



Should Filtering Software be utilised in the Workplace? Australian Employees' Attitudes towards Internet usage and Surveillance of the Internet in the Workplace.

Monica T. Whitty¹

Abstract

The notion of Internet and email monitoring in the workplace is a debatable issue. Some would argue that surveillance is necessary to prevent 'cyberslacking' which can lead to loss of productivity and be a waste of a company's resources. In contrast, others contend that cyberspace is a private space that employers do not have the right to intercept. There is currently a dearth of available Australian baseline research available on employees' opinions on Internet and email activity in the workplace. This paper reports the findings from a survey, which asked Australians about their attitudes on appropriate usage of the Internet and email in the workplace, and their opinions on filtering software. This study considers whether gender, working for a company which has implemented a company policy, and number of hours of Internet usage in the workplace are useful predictors of attitudes towards Internet and email behaviour in the workplace. This study concludes that individuals do condemn some Internet and email activities in the workplace, such as downloading material that might offend or harasses others. However, participants did not all agree that filtering software is the only solution to preventing inappropriate Internet and email behaviours. Furthermore, this study found that, at least in the Australian workplace, there is a need to begin seriously questioning what is appropriate Netiquette.

Introduction

As the Internet and email increase in importance as useful tools in the workplace, in turn, employers are concurrently considering implementing electronic surveillance as a means to monitor and control how their employees are using this tool. As Susser (1988) suggests, electronic surveillance can be employed for three main purposes in the workplace. These include measuring performance, preventing theft and ensuring that workplace rules and policies are adhered to. As detailed below, presently the opinions on electronic surveillance in the workplace are largely bifurcated – there are those who are strongly pro electronic surveillance and those who are strongly resisting this technology. The debate is a complex one, given the different motivations for monitoring as well as the variety of ways that one can utilise this technology.

¹ School of Psychology, Queen's University Belfast, UK. <mailto:m.whitty@qub.ac.uk>

While this paper acknowledges the breadth of this debate, it focuses mostly on Australian employees' attitudes towards Internet and email usage and these people's opinions on filtering software as a surveillance device.

Arguments Supporting Monitoring

Those who are supportive of Internet and email surveillance raise the point that such surveillance is necessary given that individuals in the workplace often misuse the Internet. For example, employees have been known to download inappropriate content, such as pornography, and have been caught '*cyberslacking*' (overuse of the Internet for purposes other than work). As Davis (2001) points out, the U.S. Treasury Department found that Internet activities, such as personal emails, using chat rooms, shopping and checking personal finances and stocks accounted for 51% of employees time spent online. Obviously, cyberslacking can be a problem for companies as this can lead to loss of productivity and could be considered a waste of companies' resources. Hence, some employers are turning to surveillance technology as a way to identify less productive employees.

Employers who affirm that they have a right to monitor the Internet and email in the workplace often advocate that being the owners of the computer systems gives them this right. The other dilemma, of course, is that if the computer systems are considered to be company property then companies are potentially liable for how their employees use this property. Therefore, if employees use this property for harassing or illegal purposes, part of the blame could be attributed to the employer for allowing such usage of their property. As Davis (2001) claims

Employees can also sue their employers if a co-worker has downloaded pornographic or racist materials. Clearly, it has become essential for companies to be aware of what their employees are downloading from the Internet, and for them to take steps to avoid liability by introducing employee Internet management strategies.

This perhaps varies from country to country; however, it is still an important point to consider within this ongoing debate.

Arguments against Monitoring

Those who have argued strongly against monitoring of the Internet in the workplace draw comparisons between the use of the Internet and more traditional modes of communication. Campaigners against monitoring have highlighted that the telephone has traditionally been accepted as a mode of communication used for private purposes. Given that the telephone and email share similarities as modes of communication – they argue that Internet usage should be acceptable for private purposes in the workplace, such as a quick email to one's loved one, or to organise a social gathering with friends. For example, Michael Gadiel (cited in Fisher, 2002), a member of the Labour Council of NSW, has suggested that companies need to provide access to email "for reasonable personal use, just as they would with the telephone."

