This is the authors’ final peer reviewed (post print) version of the item published as:


Available from Deakin Research Online:

http://hdl.handle.net/10536/DRO/DU:30036179

Reproduced with the kind permission of the copyright owner.

Copyright : 2011, Inderscience
Ethical issues for internet use policy: balancing employer and employee perspectives

Sharman Lichtenstein

School of Information Systems,
Deakin University,
221 Burwood Highway, Burwood,
Victoria 3125, Australia
Fax: +61-3-92446928
E-mail: sharman.lichtenstein@deakin.edu.au

Abstract: An organisational internet use policy (IUP) is a recognised deterrent to manage insider internet misuse. However, IUPs have proven ineffective against this threat, perhaps because of their neglect of the ethical issues involved. An important part of setting an IUP involves the resolution of key ethical dilemmas when employer and employee perspectives conflict. This paper explores the ethical issues that must be addressed when developing an organisational IUP. It draws on a conceptual analysis and an interpretive study of five medium-size and large organisations in Australia and North America. The paper provides a set of key ethical issues for an IUP and compares and contrasts the employer and employee perspectives. It highlights the need to balance the employer and employee perspectives when setting an IUP. Other implications for theory and practice are discussed.

Keywords: internet misuse; internet use policy; IUP; information security management; ethical issues.


Biographical notes: Dr Sharman Lichtenstein is an Associate Professor in the School of Information Systems at Deakin University, Melbourne. She is currently Course Team Chair of the university’s Bachelor of Business Information Systems. She has spent more than 30 years in industry, academe and consulting, in information systems and information technology. Her main research expertise is in information security management, knowledge management and electronic business. Her research has been published widely. She has won research grants and awards and supervised numerous research students. She is on the editorial board for several leading international journals.

Copyright © 200x Inderscience Enterprises Ltd.
1 Introduction

Organisations worldwide recognise the need to better manage internal internet misuse (‘internet misuse’), defined as internal internet use that is unacceptable in terms of an application, organisation, or ethical conduct (Phyo et al., 2007). Employees, ex-employees and contractors increasingly succumb to e-mail phishing attacks, disclose confidential business information, engage in excessive personal web use and commit other internet misuses (AMA, 2007; CSI/FBI, 2007; Deloitte, 2007; PWC, 2007). A recognised managerial measure to deter internet misuse is an internet use policy (IUP) supported by security procedures and technologies (Chen et al., 2008). An IUP sets out guidelines for employee internet use in the form of acceptable and unacceptable internet uses and sanctions for non-compliance. This policy aims to regulate employee behaviours contributing to organisational internet risk while maximising the value gained from valid internet business uses (Lichtenstein and Swatman, 1997). However, given the increased incidence of internet misuse reported in recent years, IUPs appear ineffective.

This paper argues that an overlooked but important influence on the effectiveness of IUPs is the perspective taken on the ethical issues involved. Business ethics has been defined as ‘the study of those decisions of managers and corporate management which involve moral values’ (Gandz and Hayes, 2004). Contemporary business ethics often adopts a normative perspective in which profit is not the sole measure of success (Egels, 2005). This research adopts a normative approach to business ethics, seeking to achieve ‘core human goods’ for the humans involved in business internet use and a moral outlook (Spinello, 2006). Spinello (2006) observes that justice and fairness are core human goods potentially available in a business. Core human goods may be attained by adopting a rights-based approach to ethics (‘contractarianism’) based on the need to respect an individual’s legal, moral and contractual rights (Spinello, 2006). Spinello (2006) notes the challenges of respecting often-competing individual rights. Despite these challenges, it is strongly argued next (and in this paper overall) that a rights-based approach to the ethical issues should produce a more effective IUP.

