

# R&D



Adam Joinson



Monica Whitty



**Monitored workers experienced greater stress, decreased satisfaction and a decline in the quality of relationships with other staff compared to non-monitored workers**

# Watched in the workplace

Employee surveillance is near ubiquitous, but it may be damaging both staff performance and morale, say **Adam Joinson** of University of Bath and **Monica Whitty** of Nottingham Trent University

In 2006 the UK information commissioner warned that the country was “sleepwalking into a surveillance society”. New technology combined with cheap storage has made it possible to collect data on large groups of people, and to replicate and transport that information with relative ease. This has led to a shift from targeted surveillance of a suspected individual, to mass surveillance of entire populations. The ability to assemble and search datasets, and associated behavioural profiling, means that the era of the anonymous, law-abiding individual is effectively at an end, with both the lawful and the law-breaker both placed under equal amounts of surveillance.

The workplace has not been immune to this increased implementation of surveillance technologies for a number of reasons, including a desire to measure performance, prevent loss and theft, and to ensure that procedures and policies are followed. Given that much of this surveillance is based on the use of information technology, it is hardly surprising that much of the onus for the development and implementation of surveillance technologies has fallen on information technology professionals within organisations.

Recent surveys in the US have painted a picture of near ubiquitous surveillance of

employee’s telephone records, internet activity and emails. While employee surveillance is less common outside of the US, it is increasingly apparent in the UK that the Trades Union Congress are warning against an increasing level of ‘snooping’ in the workplace (see [www.hazards.org/privacy](http://www.hazards.org/privacy)). Quite aside from the legislative implications of employee surveillance, there is an increasing body of evidence to suggest that privacy has an important role to play in the workplace.

## Defining privacy

When we talk about privacy, we often think of unauthorised or unwarranted access to personal information – for instance, reading somebody else’s e-mails, accessing their bank accounts or taking unwanted photographs of them. Indeed, many approaches to understanding privacy deal almost exclusively with the access of information. For instance, Westin (1967, p7)\* defines privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others”.

However, definitions based solely on illegitimate access to information are not sufficient. It is possible to infringe someone’s privacy without gaining new information; for instance, video filming your neighbours

in their garden will most likely violate their privacy, but it is unlikely that new information is gained. Similarly, cold calling by market researchers in the evening is an invasion of privacy, even if the recipient of the call refuses to give any information. In a legal context, privacy is largely synonymous with a “right to be let alone” (Warren & Brandeis, 1890).

The definition of privacy is further complicated because it is both a preference and a state (Margulis, 2003). That is, people can desire privacy, or can ‘have’ privacy. Privacy is also dynamic in that it serves to regulate social interaction (Altman, 1975; Derlega & Chaikin, 1977), while at the same time it can highlight uneven power relations (Derlega & Chaikin, 1977), be used to signify trust (Altman, 1975), or begin a process of reciprocation (Archer and Berg, 1978).

When looking at the impact of privacy on behaviour, a highly complex set of relationships emerge, often with people’s attitudes about privacy exerting less of an influence than their interpretation of the context in which behaviour is occurring. An important part of this context is the level of trust in the data collector – if people trust those requesting and holding the data, issues of privacy are often less pressing.

The highly complex nature of privacy has resulted in an alternative way of defining

it – through its various dimensions. For instance, philosopher Judith DeCew (1997) distinguishes three dimensions of privacy: informational, accessibility and expressive. Informational privacy includes personal information, for example personal lifestyle, finances, medical history and academic achievement. It may be viewed by an individual as information not to be divulged and to be guarded by any recipients of that information.

Accessibility privacy refers to physical or sensory access to a person, and covers both physical proximity and observation. Expressive privacy “protects a realm for expressing one’s self-identity or personhood through speech or activity. It protects the ability to decide to continue or to modify one’s behaviour when the activity in question helps define oneself as a person, shielded from interference, pressure and coercion from government or from other individuals” (DeCew, 1997, p77).

