people because of the infrastructure of the Internet and World Wide Web, and can have an influence on them. If this information is proved to be wrong or slanderous in any way, the competitor has the perfect lawsuit waiting to be filed. Or, if an employee is downloading pornographic material, or publishing pornographic material from a work computer, the entire company is liable for his actions. If those actions are illegal, as is circulating pornography in certain parts of

the world, the company once again could be facing a lawsuit. The law in these areas is still somewhat grey. However, what is not very grey is the risk of damage to a company's reputation if an employee is caught doing something that is against the law.

On the security argument, how does a company develop the information and knowledge that allows them to be a leader in their market? Of course, they have to have lots of MBA's and practice skilled management techniques, but once they have established this productive combination how do they keep their competitors from finding out their secrets? This issue could take up an entire paper on its own, but in the new information frontier where barriers to communication are so lacking, an employee can with the touch of a button zoom off confidential information to a competitor. It is just that easy to unlock the secrets of a product's development, or the latest manufacturing technique. Without the ability to monitor what employees are sending, and to whom they are sending, the corporate world could some day consist of information raiders hired by competitors to infiltrate their competition and garnish all their secrets. This may be overstating the facts a bit, but it does not take much imagination to see the possibilities.

Finally, the greatest problem facing corporations today is the fact that their employees just spend too much time "surfing" the web and E-mailing friends and checking their favourite teams results from the day before. For anyone who spends any amount of time on the Internet it is very obvious how easy it is to pass hours away venturing from one place to the next without really accomplishing anything. This is not a problem normally, just not on company time, please.

The world, and most significantly, the United States appear to be obsessed with information right now. That translates to more information, and faster please. They want it delivered to their PC's just like a television. With great new technologies like these no work would ever get done without a comprehensive policy stating that all activity will be monitored to assure that usage, within reason, will be for business purposes only. The productivity of employees is a tricky area to get a handle on even without complicating it with this topic. An employee, in the privacy of his or her own office, can often feel like "this is my place and my time, it won't matter much if I spend some time checking the latest stock quotes or sending my sister an E-mail." Granted that before technology allowed these things to happen, employees spent time on the phone in personal calls and could very

well have wasted a lot of their time doing personal things. The opinion of the corporate world is, however, that the Internet and World Wide Web offer employees such an endless array of ways to waste time that this form must be monitored and controlled at all times, or the bottom line profits will eventually suffer.

Against Internet monitoring

On the other side of the coin, opponents of Internet monitoring and E-mail usage cite a myriad of old principles that at the core are aimed at protecting a human being and his or her rights. Included in these are the right of privacy, the right of free speech and the fact that if an employee signs an employment contract and as a part of this contract there is a guideline on Internet usage then they should be trusted to follow those rules as they do all the others that make up a company's corporate handbook.

The right to free speech, an idea that is not supported in all parts of the world, and certainly not a part of a person's working life in most companies, should be more respected in the new information frontier. The issue is not so much with the companies who employ people, but with the entire effort to curb the right to say anything that a person feels like at anytime via any format. The issue within corporations is just where does the line between individual and company separate. When is an individual an employee, and working or speaking on behalf of the company, or simply him or herself?

Opponents of monitoring believe that when an employee makes a conscious decision to state his or her opinion outside on topics outside of the work arena, and they let it be known to whomever, they are acting as an individual and not as a company employee. The law should certainly understand this and not hold companies responsible for an individual's actions regardless of where they begin. However, corporations will say that when we are paying you, everything you do is a part of us. Opponents counterargue, when did life become part of an employment contract, and how did the Internet change all the rules that govern a person and his or her choices? In the past, if a human being felt like stating their opinion on some matter from the comfort of their office or workplace, nobody ever confused that message as originating from the company as opposed to from that individual. The history of the law and cases involving this area supports this assertion completely. Why the change now, and with it

the need for continuous observance by those that are unseen?

The right to privacy is at the core of this employee monitoring issue. Opponents of monitoring state that if a company is so concerned with productivity of employees perhaps they should start by instilling a sense of trust in their employees and foster an environment of productivity and enjoyment as opposed to secretly watching their every move. Maybe by stating that they trust their employees really to be adults and that they understand that knowing when and how to accomplish personal things while on the job is not a new concept, they can actually improve productivity. Now there's a novel concept. The question is who is watching those people who are doing the watching; and who is watching those who occupy the corner offices. Does the term employee mean that you have consented to expose all aspects of your life to those who lurk in the back offices? The opponents of such monitoring feel that enough is enough. If a company feels it cannot trust employees with Internet access and E-mail capabilities then the simplest thing is just not to allow certain people this access. But secretly monitoring employees' movements and analysing them, in an effort to catch offenders of "excessive surfing" or "E-mail violations", has gone too far and breached one of the only things still sacred in a human being's life, his or her privacy.