This paper argues that employee decisions about internet use, as for other employee decisions, are positively influenced by ethically-oriented managerial tools of persuasion where employee rights are respected and there is a perception of equity (Cronan and Douglas, 2006; Douglas et al., 2007). In other words, employees are more likely to comply with the policy under such conditions. Evidence from the organisational studies and information security literatures offers significant support for this proposition. Firstly, organisational citizenship improves substantially when employees feel supported (Coyle-Shapiro and Conway, 2005) and an organisation is fair to its employees (Holmes et al., 2002). Secondly, when ethical conduct is supported by management, employees are more likely to behave ethically (Kaptein, 1998). Third, information security research is progressing toward socio-cultural approaches aimed at motivating and persuading employees (e.g., Dhillon and Backhouse, 2001; Siponen, 2000). A socio-cultural approach to an IUP would reflect a belief that employees are more likely to use the internet appropriately when the desired behaviour is natural and intuitive in the workplace. Fourth, employee decisions may be influenced by ethically-oriented managerial tools of persuasion (after Cronan and Douglas, 2006) where employee rights are taken into consideration and there is a sense of equity (Douglas et al., 2007). In summary, the above evidence strongly suggests that an ‘ethically balanced’ IUP – one
regarded as fair by employees and employers alike – will be the most persuasive and effective for garnering employee cooperation and compliance with the policy.

Currently, the literature on ethical issues for an IUP is sparse and lacks a synthesis of the key ethical challenges for an IUP and interpretive studies of the topic. This paper explores key ethical issues involved in setting an IUP. It also provides an understanding of the oft-conflicting rights of employees and employers. The paper argues strongly that the employee and employer perspectives of the ethical issues should be negotiated and balanced when developing an IUP. The ethical issues and perspectives are identified in this paper from:

1. a literature review which initially synthesises the ethical issues
2. an interpretive study involving six case studies in five medium and large size Australian and North American organisations and a cross-organisational focus group of six Australian information security experts.

The paper proceeds by reviewing 11 key ethical issues to be addressed when setting an IUP. These issues were identified from a review of relevant literature. The paper then presents the main findings from six interpretive case studies exploring the issues and a validation focus group. The findings include a set of ethical issues for an IUP that highlights conflicting employer and employee perspectives. After the findings have been discussed, a conclusion section outlines theoretical and practical implications and offers closing commentary.

2 Ethical issues for an IUP: a review

According to a review of literature, 11 ethical issues are relevant when setting an IUP (Figure 1). The first ethical issue is the degree of internet use permitted to employees. Two fundamental questions are: Should employees be free to use the internet for any legal purpose? Is internet use in the workplace a privilege, right or benefit? Employers believe that internet use is a privilege and seek to restrict internal internet use with the objective of maximising business use, business access and productivity (Case and Young, 2002). However, a recent charter of internet rights includes the provision of worker access to the internet for reasons such as work education (APC, 2006). Furthermore, recent surveys demonstrate that employees seek liberal personal web use in the workplace (AMA, 2007; Reuters, 2007; CSI/FBI, 2007; PWC, 2007). Personal web use has been defined as voluntary online web behaviour during normal working hours using any of the organisation’s resources for activities outside current customary job/work requirements (Anandarajan and Simmers, 2002). It is important to understand employee motivation for personal web use and consider its legitimacy. Employees responding to a BurstMedia survey in 2007 cited a range of reasons for surfing the web (including use of social media) at work: the need to stay informed during the day, boredom, contact with family and friends and convenience (Reuters, 2007).

How can information security managers determine a fair level of personal web use? First, managers should understand that there could be positive effects from personal web use, such as improved business and technical skills and business acumen. They might also consider dysfunctional and constructive uses of the internet (Anandarajan and Simmers, 2004). The work role of an employee is also relevant. For example, an
employee performing administrative duties would have different work-based internet needs compared with a medical researcher. Setting limitations on personal web use may be further complicated in modern business environments where the line between work and home life can be blurred and the internet is commonly accessed from home for work purposes (Anandarajan and Simmers, 2004).

Figure 1 Ethical issues for an IUP (see online version for colours)

The second ethical issue for an IUP is privacy of internet use (Miller and Weckert, 2000). Many situations legitimate an employee’s internet use privacy requirements (Martin and Freeman, 2003). For example, privacy is essential for employees to communicate with unions and human resources personnel. Some internet privacy services such as anonymity can support employees’ internet privacy needs although there have been reports that employees may then be more likely to abuse internet privileges (Zhang et al., 2006). Despite legitimate employee privacy needs for internet use, managers will often seek access to internet use information to protect the organisation from harm.

