Employee Privacy in the Electronic Workplace: Current Issues for IT Professionals

Neville Meyers
Queensland University of Technology
e-mail: n.meyers@qut.edu.au

Abstract

Today’s managers – drawing on the expertise of their IT professionals – can use technology for both effective monitoring of employee output and achieving unprecedented degrees of control over their workers. On the other hand Australian workers reportedly spend 3.6 hours per week using the Internet for personal reasons. Top Fortune 500 U.S companies have also reported losing billions of dollars because of ‘cyber-bludging’. Yet workplace surveillance – taken to extremes - may also entail important “control” issues. It may impact negatively on both the organisation’s communication climate and its culture, contribute to employees’ increased stress and decreased job dissatisfaction, and affect productivity. It may also create role ambiguity for the IT professional whose loyalties may be divided between management and co-workers. This interactive presentation identifies current trends in workplace privacy, highlights key communication and control issues, points to the current legal climate, addresses IT professionals’ areas of concern and –using a ‘control’ framework – suggests future research directions.

Keywords
Electronic monitoring and surveillance – Ethics Employee privacy – Ethics

INTRODUCTION

Over the past decade the realm of technology and privacy has been transformed, creating a landscape that presents new challenges for IT professionals, management, and communication professionals. Significant changes include large increases in communications bandwidth; widespread adoption of computer networking within organisational environments; as well as new forms of digital media. Such technological adoptions have brought considerable benefits in support of a wide range of social and functional relationships in the workplace. Yet, taking a ‘complex systems’ perspective, (Hearn, Mandeville et al. 1998), these technological changes have created both mixed blessings and at times unintended consequences. For example, technological developments have always had the potential to impact positively or negatively on organisational communication practices (Irwin & More, 1994). However, in the “brave new workplace” that Gelphart (2002) has outlined, such ‘mixed blessings’ demand even more critical attention.

Amongst these ‘mixed blessings’ have emerged concerns relating to what has been called “the perceived pervasiveness of IT-generated data” (Yeuk-Mui 2001) and resultant societal as well as individual privacy issues. As part of the broader social environment in which organisations operate, some writers (e.g., Whitaker, 1999) in almost Orwellian prose have forecast an end to individual privacy in an increasingly ‘hi-tech’ world. Other writers (Mason, Mason and Culnan,. 1995; Lyon and Zureik 1996; Brin 1998) have focused on the inevitable trade-offs between needs for personal privacy and the needs of “authorities” or others to access personal information for the democratic good of society as a whole. Yet other concerns as outlined in Norris and Armstrong (1999) relate to the use of new technologies such as CCTV as new forms of social control.

At the same time, public and private corporations now have the unprecedented potential to collect vast amounts of information and to electronically profile individuals and groups as potential external clients far more effectively than do ‘police state’ regimes (Whitaker 1999), often arguing that these actions are in the public or market interest, whereas – in one national poll random sampling 12,625 people - 56% of Australians report they are worried about the invasion of privacy issues created by the new information technologies.11

As the central focus of this paper, other ‘mixed blessings’ have seen the unprecedented ability of managers to monitor and control their employees’ work output. In the majority of factories and increasingly office situations, such increased control over the work output has been matched by an equivalent decline in the control of the individual worker (Merson 2001). As will be discussed later in this paper, it is important IT professionals

1 See The Bulletin-Morgan Poll (1999), http://www.roymorgan.com/polls/1999/3221. On the other hand, in a later poll, Australians as a whole (around 90% of those polled) appear to have strong views with respect to protection of their personal privacy, especially in relation to personal health, financial, and contact details (Poll 2001).
acknowledge that employees’ perceived loss of control in their work environments may have deleterious effects on work performance and health. Moreover, where appropriate, the IT professional has an ethical responsibility to respect employees’ privacy needs as well as know and respect existing State and National laws pertaining to his or her professional work in organisations – even where such laws may be inappropriate, or need to be challenged (Mason et al. 1995; Weckert and Adeney 1997).