Finally, opponents argue that a contract represents an agreement entered into between two parties, and if as part of that contract it states that as an employee you will adhere to an Internet and E-mail usage policy that states xyz, then why is there any need for monitoring? In the past, employee handbooks and company policy guidelines stated that as an employee you will conduct yourself in a responsible and lawful manner, and you will not divulge any secrets to competitors, etc. Has the Internet really changed things so dramatically that a company must now watch employees' actions all the time? Of course information can now be transferred and accessed by others in ways thought not possible just five years ago, but at the heart of the issue is the fact that employees could do all of these wrong things in the past, and companies did not hire constant surveillance people and track an employee's every phone call or piece of mail. Where is the difference now, just because the technology is available? Opponents argue that does not make it right and proper, and that contracts entered into between employees and employer now should be treated with the same level of understanding that they have in the past.

Is Anybody Right In This Mess?

Both sides put forward very reasonable arguments, and my personal opinion is still very undecided at this point. I sympathise with those who feel that as each day passes in this "modern" world it brings a little less privacy and trust than before. Yet, I also see the point of view of the corporations world-wide who face heightening competition from a global community where productivity and retaining information is essential to their success.

As a compromise at this point, I feel companies should develop differing Internet policies based on the nature of their business. Firms more concerned with security, such as financial institutions and advanced manufacturers, might create stricter policies than companies in less sensitive industries. Consider a publisher. I don't think that it would be consistent with their business environment to begin restricting employees from accessing the World Wide Web; after all, censorship in any form within this industry would be somewhat counterproductive. In addition, every company should adopt an Internet and E-mail policy and include it in all company handbooks and guidelines to be observed in the same manner as all other guidelines.

The point where I lose my conviction for the argument in favour of companies is the consistent and relentless monitoring of all aspects of employees' computer actions. I am of the opinion that such a culture can only lead to eventual failure for a company as a whole. In the past if an employee was not performing as expected they were probably told about it and if it continued they were most likely fired. So it stands to reason that if an employee really is wasting a lot of time exploring the Internet while at work their productivity will reflect it and eventually they will be fired anyway. It is quite possible that employees may spend a lot of time on the Internet checking sports scores or reading a periodical of their choice and yet be extremely productive in their job because they work longer hours or are more organised than others. It would presumably be a mistake to

let someone like this go because you noticed they enjoyed reading the paper on the Internet everyday.

On the issue of blocking access from a corporate network to Web sites deemed "offensive" or "pornographic", I am in complete agreement with the line of arguments put forth by companies. These sites have nothing to do with work and if an individual wishes to pursue such sites they should feel free to do so outside of work on their own time, not on company time. This aspect is entirely different from your average employee who is visiting a sports or news type site.

In conclusion, corporations world-wide should adopt detailed and written policies on Internet usage and make sure that all employees are clear on the restrictions of use while at work. They should also implement advanced technology that can block offensive sites from being accessed from a corporate network. However, I argue that one should not make a mountain out of a mole hill and pretend that employees' productivity levels are strictly related to Internet usage. Foster a trusting environment that lets employees know that you understand the issues yet you trust in their own judgement to decide where and when to point and click ●

Bibliography

- "CYBERsitter provides IQS Limited in Japan its Internet filtering solution", *Business Wire*, April 22, 1997.
- "Maximising the Internet", *CIO Magazine*, February 4, 1997, pp. 123-128.
- "Don't Go There, Companies Study The Need To Limit Internet Access", D. LeDuc, *Tulsa World*, April 19, 1997.
- "Gotcha! Monitoring tools track Web surfing at work", S. Machlis, *Computerworld*, April 7, 1997.
- "Corporate America and (or vs.) the Internet", *Times Union of New York*, April 9, 1997.
- "Surveying the Wave", S. Rigney, *PC Magazine*, May 6, 1997.
- "True Stories Of The Internet Patrol - Are Once Productive Employees Now Whittling Away Their Time", K. Maddox, *Netguide*, January 3, 1997.

Copyright of Business Ethics: A European Review is the property of Blackwell Publishing Limited and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.