In our attempts to understand the complexity of this debate social researchers and policy makers need to clarify whether the Internet and email is a private or a public space or if indeed it can be

both. For example, Sharf (1999) asserts that “despite widely announced admonitions concerning the potential for public exposure, there exists the paradox that writing to others via e-mail often feels like a private or, in the case of an on-line group, quasi-private act” (p. 246). At this point, there is probably no definitive answer as to how cyberspace ought to be conceptualised and, of course, one’s objectives have some influence over how one perceives this space. It might serve an employer’s best interest to perceive the Internet as a public space, since this would justify any desire they might have to survey their employees. In contrast, it might serve an employee’s best interest to perceive the Internet as a private space, where their employer has no right to intrude upon and effectively spy on them.

Another, perhaps less intuitive argument against surveillance of the Internet and email in the workplace, is that monitoring can actually lead to poorer task performance, as opposed to curtailing cyberslacking. Past research has demonstrated that the presence of others does affect task performance. As far back as the 1960’s, Zajonc (1965) argued that social presence impairs the performance on difficult tasks, and improved the performance on 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!*” (p. 545). 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. In respect to monitoring being used to measure performance levels, 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 supervisor for their shorter than average call record. Chalykoff and Kochan (1989) have argued that employees’ satisfaction with computer-aided monitoring has a large impact on overall job satisfaction. Indeed, it could also be that employees’ satisfaction is related to the types of Internet and email monitoring that are implemented at work.

Australian Context

In developing surveillance legislation in Australia, the issue of private versus public space has been at the forefront of the debate. For example, in the New South Wales Law Reform Commission report 98, the difficulties in defining what constitutes a public space have been outlined (Goldring, Adams, Graycar, & Ross, 2001). These authors point out, for instance, that in NSW an office space is not considered private when the door is opened. Given the problems in finding consensus around what constitutes private and public space, these authors propose “that surveillance legislation which includes in its scope only activity that is considered to be private, is weak and unsound in policy and practice. It leaves too much potentially inappropriate activity unregulated and provides insufficient privacy protection” (50). Moreover, Goldring et al. (2001) contend that there is a lack of consistency across the Australian States as to what is regarded as private and public space. Taking this one step further, as argued earlier on in this paper, it is also contentious as to whether cyberspace is private or public space.

There is still much work to be done in regards to Internet and email surveillance legislation within Australia. As pointed out by Goldring and his colleagues, to date, the Commonwealth Interception Act covers voice communications, but does not adequately address Internet and email communications. Furthermore, there is an urgent need to develop such legislation in respect to the workplace. It has been suggested by Goldring et al. (2001) that if surveillance of the Internet and email is deemed to be acceptable in the workplace, then not only should this surveillance be overt, but the “employees must have ‘actual knowledge’ of the surveillance” (p.420).

This study

Both the arguments made for and against surveillance in the workplace are compelling. However, when we consider the utility of surveillance in the workplace, it is limiting to consider the Internet as one generic space. (In this paper the Internet and email are considered to be two distinct tools). Moreover, we should not lose sight of the fact that surveillance is employed for a number of reasons.

There are numerous questions that warrant addressing in respect to Internet monitoring, many of which are beyond the scope of this current study. Rather than focus directly on the effect of computer-monitoring on job performance indicators, this paper considers Australian employees’ attitudes towards appropriate Internet and email usage in the workplace, as well as their attitudes towards filtering software. Kidwell and Bennett (1994) posit 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” (p.48). Aiello (1993) has also suggested potential factors that might moderate the effects of computer monitoring. For example, he has questioned whether employees participation in the design and implementation of the system might make a difference. Furthermore, he has questioned whether employees’ full comprehension of the monitoring system (e.g., when and why monitoring is taking place) makes any difference to the effects of computer monitoring in the workplace. This study also takes this into consideration.

Given the dearth of available research in this area, hypotheses were not devised here. Instead, this study was interested in whether gender, working for a company which has implemented a company policy, and number of hours of Internet usage in the workplace are useful predictors of a) what types of non-work related Internet and email material employees access in the workplace, b) what aspects of the Internet and email employees believe should be banned in the workplace and c) opinions about the implementation of filtering software.

Method

Participants

Five hundred and twenty four Australians completed this survey online. Of this sample, 87% resided in urban areas within Australia, while 13% resided in rural areas. 54% of the sample were men and 46% were women. The ages ranged from 17 to 66 years, with a mean age of 37.4 years ($SD = 11.27$). The sample was more skewed toward an educated sample, with only

1% of the sample with primary school as their highest level of education achieved, 25% high school, 38% a university undergraduate degree and 36% a postgraduate degree.