Privacy – Definition and Perceived Relevance to Individual Well-being

According to long-standing authority Westin, privacy is “the claim of individuals, groups or institutions to determine when, how, and to what extent information about them is communicated to others” (1968, p.2). In a more abbreviated form, “privacy is the right to control information about oneself” (Westin 1968, p.2). Thus, in one sense, Westin’s is the classic definition of privacy that is typically cited and discussed in standard IT and business ethics texts (Mason et al. 1995; Weckert and Adeney 1997; Halbert and Ingulli 2003). The definition still bears restating in relation to contemporary workplace surveillance practices.

Monitoring and Surveillance: Definitions

‘Monitoring’ is a term often used in relation to set standards of performance. Thus, monitoring processes in both society and the workplace may have important functions. For both the individual and their organisational or social unit, such processes assist evaluation, they provide direction, they give feedback to ensure activities are in line with intended objectives, and where necessary, they allow corrective action. In the workplace for example, monitoring – depending on managerial intent – has a wide range of uses (many often being beneficial to the worker) ranging from “setting bonuses and keeping track of inventory to controlling individual employees” (Botan 2000), p. 2). However, problems may arise in both work and social contexts, according to (a) the degree of monitoring that is actually being carried out, (b) its actual intent, and (c) to what extent individuals perceive such monitoring as unnecessarily invasive of their privacy.

‘Surveillance’ on the other hand has quite pejorative connotations. Unlike monitoring, ‘surveillance’ usually means physical observation of either employees or citizens without their knowledge (International Labour Office, 1993, a, p.12). However, surveillance may also be overt: the video camera is watching as I walk around the store. What is it recording? And why me? According to the International Labour Office (1993a), both terms ‘monitoring’ and ‘surveillance’ tend to be used interchangeably and “hard distinctions are not made” (p.12). Yet, as recently overviewed by Urbaczewski and Jessup (2002), qualifications remain with respect to the efficacy of workplace surveillance. On balance most writers agree that workplace environments that excessively promote a “control relationship” as a result of the overt controlling policies of management are antithetical to contemporary workplace standards, and may prove dysfunctional to employee performance.

Employee Surveillance and Control in the Workplace

The potential link between levels of monitoring and surveillance on firstly employees’ privacy needs, and secondly on employees’ control beliefs, can be illustrated in the following diagram:

Figure 1: Model developed by the writer to illustrate potential impact of monitoring and surveillance on employees’ control needs. The linearity implied in the model is illustrative rather than predictive. The actual relationships between monitoring, surveillance and their impacts on employees’ privacy needs and attendant control beliefs need, of course, to be operationalised and empirically tested in actual workplace settings.

Tentatively at this stage however, it may reasonably be accepted that excessive levels of workplace monitoring and surveillance that lead to employees’ loss of privacy may also impact on employees’ levels of perceived control. Moreover, drawing on the psychological literature, such control deficits may, in turn, impact negatively on employees’ job satisfaction, productivity, and potentially, health. A wide body of literature in the fields of contemporary industrial and organisational psychology exists, for example, to support this claim (e.g., for overviews see Ganster & Fusilier, 1989; Greenberger & Strasser 1986; Greenberger, Porter, Miceli & Strasser, 1991). Drawing on Spector’s (1986) meta-analysis of 88 studies from the published literature, employees who perceive that they have adequate levels of control in their work environment, are “more satisfied, committed, involved, and motivated” (p.1013).
Two things can be emphasised here. Firstly, overt control mechanisms in the contemporary workplace can potentially alienate workers and, to re-state an earlier claim, have dysfunctional effects on the organisation’s working environment. Secondly, it is clearly the role of the IT professional to anticipate problem areas and to appreciate what extent his or her expertise may be required for use in unethical or as later will be discussed potentially illegal, ways. Accordingly, at this point, it will be useful more sharply to focus on privacy and surveillance as workplace issues.