This consideration leads to the third ethical issue – monitoring of internet use (Introna, 2001). Martin and Freeman (2003) identify a range of employee concerns about electronic monitoring, including liability, privacy, security, creativity, paternalism and social control. Work performance may be lowered when employees are electronically monitored (Adams et al., 2005; Whitty, 2004). Adams et al. (2006) research suggests that electronic monitoring may have little impact on employees’ intentions to engage in personal web use.

However, there is growing evidence that electronic monitoring can be implemented with the cooperation of employees (Stahl et al., 2005). Introna (2001) believes that when an employer justifies electronic monitoring and provides assurance regarding the planned use of collected data, employees perceive there is organisational justice. Similarly, Alge (2001) found that when electronic monitoring is linked to job-related activities and employees contribute to the development of the monitoring policy, employees perceive less privacy violation and greater procedural justice. Urbaczewski and Jessup (2002) discovered that workers monitored electronically for reasons of feedback were more...
Ethical issues for internet use policy

satisfied with monitoring than workers monitored for control purposes. A fourth and related ethical issue is surveillance of employee internet activities. In policy setting on monitoring, employees deserve greater negotiating power while managers should moderate such negotiations (Palm, 2004; Stahl, 2005).

Employee accountability is a fifth ethical issue for an IUP. The purpose of accountability is to determine which entities commit particular actions (Burmester et al., 2004). Employers may seek employee accountability for internet use so that workers who misuse the internet can be identified. For accountability, internet use should be visible, involving recording and maintaining a comprehensive secure history of employee internet actions with the support of monitoring software (Martin and Freeman, 2003). From an employee perspective, however, there may be some ambivalence as greater accountability often entails less privacy (Burmester et al., 2004). Yet there are some advantages for employees from accountability as it ensures that employees are not blamed for others’ internet misuse.

A sixth ethical issue for internet use is trust. Employee trust in an employer could influence the effectiveness of an IUP. An open honest culture, where there is no deception and employer-employee rights are compatible, supports the formation of trusting relationships (O’Neill, 2002). When an employer-employee relationship is imbued with mutual trust, conflicting employer-employee perspectives of internet use regarding security and privacy are more amenable to resolution (Mitrou and Karyda, 2006). In contrast, when employees lack trust in management, they are more concerned about due process and fairness (Tabak and Smith, 2005). O’Neill (2002) has noted that employee trust may be damaged by complex systems of accountability and control.

Seventh, employees have a right to be kept informed of their roles and responsibilities in internet use and internal controls, which affect them. Employers have a duty to inform employees of acceptable internet uses and related policy (Chen et al., 2008). Many internet risks to which employees inadvertently contribute are better managed by informed employees. For example, employees should be informed of their browsing habits to help counter spyware and adware (Shukla and Nah, 2005). However, an awareness of issues relating to internet use is often absent. For example, many employees are unaware of the monitoring of internet use (Dillon and Thomas, 2006). Signed consent of IUPs can help to promote such awareness (Woon and Pee, 2004).

The eighth ethical issue for an IUP is censorship. Here, employers aim to prevent insider non-business internet use, access to objectionable or criminal websites and defamation or harassment of others. Web filtering can be used to prevent access to inappropriate content (Bertino et al., 2006). In 2007, 65% of US companies used web-filtering software for this purpose while around 50% to 80% of US companies blocked access to social networking sites (AMA, 2007; Clearswift, 2007). In contrast is the employee perspective. Many scholars regard any form of internet censorship as counter to democratic principles (c.f. Berman and Weitser, 1997). Employees may seek democratic rights of freedom of speech in internet use (e.g., the desire to write unfettered e-mail messages) and freedom of information in internet use (e.g., the desire for unfettered access to the complete spectrum of external web content) (Godwin, 2003). The likelihood that such employee rights can be respected is less feasible in some regions where internet content is censored by national policy (c.f. Zittrain and Edelman, 2003). Surprisingly, in Whitty’s (2004) survey of Australian employee attitudes, 61% of
employees were in favour of banning offensive materials in the workplace, highlighting evolving employee views on this ethical issue.