The amount of hours each individual typically spent on the Internet each week in their workplace, the type of Internet services participants typically used, working in an organisation with an Internet policy and working in a company where filtering software is being utilised were also ascertained. Three percent of the sample stated that they do not typically use the Internet in the workplace, 42% used the Internet for 1-9 hours, 15% 10-29 hours, and 14% used the Internet for 30+ hours each week at work. Ninety six of the participants used email, 95% the World Wide Web, 37% newsgroups, 15% video conferencing, 10% ICQ and 8% chat. Of the sample, 62% stated that their company did have a policy on Internet usage, 19% that they did not and 19% stated that they did not know. In respect to Internet filtering, 43% of the sample worked in a company where the Internet was being filtered, 40% were not working in companies where filtering was occurring, whilst 17% did not know if the Internet was being filtered.

Materials

For this study, the '*Internet Privacy and Surveillance Survey*' was constructed. The survey consisted of both open-ended and forced choice questions. Qualitative type response questions were considered imperative to this study, given the paucity of data available on Internet and email behaviour in the workplace. It is hoped that the qualitative data generated from this survey will assist in shaping more structured surveys in future studies. The survey was divided into three parts: part 1 requested demographic details; part 2 asked questions pertaining to the Internet; and part 3 asked questions relating to email. (The demographics of the sample have been summarised under participants.)

The second part of the survey asked participants how they believed the Internet should be utilised in their workplaces. For example, they were asked what non-work related online material fellow workers should be allowed access to, as well as what online material should be banned. In addition, participants were asked what material they considered important to filter out. This question was added, since it could elicit a different response to what material participants should be banned from using. That is, participants might consider that individuals at work are trustworthy and responsible enough to follow work policies and do not require filtering software to monitor or control their Internet behaviour. The survey also included a question on the implementation of filtering software in the workplace and how individuals would prefer this to be carried out.

The third part of the survey asked questions about the content of email they received in their workplaces. Participants were given a list of potentially objectionable material and asked whether they believed emails containing this type of material were objectionable or not. They were also encouraged to add more items to this list. Behavioural responses to being sent objectionable email were also obtained. Furthermore, participants' views on the filtering of emails were also acquired.

Procedure

Participants were recruited by placing notices in Australian newsgroups and message boards requesting that individuals visit and complete the survey. It was decided to select Australian newsgroups, given that only a sample of Australians was required for this study. Google and Yahoo Australian newsgroups with over 100 members were approached. In addition, some websites (this included a range of Australian websites, including political, educational, leisure and work-focused sites) agreed to place links on their sites to the survey, with a short description of the survey included on their site.

The participants were required to fill in the entire survey before they could successfully submit it. While it is impossible to determine a response rate when a survey is held online, approximately eight emails were sent from participants who stated that they had opted not to submit their survey, given that they did not want to respond to all the survey items.

Results

As stated above, both qualitative and quantitative data were collected for this study. The results section considers, in order: a) what types of non-work related Internet and email material employees access in the workplace, b) what aspects of the Internet and email employees believe should be banned in the workplace and c) opinions about the implementation of filtering software.

Non-work Related Internet Material

Participants were asked to respond to a qualitative question on what non-work related material they believed fellow workers should be allowed to access on the Internet and their email at their place of work. A content analysis was performed on their responses. Some statements were coded for more than one theme, for example, this participant's response - sports, banking, news, was coded as recreation/entertainment, banking and information. As shown in Table 1 (below), the two items that topped the list included personal emails and perusing the web for information, such as current affairs, politics and the weather.

Logistic regressions were carried out using the Backward Wald method on the predictor variables: gender, Internet hours at work(0 hours, 1-9 hours, 10-29 hours, 30+ hours), and company policy (yes, no, don't know). As shown in Table 1 above, 19% of the sample wrote that '*personal emails*' should be allowed. The logistic regression revealed a significant main effect for gender, $\chi^2(1, N = 524) = 8.54, p = .003$ and company policy, $\chi^2(2, N = 524) = 8.67, p = .013$. More of the women (25%) included this theme, compared to the men (13%), whereas, those who did not have an Internet company policy (24%) and those who did not know (28%), included this theme more than those with a company policy (14%). Seventeen percent of the sample wrote that the Internet should be used at work for '*information*' purposes, such as reading the news of the day. The logistic regression revealed a significant main effect for company policy, $\chi^2(2, N = 524) = 10.47, p = .005$. Interestingly, those who stated that their company had a web policy (21%) were more inclined to write this theme than those who did not (10%) and those who stated that they did not know (10%).