**HOW PRIVATE IS THE CONTEMPORARY WORKPLACE?**

Privacy has now emerged as the centre-piece of debate concerning information technology and the workplace according to an international canvassing of issues by the International Labour Office (1993). The most common forms of monitoring and surveillance as extensively documented on a country-by-country basis by the ILO (1993) and representatively communicated in contemporary literature include:

- computer-based performance monitoring
- monitoring of telephone calls and other communications
- video surveillance
- searches of employees and their possessions
- “smart cards”, badge systems and other locational devices

But how pervasive is workplace surveillance? According to the American Privacy Foundation, for example, some 27 million employees (representing one quarter of the global online workforce) are being monitored for e-mail and Internet use (www.privacyfoundation.org/privacywatch/report). Research by the American Management Association has similarly reported that in the year 2000 nearly three-quarters of major U.S firms (73.5%) recorded and reviewed employee workplace communications (American Management Association, 2000). This figure represented a doubling of the workplace monitoring practices noted in 1997 (American Management Association, 2000). According to the most recent figures available from the American Management Association (2001) 62% of companies surveyed said they monitored employees’ internet connections; storage and review of e-mail messages (46%); and storage and review of computer files (36%). In February, 2000 it was estimated that more than 75 percent of 400 Australian companies surveyed monitored staff e-mail on a periodic basis, often without notifying employees (front page story The Age, 25/02/00, p.1).

Ethicists (representatively, the International Labour Office, 1993a; Mason et.al. 1995; Weckert and Adeney 1997) have endorsed such invasions into workplace privacy as a major issue. Similarly, in the business ethics literature, loss of personal privacy – fuelled by the growing application of surveillance technologies - has been touted as a negative influence on employees (Velasquez 2002; Halbert and Ingulli 2003). Because of the growing range and sophistication of monitoring devices (e.g., most recently, Orvell Monitoring 2002) allowing monitoring of employees’ web site visits and every e-mail received and sent, it is not unreasonable to expect that some managers may find it even more tempting to engage in workplace surveillance. Yet, in a recent seminar that the writer conducted for the Australian Computer Society in Brisbane, information technology professionals were found to be somewhat ambivalent about the extent to which they might provide their own technical expertise in the interests of workplace ‘snooping’.

Computer-based performance monitoring has, however, reached its zenith in the call centre. Close monitoring of the number and duration of each operator’s calls; rigid guidelines on how to “own” the caller’s problem within set time limits; and regular management checklist assessments of the quality of the communication act – these factors are amongst formal criteria regularly cited for assessing each operator’s effectiveness. Thus, the call centre has become the exemplar organisational model for contemporary forms of employee monitoring and surveillance (Van Den Broek 2002).

**The Case for Workplace Monitoring and Surveillance**

On the other hand employers argue that the real purposes of workplace monitoring and surveillance are justifiable, and are in the interests of both their employees and the general public (Weckert and Adeney 1997, p. 84). As summarised by the International labour Office (1993), these employer arguments relate to concerns about lost productivity; quality control of customer services; compliance with laws and regulations; assistance in training and supervision; protection of employer assets; and lastly, maintenance of a safe and secure workplace (pp.17-19). These findings documented by the International Labour Office in 1993 after its international survey of organisational practices still resonate in the contemporary literature. The most frequently cited argument concerns workplace productivity, given that United States’ corporations reportedly lose more than $US54 billion annually through non-work related Internet use (Contry-Murray 2001). Similarly a U.S company that has 1,000
Internet users reportedly can expect annual productivity losses of up to $US35 million because of employees’ unauthorised web surfing (Saratoga Institute of Human Resources www.saratogainstitute.com). A wide body of literature, much of it empirically grounded in survey data, now exists to support the ‘cyberslacking’ (or, in Australian parlance, ‘cyberbludging’) metaphor relating to employees’ online recreation (playing computer games and social correspondence amongst other uses). Internet pornography is also a concern of some employers leading to the sacking of one educational worker for allegedly assessing pornographic websites while working at Education Queensland (Anon 2002; Panko and Beh 2002). Although up-to-date representative data for Australian organisations is hard to elicit, it is perhaps reasonable to assume that the ‘cyberslacker’ metaphor is well-entrenched in the minds of Australian managers.