Information ownership is the ninth ethical issue. Employees expect ownership and control over their e-mail messages and web-based content (Everett et al., 2004–2005). Employers can be liable for discriminatory or harassing messages authored by employees. In the US, ownership of electronic information is based on property rights while in Europe it is based on human rights (Everett et al., 2004–2005). Therefore, employee rights to information ownership may be better honoured in Europe than in the US.

Tenth, there is an ethical issue concerning IUP compliance and sanctions. The employer perspective seeks compliance and advocates the use of sanctions. The employee perspective takes into account regulations such as industrial relations law. Sanctions have been found to be effective for enforcing information security policy enforcement (Straub, 1990). However, more recent results suggest that no such relationship exists (Pahnila et al., 2007).

Eleventh, there is an ethical issue regarding the values that should underpin employee conduct when using the internet. Honesty, fairness, trust, willingness to share and a readiness to assist other people, are considered exemplary values (Deshpande, 1997). Employer values may be represented in a company code of ethics or in an ICT Professional Code of Conduct (Bia and Kalika, 2007). However, employee values might conflict with such codes and thus limit the effectiveness of the policy. For example, a lack of moral awareness by some employees can influence the appropriateness of their internet use (Leonard et al., 2004).

This section has reviewed eleven ethical issues for an IUP, often viewed differently by employers and employees, but important to balance (Figure 1): freedom of internet use; privacy; monitoring; surveillance; accountability; trust; the right to be kept informed; censorship; information ownership; compliance and sanctions; and ethical conduct. An important theme emerging from the above review is that while the literature clearly suggests differences in employer-employee perspectives for each ethical issue, there may be conditions under which both employers and employees will be willing to align their perspectives on the issue more closely.

3 Methodology

This section describes the design of a ‘three stage interpretive research study’ that investigated key ethical issues for an IUP (reported in this paper) and internet risks (reported elsewhere). In Stage One, a literature review was conducted, culminating in the synthesis of eleven ethical issues, discussed in the previous section. In Stage Two, six interpretive case studies were conducted at five medium and large organisations (three large Australian organisations, one medium size Australian organisation and one large North American organisation). The eleven ethical issues were explored at the five case companies by the use of a questionnaire (as will be explained) and semi-structured in-depth interviews. For reasons of anonymity, pseudonyms for company names are employed in reporting the cases.

In the first case study, the researcher explored the views and expectations of ethical issues for an IUP of a class of final year undergraduate information systems (IS) students who were studying IS security at a large Australian university, AusEd. In a lecture room
setting, 79 students (age 20–22 years) were briefed by the researcher on the key objectives and background for the study and the purpose of a printed questionnaire which was distributed to all present. This questionnaire was developed from the 11 ethical issues and comprised 19 questions exploring the ethical attitudes of respondents to the 11 ethical issues. The researcher asked students to respond, in a two-hour session, to the questionnaire in the role of new employees who were expected to use the internet daily for work purposes in a business setting. Seventy-two (72) students returned a completed, usable questionnaire. The students thus served as surrogates for new (adult) employees who use the internet regularly at work.

The decision to use students as surrogates for adult employees is justified as follows. While several studies have cautioned against the generalisability of results obtained by studying student proxies in social science contexts (e.g., Peterson, 2001), other studies have suggested that undergraduate students can be used as surrogates for employed adults when ethical issues are the subject of study (e.g., Morris and McDonald, 1995). Another study suggests that IS undergraduates have different ethical views of IS ethical dilemmas compared with IS professionals (Wagner and Benham, 1995). However, Cleek and Leonard (1998, p.64) note that many students have work experience and can therefore be representative of new employees. As the students studied in this research were in the final year of their bachelor degree and were planning to enter the information technology workforce full-time the following year, their views were likely to be representative of at least part of the population of interest – graduate adult employees who use the internet regularly for work.

The questionnaire data collected from the students were later analysed by quantitative content analysis and qualitative content analysis techniques, with findings grouped into 11 themes corresponding to the ethical issues reviewed earlier. Supplementary data collected included relevant university documents such as the university internet use regulations. These data were employed to help interpret student responses.

In the second case study, also conducted at AusEd, another class of 55 similarly aged computer security final year undergraduate students was polled in a similar manner, using an enhanced printed questionnaire that comprised questions about internet risks including student misuse (but not specifying the ethical issues). 49 completed usable questionnaires were collected. The data were analysed by quantitative and qualitative content analysis and where findings related to any of the 11 ethical themes, they were used to enhance the findings from the first case study.