## Privacy and the workplace

Surveillance of employees can, in its various forms, threaten informational privacy (eg through medical history checks), accessibility privacy (eg through cameras, open-plan offices) and expressive privacy (eg through monitoring of communications). Expressive privacy is closely linked to the development and expression of autonomy, something often encouraged in the workplace. For instance, monitoring people during brain-storming sessions has been shown to limit creativity. Similarly, the introduction of video cameras into internet-related discussions reduces the amount of social communication.

Another, perhaps less intuitive argument against surveillance of the internet and e-mail in the workplace is that monitoring can actually lead to poorer task performance. Past research has demonstrated that the presence of others does affect task performance. As far back as the 1960s, Zajonc (1965) argued that social presence – that is, having another person co-present and observing – impairs the performance of difficult tasks, and improved the performance of easy tasks.

In considering such past studies, researchers have questioned whether computing monitoring has a similar effect. Interestingly, Aiello and Svec (1993) have found that computer monitoring does impair

complex task performance. These theorists emphatically recommend: “*with complex tasks do not use computer monitoring at all!*” (p545). Others have also argued that computer monitoring can have deleterious effects upon employees. For instance, Irving, Higgins and Safayeni (1986) found that monitored workers experienced greater stress, decreased satisfaction and a decline in the quality of relationships with other staff compared to non-monitored workers.

The implementation of surveillance technologies can also lead to resistance or ‘gaming’ of the behaviours being monitored. For instance, Aiello (1993) found that 25% of directory assistance operators attempted to cheat the system by disconnecting customers in order to be able to reach their goal, and in turn were rewarded by their supervisors for their shorter than average call records. Others (eg Chalykoff and Kochan, 1989) have argued that employees’ satisfaction with computer-aided monitoring has a large impact on overall job satisfaction.

Surveillance can also reduce the levels of trust in a workplace. And, the transaction costs of working in a low trust environment are generally higher than those incurred working in a high trust environment. For instance, we trust people to engage in various actions on our behalf (eg growing food, educating our children, protecting national security). This level of trust allows us to concentrate on other specialised activities, and therefore increases productivity. In situations where there is low trust, various mechanisms (eg escrow payment systems) need to be introduced in order to allow a simple exchange to take place.

## Security and privacy

If surveillance in the workplace has deleterious consequences, then security professionals face a potential problem. Many security systems link authentication and access to the surveillance of activity – for instance, in terms of monitoring access to buildings or systems. Given the complex, sometimes chaotic, nature of modern organisations, it is hardly surprising that information security professionals face the unenviable task of balancing managers’ desire for greater information about the processes within their organisation with

both the regulatory environment and employee privacy.

However, the complex nature of privacy offers some solutions. For instance, there is evidence that people will willingly trade one form of privacy in order to gain another. To give an example, people will give up reasonably large amounts of informational privacy to websites (in the form of registration forms) in order to gain expressive privacy (in the form of access to a pseudonymous communication system). In this case, the key issue is the amount of trust placed in the gatekeeper (ie the website owner). Other techniques (eg limiting the amount of time data is held for) can support both security and privacy concurrently. We would also suggest that training users to establish strong security habits is as likely to be successful as increased monitoring, but without the negative outcomes associated with increased surveillance.

If companies decide that at least some forms of surveillance are necessary in their places of work, then they might consider including employees’ input into the level of surveillance needed, and how this should be implemented. Kidwell and Bennett (1994) have argued that “reactions of employees to electronic control systems indicate that employee participation in setting up rules to govern use of electronic monitoring and surveillance is desirable and probably necessary” (p48).

Research has found that employees are happy to have some of their internet and email content filtered (in particular, offensive material such as pornography, and unethical, discriminating, criminal and violent material – Whitty, 2004). Moreover, when surveillance is implemented the type of monitoring that is taking place needs to be clearly communicated to all employees, with regular reminders. ■

*Dr Adam Joinson is senior lecturer in information systems at the School of Management, University of Bath ([www.joinson.com](http://www.joinson.com)). Dr Monica Whitty is senior lecturer in psychology at Nottingham Trent University. Their latest book, *Truth, Lies and Trust on the Internet*, is published by Psychology Press in April 2008.*

\* Bibliography for this article: [inf-sec.com/features/janfeb08/workplace.html](http://inf-sec.com/features/janfeb08/workplace.html)