Workplace Privacy and Surveillance: The Legislative Response

It is impossible to cover the entire Australian legal system, but a growing body of legislation now exists that both sets new scenarios and provides fresh regulatory contexts for workplace privacy and surveillance issues. Indeed, IT professionals, managers and unions alike – given United States’ legal precedents where employees have sought redress from the courts for breaches of their workplace privacy rights (see Halbert & Ingulli 2003) - might consider specialist advice on the extent to which current legislation-regulations could impact on their own individual responsibilities within particular workplaces. In terms of the Australian legislation, representative are: the New South Wales. Workplace Video Surveillance Act (1998); Victoria’s The Surveillance Devices Act (1999); and Federal Government legislation embodied in The Workplace Relations Act (1996), The Australian Privacy Act 1988; The Privacy Amendment (Private Sector) Bill (2000). Discussion of such legislation and attendant limitations that relate to Australian workers can be found in Poulton (2000) and Sempill (2001). In Australia, the Federal Privacy Commissioner has also released non-binding guidelines on workplace-mail and web browsing, after growing numbers of enquiries about workers’ rights (see www.privacy.gov.au). However, in both the United States’ and the Australian legislation, considerable uncertainties remain with respect to employee privacy and surveillance rights that give pause for concern amongst both IT professionals and their managers on what constitutes “ethical practice” (for example, see Halbert and Ingulli 2003; Sempill 2001).

WORKPLACE PRIVACY: COMMUNICATION AND CONTROL ISSUES

Cognitions about “control” as indicated in Figure 2 offer a useful framework to consider ethical issues. For example, the centrality of control beliefs in human behaviour has been a long-standing tradition in psychological research (for an overview, see Strube 1993). Moreover, control is a useful psychological construct that can in many areas be usefully applied in framing IT-related issues as well as in understanding the behaviour of organisational members (Greenberger and Strasser 1986; Brenders 1987; Albrecht 1988; Parker 1989; Parkes 1989). To be specific, control can be linked to an individual’s latent desire for control, as well as the strength of his or her motivation to exercise that control (Burger 1992). Where managers attempt to adopt excessive levels of control over employees, this may cause employees to behave in ways to enhance or regain their control (Greenberger et al. 1991). Accordingly, communication and control issues that arise in workplace privacy contexts can be suggested by way of Figure 2.

![Figure 2: Control model adapted from Parkes (1989) illustrating components of control and their relationship to outcomes. Main effects are shown by solid lines Double-headed arrows indicate likely reciprocal relationships which the writer intends to explore in a later workplace study.](image-url)
the individual’s desire for control; see Burger 1992). Another control aspect is that privacy can be linked to person-centred needs for autonomy and self-determination: namely, the individual’s sense of initiating and maintaining choices in important personal and work domains, as well as the desire not to be manipulated or dominated by others (Deci 1989). From a rich body of other psychological theory (for example, see Langer and Abelson 1983; Weary et al. 1993; Bandura 1997) such expectancies about lack of control may considerably impact on self-efficacy and perceived abilities to cope with stressors in one’s work and other environments, and have deleterious health effects. Bosma (1997) for example, in a carefully controlled longitudinal study of 10,308 United Kingdom office workers, found that perceived loss of control in the workplace correlated with increased stress and other health deficits.

The call centre – to return to one of our earlier themes – is one of the most salient examples of loss of perceived control in workplace privacy contexts as a result of excessive workplace monitoring. Identifiable factors that have been noted from the research literature are: reported levels of considerable call centre employee dissatisfaction (Van Den Broek 2002); ineffective matching between people and their jobs (Toplis 2000); a ‘sacrificial HR strategy’ to periodically cull out tired employees and replace them with enthusiastic new recruits at low cost to the organisation (Wallace 2000), and problematic levels of call centre customer satisfaction (Bennington 2000). Yet much work needs to be done in order to parcel out actual surveillance aspects that actually effect call centre employee work dissatisfaction levels along with possibly other mediating factors as earlier reported (Yeuk-Mui 2001). Similarly, the above control model (Figure 2) needs to be empirically tested in the electronic workplace to establish causal links. Such control paradigms provide, nonetheless a useful framework to allow further exploration of workplace surveillance and its impact on employees’ general sense of well-being.

RESOLUTION SCENARIOS

General statements of ethical practices in business organisations relate to a desired level of commitment that the organisation should provide as a foundation for the conduct of its operations (Grace 1995). As has already been outlined, employee surveillance and its impact on individual privacy and perceived control are becoming central issues in the contemporary workplace. Despite perceived benefits, applications of technologies in these areas also have the potential to lead to job dissatisfaction, increased stress, and organisational dysfunctionality. For the IT professional, there is also the potential for role ambiguity and loyalties that are divided between the employer and the employee. Clearly however, in many organisations, it will be desirable that the IT professional be proactive and seek to engage in policy formulation with managers and employees (and forestall later problems) in these key areas.