Next, four detailed case studies at three Australian organisations (FlyPass, MedSearch and AusRetail) and one North American organisation (Total Energy) were conducted using a case study protocol, as follows. Information security managers and network administrators (collectively termed ‘managers’ hereafter for brevity) were interviewed by the researcher in semi-structured interviews, seeking employer perceptions of internet misuse and other internet risks occurring at their companies and the ethical issues involved in internet misuse. The questions probed the AusEd students’ perspectives on the 11 ethical issues involved in an IUP. The researcher disclosed the students’ perspectives (acting as proxies for employees) on each issue and asked whether the managers agreed with these perspectives. The researcher also enquired about any differences in the employer perspective. The researcher took extensive interview notes, which were later analysed. In the analysis, significant differences between employer perspectives and employee perspectives emerged for many of the issues.
In Stage Three, the 11 ethical issues and employer/employee perspectives of these issues were discussed at a validation focus group of six information security experts from six medium-size and large Australian organisations. The focus group was videoed and the video later transcribed and analysed using qualitative content analysis. The set of ethical issues with differing employer-employee perspectives was enhanced using the focus group findings and is summarised in Table 1. The main findings from the study are discussed in the next section.

4 Ethical issues in an organisational IUP – employer-employee perspectives

The research study revealed a range of significant internet misuses occurring at each organisation, including personal internet use, downloading of infected e-mail attachments and software piracy. The internet misuses were identified by managers as significant internal internet use risks. Each company had implemented a formal policy to deter internet misuse. However, according to the managers interviewed, existing policies were clearly ineffective. The 11 ethical issues identified in the study are summarised in Table 1 and discussed below in terms of the case studies. The table highlights ethical dilemmas resulting from differing employer and employee perspectives of the issues.

First, controversy surrounded the issue of ‘freedom of internet use’ for employees. Students at AusEd, responding in their role of proxies for employees, clearly believed that workers possessed rights to the use of the internet at work. Most students believed that personal internet use should be constrained but not entirely prohibited, while noting employer challenges for enforcing such restrictions on employees, such as the difficulty of differentiating business from non-business internet use. Several students were puzzled by the idea of restricting a tool apparently designed for sharing information. Student suggestions for restrictions on personal internet use included time limits such as two hours per day at lunchtime, or after work hours. However, a significant group of students believed that as long as their work was completed, there should be no restrictions on personal internet use.

By contrast, the managers interviewed at the case organisations did not share this view. First, they reported that many employees were spending significant internet time on personal internet use (an incidence as high as 50% was reported at Total Energy in the US). The managers found it difficult deciding whether employee internet use was a privilege, right, tool or benefit. However, overall, their perspective was that employee internet use was a privilege. There was also considerable uncertainty regarding the permitted degree and scheduling of any personal internet use. For example, in their IUPs, four organisations prohibited non-business use entirely while one company permitted it ‘where necessary’. Highlighting employer difficulties with accommodating the views of this topic espoused by the students, AusSales felt that the two hours a day of personal use, suggested as fair by some students at AusEd, was feasible, provided that supervisors took some monitoring responsibility. FlyPass commented that if many employees used lunch hours for personal internet use, not only would the server be saturated and the printer(s) consumed by the printing of non-business material, but monitoring would be more difficult. Despite the restrictions to personal use in the official IUP, all companies had been turning a blind eye to such use unless it was particularly noticeable or a complaint had been made.
### Table 1  Employer and employee perspectives of ethical issues for IUP