Twelve percent of the sample stated there should be ‘no restrictions’ on using the Internet for personal reasons. The logistic regression revealed a significant main effect for Internet hours, $\chi^2(3, N = 524) = 21.01, p < .001$. Those who used the Internet the most at work (27%) stated this more than the others: 0 hours (6%), 1-9 hours (6%), 10-29 hours (13%).

<u>Themes</u>	Frequency (percentage)	Significant Results
Personal emails – people outside the workplace	97 (19%)	Gender Company policy
Information – current affairs, politics, weather, virus information, public transport, health and children’s homework	88 (17%)	Company policy
Recreation/entertainment	61 (12%)	not sig
No restrictions – workers should be allowed to access anything and everything	61 (12%)	Internet hours
Banking	54 (10%)	not sig
Should only use Internet for work purposes.	50 (10%)	not sig
Personal development – education, research, job search, library	26 (5%)	not sig
Internet tools – yellow and white pages, search engine	18 (3%)	not sig
Equivalent to the telephone – workers should be allowed to access the same type of material they typically use the phone for	11 (2.1%)	not sig
Porn	6 (1%)	not sig
Chat Rooms	5 (1%)	not sig
Jokes	4 (1%)	not sig

Table 1: Non-work Related Internet Material

Non-work related Email Material

In addition to the qualitative question described above, participants were questioned about acceptable email behaviour in the workplace. They were asked to respond to yes/no items on the following two items shown in Table 2 (below).

Logistic regressions were carried out again using the Backward Wald method on the predictor variables: Internet hours at work, company policy. The logistic regression for whether individuals believed that workers should be allowed to discuss ‘sexual matters at work using their email’ revealed a significant main effect for gender, $\chi^2(1, N = 524) = 22.73, p < .001$, and Internet hours $\chi^2(2, N = 524) = 7.81, p = .05$. Men (41%) were more likely to respond with a yes to this item compared to women (20%). Those who claimed to spend on average 0 hours per

week on the Internet answered yes to this item (59%) more than the other groups: 1-9 hours (25%), 10-29 hours (35%) and 30+ hours (37%).

Items	Frequency (percentage)	Significant Results
Do you think it is acceptable for workers to discuss sexual matters at work using their email?	166 (32%)	Gender Internet hours
Do you think that workers should be allowed to use company email for other personal reasons unrelated to work?	456 (87%)	not sig

Table 2: *Non-work related Email Material*

Aspects of the Internet and Email that Should be Banned in the Workplace

Participants were asked to respond to another qualitative question, which asked what aspects of the Internet and email should be banned in the workplace. A content analysis was performed again on their responses. As illustrated in Table 3 below, offensive material was a common response.

<u>Themes</u>	Frequency (percentage)	Significant Results
Offensive material – including pornography, unethical material, discriminating material, criminal material, and violence	318 (61%)	Gender Company policy
There should be no banning	68 (13%)	Company policy
Recreation/entertainment	60 (12%)	not sig
Anything not related to work	45 (9%)	not sig
Gambling sites	25 (5%)	not sig
Against departmental policy	21 (4%)	not sig
Chat	20 (4%)	not sig
Private email	9 (2%)	not sig
Sites with viruses	5 (1%)	not sig

Table 3: *Banned Internet and Email Material in the Workplace*

Logistic regressions were carried out again using the Backward Wald method on the predictor variables: Internet hours at work, company policy. Sixty-one percent of the sample wrote that ‘*offensive material*’ should be banned in the workplace. The logistic regression revealed a significant main effect for gender, $\chi^2(1, N = 524) = 8.58, p = .003$, age $\chi^2(3, N = 524) = 12.24, p = .007$, and company policy, $\chi^2(2, N = 524) = 12.94, p = .002$. More of the women (67%) included this theme, compared to the men (55%). Those with a company policy were

more likely to state that offensive material should be banned (65%), compared to those who did not (48%) and those who did not know (59%). Thirteen percent of the sample stated that *'there should be no banning'*. There was a significant main effect for company policy $\chi^2(2, N = 524) = 15.04, p = .001$. Those without a company policy (24%) were more likely to state that there should be no banning, compared to those who did have a company policy (9%), and those who did not know (14%).

