ACTU
australian council of trade unions

level 6 365 queen street
melbourne victoria 3000
t +613 9664 7333
f +613 9600 0050
w actu.org.au

President Sharan Burrow
Secretary Jeff Lawrence

Committee Secretary
Senate Standing Committee on Environment, Communications and the Arts
PO Box 6100
Parliament House
Canberra ACT 2600

Via e-mail: eca.sen@aph.gov.au

Friday, July 23, 2010

Inquiry into the adequacy of protections for the privacy of Australians online

Our organisation is the peak national body representing trade unions. We welcome the opportunity to make a submission to the above inquiry.

We agree that it is timely to re-examine the adequacy of privacy protection in light of technological advances in online services and changed social and usage patterns, including a broader demographic among the users.

Our key concerns in this space relate to the adequacy of privacy protections for workers using online services:

- At work;
- Away from work, on employer owned equipment; and
- Away from work, on their own equipment.

At our 2009 Congress our affiliates endorsed a *Decent Work Agenda,* which included the following policy points relevant to this enquiry which we are committed to pursing:

- Employers should respect employees' freedom of communication. Unless there are exceptional circumstances, employees should not be prevented from discussing their employment with friends, family or union, or from making complaints of corrupt or inappropriate conduct by their employer.

- Employers should respect employees' privacy. Employees' personal information should be collected and handled in accordance with the National Privacy Principles.
- Some technologies bring employees' private lives into the workplace. These include internet access to personal e-mail and social networking sites, or access to online banking sites. Unions believe that to a reasonable extent, use of these technologies in the workplace is acceptable. Employers should not automatically ban access to these sites, in the absence of any evidence of abuse. Similarly, employees should not be disciplined for making reasonable use of the internet for private purposes on work time.
- Some technologies allow the employer to better monitor employee whereabouts and performance. These include video cameras, GPS devices, barcode scanners, electronic sign in machines, computer keystroke trackers and so forth. Unions support certain reasonable uses of such technologies, for instance to promote employee safety. However, unions oppose the use of such technologies where a major purpose is to spy on employees for disciplinary purposes, or intensify work.
- In particular, unions strongly believe that employers must not monitor employees movements or private communications without their express, informed and genuine consent (and where the granting of such consent cannot be made a condition of employment, promotion, or pay rise). Such monitoring is illegal in Victoria, and should be made illegal elsewhere.

We set out our concerns below where relevant in response to the terms of reference for the instant inquiry.

(a) Privacy protections and data collection on social networking sites

Social networking services are a medium through which people communicate with one another. Users of the services may do so for commercial, political, entertainment or social reasons. Whilst a small number of persons use these services as a requirement of their employment, for example persons employed in advertising or public relations roles, the overwhelming use of this service by

Austalian workers is for purposes which they would consider as "personal". In this regard, the use of social networking services is akin to that the use of e-mail, telephony services and indeed face to face discussions in that they are all different forms of having a conversation.

Our understanding of social networking sites is that they generally enable the user to specify the scope of persons who can observe the conversation, or contain some level of advice to users (although not necessarily in the most accessible fashion) that the information they "post" is or may be publically available and/or becomes the property of the service provider once it is posted.

Notwithstanding the capacity to restrict the participants to an online conversation at first instance, the reality is that (as with any other communication or conversation) the online conversation can be referred to or quoted outside of the forum in which it occurs, either by a participant in the conversation or a covert observer to it. For this reason, it is desirable that the terms of use of social networking services are in plain language and that users are fully informed of the *direct* or first instance availability of the information posted on the service. In addition, users should be advised of the potential for *indirect* reproduction or use of the posted material (for example by quoting, forwarding, e-mail, printing etc).

Further, it might assist if the terms of use of social networking services included terms to the effect that persons who are able to access the device(s) on which a user accesses the service (for example an employer) may become aware of the content of information accessed or submitted by the user, and that the user may be obliged by their employer to refrain from accessing or submitting certain types of information to the service.