<table>
<thead>
<tr>
<th>Ethical issue</th>
<th>Employer perspective</th>
<th>Employee perspective</th>
</tr>
</thead>
</table>
| Freedom of internet use | • Internet use is a privilege  
• Restricted personal internet use | • Internet use is a right  
• Significant personal internet use |
| Privacy             | • Accountability for internet use  
• Recording of internet use | • Privacy of internet use  
• Anonymity of internet use |
| Monitoring          | • Electronic monitoring of internet use | • Trust demonstrated by absence of electronic monitoring.  
• Trust demonstrated by absence of electronic monitoring.  
• Trust demonstrated by absence of electronic monitoring. |
| Surveillance        | • Use surveillance only to control high risks | • No surveillance  
• No surveillance |
| Accountability      | • Hold employees accountable for their internet actions, requiring monitoring, possible surveillance and sanctions on non-compliance  
• Signed consent forms | • Roles and responsibilities to be clearly identified in policy  
• Evidence in policy of services that support accountability |
| Trust               | • Employers need to manage levels of security and risk while showing sufficient trust | • Employees need to feel trusted by employers through liberal policies and limited monitoring |
| Right to be kept informed | • Internet use awareness activities | • Internet use awareness activities  
• Internet use awareness activities |
| Censorship          | • Restricting internet material for legality, decency, confidentiality and reputation reasons  
• Restricting internet access to business information  
• Protection of employees from harm in accessing objectionable and harmful internet content | • Freedom of expression/speech  
• Freedom of information |
| Information ownership | • Company ownership of all postings and employee-authored internet materials  
• Need for disclaimers on personal messages and employee home pages | • Employee ownership of authored personal messages and other personal internet materials created in the workplace  
• Warnings  
• Specific sanctions |
| Compliance and sanctions | • Flexible sanctions culminating in dismissal | • High ethical standards  
• Specific sanctions |
| Ethical conduct     | • High ethical standards  
• Consistency with code of ethics | • High ethical standards, but not excessively restrictive |
The study also revealed conflicting employer-employee perspectives on privacy, monitoring, surveillance and accountability. Students, participating as proxies for employees believed that employee internet use should be anonymous, that it should not be recorded or monitored by employers and that employer insistence on accountability reflected a lack of trust. Surveillance, such as video surveillance, was considered unethical. Interestingly however, many students noted a preference for human supervision of internet use rather than electronic monitoring. They saw traditional management by walking around as an acceptable form of monitoring.

The managers, on the other hand, argued against anonymous internet use as it precludes accountability. Indeed, they sought electronic monitoring in order to fulfil risk management obligations to stakeholders and protect employees. While the organisations electronically monitored employee internet use, they were nevertheless slow in following up detected misuses. ‘Turning a blind eye’ was considered an easy way to deal with a seemingly intractable problem. Personal surveillance was viewed as necessary if and only if there were very high risks of internet misuse (however, none of the companies studied were in such a position).

Managers also noted that accountability for internet use requires not only electronic monitoring and sometimes physical surveillance, but sanctions for enforcement. Signed consent for policies also support accountability. Students at AusEd noted a need for definitions of employee roles and responsibilities in internet use. They also wanted evidence of any services offered that enabled employee accountability for internet use.

Conflicting perspectives emerged on the ‘censorship’ issue. All students at AusEd opposed the filtering of internet content while censorship was clearly favoured as the employer perspective. Surprisingly, not all companies were filtering websites. Managers at the two companies, which did not filter websites, believed it was up to employees to access appropriate sites as directed by policy and not up to the company to actively censor content. Nevertheless, electronic monitoring enabled detection of accesses to objectionable websites, at which point action was taken as directed by the official policy. FlyPass filtered websites with managers citing the potential damage to its reputation that could eventuate if a company such as a pornography business reported that FlyPass employees had accessed the website.

The managers interviewed clearly recognised the censorship issue as contentious and ceded that it needed careful consideration prior to setting an IUP.

The issue of employer-employee mutual ‘trust’ was important to both groups. Students at AusEd, participating as proxies for employees, believed that logging of internet use and monitoring indicated employer mistrust and would be deleterious to the organisational culture. Employers at two organisations had adopted the policy of ‘some rights and some responsibilities’ which they believed conveyed trust and care. Generally, the students at AusEd felt that employers should trust that employees are trying to do the right thing by the organisation when using the internet, while employers felt that employees should trust them to look after the best interests of the organisation and its employees when setting an IUP.

The ‘right to be kept informed’ is important to both employer and employee. One company, MedSearch, which had an informal IUP, believed in the old adage ‘buyer beware’ in relation to employee activities in internet use. The manager interviewed at MedSearch saw this as a legal issue, however, noting that when MedSearch developed a formal IUP, it would need to inform its employees regarding policy matters for legal
reasons. Overall, the right to be kept informed was not a contentious issue, although companies found it difficult to schedule and resource adequate IUP awareness activities.