Web Filtering

In addition to questions on what Internet material ought to be banned in the workplace, participants were asked about which aspects of the Web they thought their employer should filter? The themes that were generated from this qualitative question are presented in Table 4 below:

<u>Themes</u>	Frequency (percentage)	Significant Results
Offensive material – including pornography, unethical material, discriminating material, criminal material, and violence.	192 (37%)	not sig
Should not filter anything	100 (19%)	Company policy Internet hours
Filter everything	23 (4%)	not sig
Viruses	22 (4%)	Company policy
Spam	15 (3%)	not sig
Non-work material	14 (3%)	not sig
Filter everything according to departmental policy	13 (3%)	not sig
Gambling sites	11 (2%)	not sig
Recreation/Entertainment	9 (2%)	not sig
Chat	8 (2%)	not sig
Large /bandwidth	7 (1%)	not sig

Table 4: Web Filtering in the Workplace

Nineteen percent of the sample stated that *'filtering should not be used in the workplace'*. There was a significant main effect for company policy $\chi^2(2, N = 524) = 9.69, p = .008$. Those who worked in an organisation without a company policy (28%) were more likely to state this compared to those who did (15%) and those who did not know (23%). There was also a significant main effect for Internet hours $\chi^2(3, N = 524) = 8.45, p = .04$. Those who used the Internet the least, 0 hours (29%) and the most at work, 30+ (25%) stated this more than the

others: 1-9 hours (13%), 10-29 hours (22%). Four percent of the sample stated that their workplace should employ filtering software to ‘*filter out viruses*’. There was a significant main effect for company policy $\chi^2(2, N = 524) = 6.71, p = .035$. Those who did not have a company policy (10%) were more likely to state this than those with a company policy (3%) and those who did not (2%).

In addition to the qualitative data presented above the participants were asked a few quantitative questions, where they were asked to rate items on a 5-point Likert scale, with 1 representing strongly agree and 5 representing strongly disagree. The means and standard deviations for each of the items are presented in Table 5 below:

Item	Mean (SD)	Significant Results
I approve of my employer using filtering software to control access to certain websites at work if I am informed	2.25 (1.32)	Internet hours Company policy
Workers should be allowed to access sexual material on the Web at work	4.22 (1.15)	Gender Internet hours Company policy
Workers should be allowed to access non-work material on the Web at work	2.24 (1.11)	not sig
I would like to participate with my employer in the Web filtering process	2.51 (1.07)	Internet hours Company policy

Table 5: Views on Web Filtering

ANOVAs were performed on the items presented in Table 5. The independent variables again included: gender, Internet hours at work and company policy. For the item, ‘*I approve of my employer using filtering software to control access to certain websites at work if I am informed*’ there was a statistically significant main effect for Internet hours [$F(3, 517) = 4.39, p = 0.005$; partial eta squared = .025], and company policy [$F(2, 517) = 7.06, p = 0.001$; partial eta squared = .027]. Multiple comparisons for Internet hours and company policy were carried out using the Scheffe method with a significance level of .05. Individuals who spent 30+ hours online ($M = 2.76, SD = .16$) scored higher than individuals who spent 1-9 hours online ($M = 2.18, SD = .09$). Those who did not have a company policy ($M = 2.75, SD = .15$) scored significantly higher to those with a company policy ($M = 2.325, SD = .11$). For the item that ‘*workers should be allowed to access sexual material on the Web at work*’, there was a statistically significant main effect for gender [$F(1,517) = 17.54, p < 0.001$; partial eta squared = .033], company policy [$F(2, 517) = 5.56, p = 0.004$; partial eta squared = .021], and Internet hours [$F(3, 517) = 3.43, p = 0.041$; partial eta squared = .016]. Women ($M = 4.20, SD = .10$) scored higher on this item compared to men ($M = 3.79, SD = .09$). Those who had a company policy ($M = 4.23, SD = .09$) scored significantly higher than those without a company policy ($M = 3.88, SD = .13$). Furthermore, those who spend 1-9 hours ($M = 4.27, SD = 0.08$), scored higher than those who spend 30+ hours ($M = 3.90, SD = .14$). There were significant differences for the item ‘*I would like to participate with my employer in the Web filtering process*’ including differences for Internet hours [$F(3, 517) = 3.96, p = 0.008$; partial eta squared = .022], and company policy [$F(2, 517) = 3.70, p = 0.03$; partial eta squared = .014].

Multiple comparisons revealed that those who on average spend 0 hours online ($M = 3.07$, $SD = .26$) scored significantly higher than those who spend 10-29 hours online ($M = 2.46$, $SD = .08$). Multiple comparisons also revealed that those who did not have a company policy ($M = 2.86$, $SD = .12$) and those who did not know ($M = 2.82$, $SD = .12$) scored significantly higher than those who did ($M = 2.57$, $SD = .09$).