Given such proactivity, IT professionals may experience greater control of both their own work environments and professional standing when they are aware of the full range of ethical options open to them when attempting “to minimize negative consequences of computing systems” (The Association for Computing Machinery ACM Code of Ethics and Professional Conduct, cited in Mason et.al. 1995, pp.269-277). Accordingly, the ACM Code has a series of guidelines (ACM Code Sections 1.1 to 4.0) regarding harm avoidance to others, respect for others’ privacy, adherence to legal frameworks impacting on workplace roles, amongst other guidelines. Similarly, IT professionals need choices in the ways they conduct themselves. One such arena deserving the IT professional’s attention are the professional Codes and attendant guidelines for conduct guiding the profession. Similarly, the Australian Computer Society Code of Ethics in various sections includes value statements and operational guidelines for ethical conduct so that employees may be treated fairly and without discrimination.

Despite the existence of such guidelines a realistic appraisal is needed. For example, a host of environmental variables may interact to either facilitate or inhibit such proactivity on the part of the IT professional: among them, management style, the organisation’s culture, the motivations of its employees to contribute and adhere to ethical standards; and, not least of all, the values and attitudes that the IT professional brings to his or her workplace role. As overviewed in (Wood, Wallace et al. 2001) organisational cultures vary: the ethical climate in some organisations may favour ethical reform and transparency in what may often be deemed quite reasonable levels of workplace monitoring: by contrast, other organisational cultures – as well as management styles - may have greater concerns for operational efficiencies rather than for ethical or social considerations. Barton (1995), for example, offers a comprehensive “ethical audit” benchmarking desirable standards for the contemporary workplace. Because of such caveats, what follows is a set of guiding principles that IT professionals might consider as the basis for the level of their involvement in the establishment and review of ethical practices.

CONSENSUS AGENDAS

Electronic monitoring and surveillance in the workplace may be justifiable in the organisation’s interest on a number of grounds. However, its potential negative effects (or intended consequences) as outlined earlier in this
paper need also to be taken into account. Specifically, control deficits that employees report they face and the actual impact of such deficits on job satisfaction and health – as indicated in the control model in Figure 2 – need further exploration and go beyond the discussion limits for the present paper. On the other hand it has become clear that monitoring that increases employees’ stress and has a negative effect on productivity can be considered antithetical to present-day management cultures and practices (ILO 1993, p.11) In summary, the IT professional should:

(i) Consider, realistically, his or her own value set relating to professional conduct on-the-job; or at least be familiar with the extant guidelines as well as legal aspects that increasingly surround the “brave new workplace”. During the writer’s Conference presentation, a self-evaluation tool, The Employee Monitoring Questionnaire (Appendix) recently used in a seminar the writer conducted for the Australian Computer Society, Brisbane, will be available for interested persons to complete and invite comment. A suggested ‘model’ privacy policy will also be included in the actual presentation.

(ii) Consider, realistically, what might reasonably be accomplished within the organisational culture towards an Acceptable Use Policy for the internet as well as deciding where and how – in partnership with management and employees – reasonable levels of workplace monitoring and surveillance are to be employed and with what optimum levels of transparency.

(iii) Give realistic assessment to employees’ control needs. Virtually all situations, personal and interpersonal, contain elements of control (Langer & Abelson, 1983, p.291; Langer & Dweck, 1973). But in today’s organisations the control is reciprocal: managers and IT professionals whose involvement is being sought to implement employee monitoring practices are likely to get more cooperation from employees where trust and transparency are parts of the processes being instituted. This need not be an over-elaborate process: the use of focus groups or data collection via a questionnaire can be accommodated in most organisations are For example, a standard “gap analysis” assessment asking employees to consider how “important” they rate selected components of workplace privacy and surveillance and how “satisfied” they are with those same privacy and surveillance aspects in their own workplace (using a 7-point rating scale from Low, Medium, to High will suffice and provide useful data).