‘Information ownership’ is another key ethical issue for an IUP. Managers believed that employers owned the content of all websites on company servers including the content of employee home pages. This stance mirrors the legal position. However, managers believed that some employees would claim ownership of any internet information, which they had authored.

‘Compliance’ and ‘sanctions’ were contentious issues. Students believed in a range of persuasive approaches to compliance, including: gaining employee cooperation; explaining policy benefits to employees; setting and enforcing penalties; monitoring (via human supervision); awareness sessions; and displaying of the policy on browser start-up. Penalties nominated by students centred on warnings and suspension of connection to the internet. Some of the case organisations agreed with such penalties. However, it was suggested by managers that the highly specific sanctions, which AusEd students advocated, conveyed distrust between employers and employees. Flypass had specified a flexible sanction for non-compliance, ‘Disciplinary action will be taken’. In contrast, Total Energy delegated total responsibility to information security managers for dealing with incidences of non-compliance.

The ‘ethical conduct’ of employers and employees was an important consideration when developing an IUP, according to managers at the case organisations. Managers discussed the need for an IUP to comply with organisational ethical codes. In contrast, AusEd students, responding as proxies for employees, were concerned that existing ethical codes may already be too restrictive and sought less restrictive codes.

5 Discussion

The first key difference in the employer and employee perspectives of an IUP relates to the level of acceptable personal web use. According to Table 1, the employee perspective is rights-based, but seeks significantly broader rights than the charter of internet rights (APC, 2006) allows. The charter emphasises the right to internet use for legitimate work-based reasons such as work education. However, in the study findings, the employee perspective reflects the reality of personal web use in the work place as also highlighted by recent surveys (AMA, 2007; Reuters, 2007; CSI/FBI, 2007; PWC, 2007). The employer view identified in Table 1 – that internet use is a privilege – supports related findings by Case and Young (2002). Yet, nowadays there is a blurring of the boundary between work and home (Anandarajan and Simmers, 2004) which suggests that employers should adopt a more flexible approach to personal internet use in an IUP, gaining employee trust in the process. As the findings from this study have suggested that trust of employers is an important factor in IUP effectiveness, employers may be persuaded to draw closer to more liberal personal web use by realising that there can be work-related benefits from personal web use, such as skills and knowledge development (Anandarajan and Simmers, 2004). Considering the work roles of employees may also help to make the policy more flexible and relevant.

The study also found that privacy and monitoring were contentious issues for an IUP and that when employers implemented electronic monitoring it was reflective of a lack of trust in employees. Some researchers have discovered that different forms of electronic
monitoring may be better accepted by employees than others. Cooperation (Stahl et al., 2005), justification of policy and assurances regarding planned use of collected data (Introna, 2001), employee participation and negotiation in policy-making (Alge, 2001; Palm, 2004; Stahl, 2005), clear linking of electronic monitoring to work activities (Alge, 2001) and feedback-oriented monitoring (Urbaczewki and Jessup, 2002) are possible complementary approaches to electronic monitoring to engage employee trust and align the IUP more closely with the employee perspective.

The study suggests that employees are ambivalent about their accountability for internet use. The electronic monitoring required to achieve such accountability is considered unethical by employees. Suggestions for making monitoring more acceptable ethically have been given above. Employees are also keen to know what they are supposed to be doing when using the internet. They would clearly benefit from definitions of their internet roles and responsibilities and related awareness activities. They should also be educated about the services (e.g., monitoring) employed to implement accountability, such as authentication, action/event binding (non-repudiation), monitoring and trust infrastructures (Burmester et al., 2004).

Given employee concerns about website filtering, there could be a greater effort made by management to explain the need for filtering to employees. Greater commitment to the policy may develop if employees participate in the identification of websites to be blacklisted. Such participation would include discussing whether to ban popular social networking sites as many companies have recently done (AMA, 2007; Clearswift, 2007). In countries where heavy internet censorship applies, there may not be much opportunity for this level of flexibility, however. Whitty’s (2004) survey of Australian employee attitudes provides evidence of evolving employee views on the filtering of objectionable sites. Clearly, ongoing participation in policy-making will ensure that changing employee attitudes are captured.