Email Filtering

Participants were asked to provide yes/no responses to whether they believed a particular type of email was objectionable. These are shown in Table 6 below:

Items	Frequency (percentage)	Significant Results
Chain email	472 (90%)	not sig
Nuisance messages – e.g., get an easy PhD	465 (89%)	not sig
Credit offers	463 (88%)	not sig
Money-making offers	454 (87%)	not sig
Porn	402 (77%)	Gender Company policy
Email list	389 (74%)	not sig
Jokes	91 (17%)	gender

Table 6: Participants who Responded stated that the Following Types of Emails were Objectionable

Logistic regressions were again performed using the same predictor variables. The logistic regression for 'porn' revealed a significant main effect for gender, $\chi^2(1, N = 524) = 31.17$, $p < .001$, and company policy $\chi^2(2, N = 524) = 20.02$, $p < .001$. Women (87%) scored higher than men (68%) did. Those who had a company policy (82%) were more likely to object to porn than those who did not (70%) and those who did not know (68%). There was also a significant gender effect for jokes, $\chi^2(1, N = 524) = 5.12$, $p = .024$. Men (21%) objected to jokes more than women did (13%).

In addition, participants were requested to include any other emails that they found objectionable. While few responded to this question, (which made it impossible to carry out a quantitative analysis on) the following responses were elicited: unsolicited emails, religious, advertising, emails forwarded without the author's permission, Microsoft propaganda, emails containing viruses, Internet petitions, pictures, urban myths and free gifts.

Opinions about Filtering Software

Finally, participants were asked to express their views on filtering in the workplace. They were asked to rate on a 5-point Likert scale, with 1 representing strongly agree and 5 representing strongly disagree, the following items presented in Table 7 below:

Items	Mean (SD)	Significant Results
I am not worried about unsolicited email at work	2.96 (1.27)	not sig
I am happy with my email being monitored at work	3.28 (1.42)	Gender Company policy
I welcome offensive materials being filtered from my work email	2.48 (1.33)	Gender Company policy

Table 7: Views on Filtering Software

ANOVAs were performed on the items presented in Table 7. The independent variables again included: gender, Internet hours and company policy. There was a significant gender [$F(1, 517) = 7.21, p = 0.007$; partial eta squared = .014], and company policy [$F(2, 517) = 15.25, p < 0.001$; partial eta squared = .056], effect revealed for the item *'I am happy with my email being monitored at work'*. Men ($M = 3.80, SD = .11$) scored higher on this than women did ($M = 3.48, SD = .12$). Moreover, multiple comparisons for company policy revealed that those with a company policy ($M = 3.18, SD = .12$) scored significantly lower than those without a company policy ($M = 3.89, SD = .16$) and those who did not know ($M = 3.85, SD = .15$). There was a gender [$F(1, 517) = 11.50, p = 0.001$; partial eta squared = .022], and a company policy [$F(2, 514) = 9.74, p < 0.001$; partial eta squared = .036] main effect for the item *'I welcome offensive materials being filtering from my work email'*. Men ($M = 2.91, SD = .11$) scored higher than women ($M = 2.51, SD = .12$) on this item. While those without a company policy ($M = 3.04, SD = .15$) scored higher than those with a company policy ($M = 2.40, SD = .11$).

Discussion

A striking result raised by this current study was the lack of knowledge exhibited by many of these Australian participants in respect to company policy and monitoring in their workplace. Nineteen percent of the sample did not know if their company had a policy in respect to Internet usage and 17% did not know if the Internet was being filtered. Moreover, an outstanding number of participants (19%) stated that their company did not have a policy in respect to Internet usage. This compares to Greenfield and Davis' (2002) US study, which found that 17% of the organisations that they surveyed did not have a company policy. In addition, the result that 10% of the sample use ICQ and 8% use chat rooms in the workplace suggests that some Australians are using the Internet at work for play (a type of play that can be rather time consuming). This gives further support to employers' concerns that some of their employees are cyberslacking. Overall, these results suggest that Australian companies need to urgently address the means by which policies are communicated to their employees. These results also imply that some companies in Australia will be breaking the law if new legislation is brought in (as

suggested at least in NSW, by Goldring et al., 2001) requiring organisations to not only be overt about their Internet and email surveillance, but to also ensure that their employees have ‘actual knowledge’ of the surveillance.