(iv) Work with management via the data obtained to ensure that implementation strategies are structured – drawing on principles of positive reinforcement (Langer & Dweck 1973) - so as to encourage employees to do things for positive reasons and with targeted positive outcomes for both the organisation and the employee. In short, what needs to be expanded in particular organisational settings, given the inherent limitations of this paper, is not so much why employees might choose to behave unethically, but rather, how they can be induced to behave well.

(v) Work with human resource and the organisation’s other professionals- including a cross-section of employees - and negotiate what are appropriate ethical standards for the organisation. Communicate the standards to all stakeholders, preferably in the form of a policy that acknowledges the needs of the employer while reasonably protecting the interests of his or her employees.

(vi) Assist management and other stakeholders to periodically conduct an “ethics audit” ensuring that, as far as practicable, current workplace privacy policies are in line with both emergent legal requirements and the interests of management as well as its employees.

CONCLUSION

Employee monitoring and surveillance within organisations may exist on a continuum ranging from excessive to relatively acceptable levels, according to individual perceptions. Links between unacceptable levels of employee monitoring and surveillance and their impacts on levels of perceived control may also negatively impact on employees’ job satisfaction as well as impact negatively on employees’ health – aspects which the writer proposes to examine further by operationalising the “control construct” and establishing relationships between “monitoring” and “surveillance”, in actual workplace settings. On the other hand it remains conceivable that excessive levels of work monitoring and surveillance may, in turn, lead to higher levels of employee job stress, impact negatively on productivity, and increasingly in the future raise legal questions, amongst potentially other deleterious effects. Since the IT professional is at the front line in providing technical advice on how, when and where employee monitoring and surveillance are to occur, it is impossible to ignore this issue. Following United States’ precedents, it is also conceivable that managers and IT professionals may, in time, become liable for employees’ perceived undue stress caused by monitoring and surveillance procedures. In short, this is an issue that will not go away: it is necessary that all IT professionals be ethically aware, whether or not they choose (or are able) to act ethically in all work situations. Finally, and in the absence of empirical data establishing links between workplace surveillance and employees’ control needs, successfully negotiated and clearly communicated workplace privacy policies can go a long way to help create a balance between the
employer’s needs and the employee’s rights and responsibilities – a balance that well might promote much-needed levels of harmony in the “electronic workplace”.

REFERENCES


APPENDIX 1

The Employee Monitoring Questionnaire

The following questions are about YOUR attitudes to employee monitoring in the workplace. Please answer using the following scale:

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly disagree</td>
<td>neutral</td>
<td>Strongly agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(a) Employee monitoring is a good thing for most organisations.

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly disagree</td>
<td>neutral</td>
<td>Strongly agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(b) IT professionals shouldn’t feel any conflict about implementing a workplace privacy policy

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly disagree</td>
<td>neutral</td>
<td>Strongly agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
(c) Employees are likely to be more motivated – achieve more - if they are electronically monitored

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly disagree</td>
<td>neutral</td>
<td>Strongly agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(d) Electronically monitored workers are likely to be more productive than non-monitored workers

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly disagree</td>
<td>neutral</td>
<td>Strongly agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(e) Technologically determined work solutions usually work for the better

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly disagree</td>
<td>neutral</td>
<td>Strongly agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(f) Managers are in the best position to determine an employee privacy policy

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly disagree</td>
<td>neutral</td>
<td>Strongly agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(g) Many workers deserve to be electronically monitored to stop bludging

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly disagree</td>
<td>neutral</td>
<td>Strongly agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(h) If I were constantly monitored on my own work I would be stressed

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly disagree</td>
<td>neutral</td>
<td>Strongly agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(i) Employees use the Internet a lot for personal matters

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly disagree</td>
<td>neutral</td>
<td>Strongly agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(j) Electronic monitoring can only increase employee job satisfaction

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly disagree</td>
<td>neutral</td>
<td>Strongly agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

COPYRIGHT

Dr Neville Meyers © 2003. The author assigns to ACIS and educational and non-profit institutions a non-exclusive licence to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The author also grants a non-exclusive licence to ACIS to publish this document in full in the Conference Papers and Proceedings. Those documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the author.