While the right to be kept informed was not a contentious issue, the study highlighted a lack of resources for awareness activities and a concern from employees for their rights and responsibilities in internet use to be clearly communicated. Thus, the findings support existing research on awareness for acceptable internet use (Chen et al., 2008; Shukla and Nah, 2005; Woon and Pee, 2004).

While managers in the study believed in the employer’s right to the ownership of internet-based information, they also noted that some employees sought ownership, supporting related findings by Everett et al. (2004–2005). There may be ways that employers can provide greater control of employee-authored information to employees through the policy and greater levels of privacy. For example, the policy could state that employees will be notified if management are considering taking actions with e-mails (such as regular culling) or websites.

Showing trust through an IUP was considered very important for an effective policy. A fair negotiation of employer and employee perspectives of the ethical issues is part of the process of developing such trust holistically. Providing greater awareness of an IUP and related issues affecting employees may also help promote employee trust and a more effective policy.

The differing views on compliance and sanctions identified in the study suggest a need for engaging employees in setting sanctions. Employees were in favour of more generic, flexible sanctions with warnings for initial breaches. The findings suggest that employers and employees are concerned about the types of sanctions and approaches used. However, Pahnila et al (2007) have conducted research suggesting that sanctions
have very little deterrent impact. Perhaps, yet again, this is a trust issue. If employees have been fully involved in policy-making and have had an opportunity to help set the sanctions, employees may be more likely to comply with the policy overall.

The findings also suggest that the best value for representing ethical conduct in an IUP may be found in referring to pre-existing recognised ethical codes which are well recognised and accepted by employees. The company code of conduct may, however, need review if regarded by employees as too restrictive for acceptable internet use.

6 Conclusions

Drawing on a literature review and an interpretive study, this paper has contributed to existing theory on the management of organisational internet misuse by providing a set of ethical issues for an IUP (Table 1) that adds to understandings in this important area. The paper has also provided important insights into the sometimes-conflicting employer and employee perspectives of IUP and how they could be resolved in the policy.

The findings from this paper have important practical implications for information security managers. First, the set of ethical issues (Table 1) may be useful as guidelines when managers are developing or reviewing an IUP. Managers can consider and debate the various ethical issues with employees, seeking resolution wherever there are conflicting perspectives. The use of the set of ethical issues as a reference point could help to clarify opposing employer/employee positions and whether the final developed policy has indeed taken an equitable approach. As an example, the use of the set of ethical issues may suggest to a company to take a more constructive employee-oriented approach to electronic monitoring and to set flexible sanctions.

This paper suggests to information security managers that employees would benefit from having clearly articulated roles and responsibilities regarding acceptable internet use. This point is rarely addressed in academic or popular literature on IUP. The paper also loans support to researchers who have called for comprehensive IUP awareness (e.g., Furnell et al., 2004) to help employees better understand and comply with an IUP. The findings in this paper are also consistent with research advocating the use of socio-cultural approaches for organisational information security management (e.g., Dhillon and Backhouse, 2001). Finally, the findings suggest that adopting a balanced view of the ethical issues for IUP will help develop mutual trust and that such trust may play a key role in providing a more persuasive IUP.

The findings reported here are clearly limited as they are based on a study that tapped student perceptions as proxies for employee perceptions. Employer perspectives were identified from interviews with information security managers and network administrators at the case organisations. These managers also gave their perceptions of how employees in their companies thought and behaved. Clearly, future research on the ethical issues for an IUP should involve tapping into employee perspectives directly.

This paper suggests that despite often-conflicting ethical perspectives of employers and employees in IUP, a more complex reality exists. There is an opportunity for information security managers to develop more persuasive IUPs by tapping into employee goodwill in policymaking by negotiating differing ethical perspectives, thereby increasing trust. As Mason et al. (2002) found, employers and employees work toward
the same organisational objectives and therefore may seek synergies and similar worldviews in an IUP.

References


Ethical issues for internet use policy


Reuters (2007) One Fourth of Internet Usage at Work is Spent on Personal Tasks, Reuters Online, Wed 5 December.