(b) Data collection activities of private companies

As highlighted above, our primary concern is not with the privacy controls required of the operators of online services, provided there is a transparent disclosure by the service provider and consent by the users of the service, but with the privacy protection of users of these services in the employment context.

Employers have the capacity to monitor their employees' activities. Online technology has heightened this capacity. Monitoring of online activities may be actively pursued by employers, or alternately the contents of an employee's online activity may be reported to the employer by another employee or a third party. The extent to which employees' privacy is appropriately protected in this setting is marred by the complex application of the "employee records exemption" to the *Privacy Act* 1988[1] and the common law employment duties and obligations relating to confidentiality, good faith, trust and confidence, reasonable directions and bringing the employer into disrepute. The application of all of these legal concepts in a particular case often comes down to a question of the extent to which the employee's online activity is related to or impacts on their employment relationship[2]. After a considered review of the law, the NSW Council of Civil Liberties concluded that protections in this area are currently insufficient and made a number of recommendations which we endorse in principle[3]. Similarly, the Victorian Law Reform Commission has identified a number of significant gaps in the privacy protections for workers as public rights while recognising that there is some scope to create more private rights through the negotiation of industrial instruments, provided of course the employer agrees to do so[4].

Use of online services at work

E-mail is widely used as a business tool in Australian workplaces. It is similarly used as a means of non-work related communication, for example in connection with the supply of personal goods and services and to converse with friends or relatives. Further, it is used extensively as an alternative to "water cooler" discussions among colleagues. Web based services including social networking media are increasingly used for these later purposes, as well as the more traditional uses such as purchase of goods and services or personal research, recreation and entertainment.

---

[1] For instance the mere assertion that monitored online activity is for "disciplinary" purposes may be sufficient to enliven the exemption.

[2] There may be other issues to consider when determining compliance with State based legislation such as the *Surveillance Devices* Acts and the NSW *Workplace Surveillance Act* 2005.

[3] "Workplace Surveillance", New South Wales Council of Civil Liberties, November 2004.

[4] See "Workplace Privacy Issues Paper", Victorian Law Reform Commission, 2002, ISBN 0 9581829 2 2.

It is readily accepted that employers have a legitimate interest in the productivity of their employees. For this reason, personal use of web-based services and e-mail, much like personal use of telephones, can legitimately be subject to reasonable limits to ensure that its usage does not unreasonably interfere with the performance of an employee's duties. However, it is the means by which this is monitored that creates an opportunity to interfere with employees' privacy.

The e-mail infrastructure available at workplaces necessarily keeps a record of employee communications and activities which is readily accessible by the employer. The internet web access infrastructure at workplaces ordinarily creates an electronic "trail" by which the services the employee has accessed can later be viewed. If additional software is installed, employees' use of the web can be viewed at a remote location in real time or each interaction logged for later review. The availability of technological means for such monitoring does not mean that it is good policy or industrial relations practice to utilise it.

It seems that there is a heightened sensitivity among employers to the content of employee online communications. This may be borne of a concern that the communications are reproducible rather than transitory, have (or are perceived to have) the potential to reach a wider audience, and actually come to the employer's notice in a context where they feel it is impossible for them to be passed over or ignored. But this does not alter the fact that the communications are of a nature that is regarded as private by the employees participating in them.

To illustrate, an employee might say "The new CEO is taking the company in the wrong direction":

- to a colleague in an office tea room;
- over a drink with another colleague after work;
- to their partner after work; and
- in the company of friends on the weekend

all in the space of a week. The employee would no doubt regard each of these communications as private. No written record would be kept of them. The

employee's manager may in time learn of those comments. The manager's action toward the employee, if any, would likely be to at most disagree with the assertion about the CEO, and encourage the employee to be more discreet in future.