This study elicited an interesting list of non-work related material that participants believed they should have access to in the workplace. Although the percentages do not represent whether all participants believed that one should have access to this material (since this was an open-ended qualitative question) it is probably not surprising that personal emails topped the list; especially, given that some have emphatically argued that the phone and email should be considered as similar modes of communication (e.g., Gadiel; cited in Fisher, 2002). It is noteworthy that those who use the Internet for the most amount of time in the workplace were most likely to write that there should be no restrictions on access to the Internet. Further research is required to determine if these particular individuals hold such views because they are using the Internet for extended periods for work (and their work requires that they access numerous online sites – making restrictions impracticable) or whether these individuals are ‘cyberslackers’. Another important result revealed here was the amount of people (17%) who wrote that one should be allowed to use the web at work to access information, such as news, politics and the weather. Hence, in some ways the Internet is just another tool to carry out some of the non-work activities we already engaged in at work (such as personal phone calls or reading the newspaper); however, it is also adding to the range of possible non-work related activities. Such results suggest that we are currently in the process of re-establishing the rules as to what types of non-work related activities are deemed appropriate in the workplace. Perhaps these new activities are replacing old ones, such as cigarette breaks and chats around the water-cooler.

Sixty one percent of this sample responded that offensive material should be banned in the workplace. Women stated this more than men did. Women also disagreed more strongly than men did to the quantitative question that asked whether workers should be permitted to access sexual material on the Internet at work. Perhaps this is because such material harasses or offends women more than it does men. Despite this strong opposition towards offensive material in the workplace, 32% of the sample stated that it was accepted to discuss sexual matters at work using their email. Men stated this more than women did, again perhaps because men are less likely to see this as offensive or harassing. Those who used the Internet on average 0 hours per week were also more likely to say this was acceptable than the other participants. It could be that these individuals are less savvy when it comes to Netiquette. Such results highlight the need to make transparent the more specific details about what is acceptable email behaviour in the workplace and where email discussions might border on harassment. Furthermore, these results suggest that rather than being strongly divided for or against Internet and email monitoring, that individuals are simultaneously arguing both for and against this kind of surveillance. That while, they believe that offensive material is unacceptable within the workplace, they do not necessarily believe that what they are doing online could be deemed offensive.

Previous research carried out by Novell in 1998 in the UK found that 41% of the women in their sample had been sent pornographic material or were harassed on the Internet (Gumbel, 1999). In considering both these studies, side by side, the implication is that companies do need to ensure that policies reflect individuals’ concerns about offensive material. Moreover, individuals

need to internalise that these rules also apply to their own behaviour. In addition, it does raise some concerns about harassment in the workplace and future research needs to consider what specific types of harassment people are experiencing and how we might best deal with this problem. In addressing this issue, we need to bear in mind that nature of email. Email, unlike face to face or telephone conversations, can present the illusion of a private forum. For example, there is the possibility that others might overhear a telephone conversation where one harasses another over the phone. This of course would act as a deterrent for individuals to use the phone in this way. However, while there is the illusion that what you send to another over the email will only be read by that same individual, the reality can be quite different. In addition, once material is sent via email some individuals fail to register that this is a permanent record (this is different to letter writing where it is obvious that the letter can be a permanent record), and unlike a conversation face to face or a telephone conversation, can in fact come back to haunt a person.

Interestingly, those who did not have a company policy stated more than those who did have a policy, that there should not be any Internet material banned in the workplace. A possible explanation for this result could be that company policies are actually quite successful in those companies which hold them and that these policies are not preventing workers from accessing Internet sites that they need to and desire to visit. Again this implies a need for further discussion in the workplace as to what is considered appropriate Internet and email behaviour.

Although over half of the participants stated that they wanted offensive material banned from the workplace, this current study suggests that filtering software is not the only way forward to the prevention of offensive material. In fact, only 37% of the participants stated that they would like their employer to utilise filtering software to filter out offensive material. It is also noteworthy that those who did not have a company policy and those who used the Internet the most at work stated that their employer should not be using filtering software. This result was replicated in the quantitative question that asked if participants approved of their employers using software to control access to certain websites at work. Hence, it might be concluded from this study that while filtering software can be a useful tool for some companies, it is probably not the only or most popular solution. Perhaps the use of this software is more appropriate in some workplaces as opposed to others, or perhaps this depends on how the software is implemented. For example, how the workers are informed or involved in the process, what content is filtered, and who is in control of the filtering process might affect individuals' opinions towards Internet and email filtering in the workplace.

A fascinating and unexpected result yielded from this study was the participants' responses to objectionable emails. The highest rating objectionable email was chain email, which rated higher than porn emails. This result is perhaps counter-intuitive given that chain emails are most often sent by a person known to an individual. While discourses are bantered around in respect to the need utilise sophisticated software to control for unwanted spam sent by organisations attempting to sell their wares, this result suggests that there is another type of email that we need to control for. Rather than filtering software being the ultimate solution to all our email frustrations – this result highlights a need to redress what is appropriate Netiquette. While forwarding on an email can occur in seconds with the click of a button, the sifting through of relevant and irrelevant email can be time consuming. Although the intention behind the email might be virtuous (e.g., signing

petitions) the receiver might not always be interested in these causes or has perhaps been sent the same email on several other occasions by other friends with a social conscience. Again this result implies, that while individuals might have strong attitudes towards what's inappropriate behaviour online, they do not necessarily believe that this relates to them. This would, in part, explain the increase in chain emails.

In concluding, the results from this study do support the notion, as suggested earlier on in this paper, that adopting an either/or view on Internet surveillance can be problematic. A fourth purpose for surveillance has also been revealed in this study; that is, to save workers wasted time sifting through unwanted email. However, rather than reducing the solution to a reactionary approach this study suggests that we need to also consider appropriate Netiquette so that unwanted emails are not sent in the first instance. These results also highlight that there is no silver bullet when it comes to dealing with Internet and email problems in the workplace. While filtering software and clear policies can be part of the solution, these results suggest that the solution also needs to be tailored made to fit both organisations' and individuals' needs. Although this study does contribute to this important debate, more research into the attitudes of Internet filtering in the workplace and how the Internet and email is used in the workplace is critical. For example, future research might consider different types of workplaces as well as different levels of responsibility and level of management. The way forward is not to reduce the debate to outcomes of productivity. Instead, as suggested by Kidwell and Bennett (1994) we need to take account of the workers' opinions.

References

- Aiello, J. R. (1993) Computer-based work monitoring: Electronic surveillance and its effects. *Journal of Applied Social Psychology*, 23: 499-507.
- Aiello, J. R. and Svec, C. M. (1993) Computer monitoring of work performance: Extending the social facilitation framework to electronic presence. *Journal of Applied Social Psychology*, 23: 537-548.
- Chalykoff, J. and Kochan, T. A. (1989) Computer-aided monitoring: Its influence on employee job satisfaction and turnover. *Personnel Psychology*, 42: 807-834.
- Davies, R. A. (2001) *Cyberslacking: Internet abuse in the workplace*. Retrieved August 20th, 2001 from the World Wide Web: <http://www.internetaddiction.ca/cyberslacking.htm>
- Fisher, V. (2002) *Is it OK to monitor employees?* ZDNet Australia. Retrieved September 17th, 2002 from the World Wide Web: <http://news.zdnet.co.uk/story/0,,t300-s2118847,00.html>
- Goldring, J., Adams, M., Graycar, R., & Ross, I. (2001) Report 98 (2001) - Surveillance: an interim report. Sydney, Australia: Law Reform Commission Publications.
- Greenfield, D. N. and Davis, R. A. (2002) Lost in cyberspace: The web @ work. *CyberPsychology & Behavior*, 5: 347-353.
- Gumbel, A. (1999) Techno detectives net cyber-stalkers. *Independent on Sunday*, January 31: 17.
- Irving, R. H., Higgins, C. A. and Safayeni, F. R. (1986) Computerized performance monitoring systems: Use and abuse. *Communications of the ACM*, 29: 794-801.

- Kidwell, R. E. and Bennett, N. (1994) Employee reactions to electronic control systems: The role of procedural fairness. *Group and Organization Management*, 19: 203-218.
- Sharf, B. F. (1999) Beyond Netiquette: The ethics of doing naturalistic discourse research on the Internet. In S. Jones (ed.) *Doing Internet research: Critical issues and methods for examining the net*. Thousand Oaks: Sage Publications, 243-256.
- Susser, P. A. (1988) Electronic monitoring in the private sector: How closely should employers supervise their workers? *Employee Relations Law Journal*, 13: 575-598.
- Zajonc, R. B. (1965) Social facilitation. *Science*, 149: 269 - 274.