However, the response by the employee's manager would likely be different if the comment:

- was found on the workplace e-mail system;
- was found on paper in the office having been printed from the e-mail system by the person to whom it was directed;
- was found on a social networking site by a person who had the required access to that site (e.g. a "Facebook Friend"), and printed and brought to the attention of the manager (even if the site did not identify where the employee worked); or
- Was found by monitoring software to have been posted on a social networking site by use of the workplace computer system.

To the extent that the comment might fall within the scope of the employment relationship, the legal basis on which the employer might take exception to the comment (for example bringing the employer into disrepute or breach of duties of good faith or trust and confidence) is the same irrespective of the scenario. The nature of the comment has not changed. The medium of its communication has changed and the size of the audience of the comment *may* have changed, however as is the case with a verbal communication, this is largely beyond the control of the person who made the comment. In any event, the audience potential and the intention and identifiably of the speaker and his or her employer is far different than is the case with a submission to broadcast media such as a letter to the editor in a newspaper. In this context, the basis for differential treatment becomes questionable as does the need to monitor workplace activity in search of communications of this kind.

Notwithstanding this, there are reportedly real life examples of employees being disciplined or worse for comments which, if merely overheard in the workplace, would unlikely to attract any or any serious consequence:

- A supermarket employee reportedly being dismissed for commenting to another employee via Facebook that a third employee "will get what's coming to her"[5]
- An employee reportedly being dismissed for posting a Facebook profile update during working hours that he was "pissed off", shortly after having a disagreement with his supervisor over the telephone[6].
- Two secretaries reportedly being dismissed after having an argument via work e-mail regarding the whereabouts of the ingredients of a sandwich (the workers who circulated the e-mail exchange outside the workplace were not however dealt with as harshly)[7]

In our view, there ought to be greater controls on employer monitoring of the contents of online communications made while at work. Monitoring ought to be limited to legitimate business purposes, should not be oppressive, and should respect the privacy of employees' personal communications and activities.

As part of legitimate monitoring, we support efforts to ensure that employees do not use computers in a way which may constitute sexual harassment – for instance, by displaying offensive material on screen in a public workplace, or printing such material out on common photocopiers.

Use of online services away from work on employer owned equipment

Under this heading we are concerned with the communications made by employees when they are not "on duty" but may be "on call" or otherwise required to be contactable. Often such employees are provided with devices such as "smart phones" which provide access to telephony, e-mail and web services. These may be provided either on the basis that they are solely for business purposes, or also available for personal use.

[5] http://www.adelaidenow.com.au/news/south-australia/woman-fired-for-facebook-threat/story-e6frea83-1225852231432
[6] *Lukazsewski v. Capones Pizzeria Kyneton* [2009] AIRC 280
[7] http://www.smh.com.au/news/national/cheesed-off-by-heated-food-fight/2005/09/08/1125772641103.html

In the former case, there seems to be little room for argument that irrespective of the content of the communications initiated by the user, if the uses are not for business purposes, the employee has acted wrongly. In that circumstance, there seems to be little objection to monitoring of the usage of the device where necessary for operational or regulatory reasons to access business records retained within it or generated on it. Monitoring of unpermitted personal communications should only occur if there is evidence to suggest they have occurred and in the context of an agreed policy.

In the latter case, where the employer has accepted that personal use is permitted, there is in our view no legitimate basis for those personal communications to be monitored in the absence of consent. Any monitoring facilities would ideally be able to be activated and de-activated by the employee user in accordance with whether the communication is personal or for business purposes. It is recognised that it is likely to be more technically achievable for any monitoring and filtering to be automatically activated or de-activated based on whether the traffic originates from or is destined for the employer's network.

<u>Use of online services away from work on the employee's own equipment.</u>

We do not accept that the employer has any legitimate basis to monitor an employee's usage of their personal devices outside of working hours, for instance by hacking into private computer systems.

Where communications are made from the employee's device into the employer's own network, we submit that the views we express above in relation to the use of online services at work are relevant.

(c) Data collection activities of government agencies

We believe our comments as above are applicable to the activities of government employers, save that the position under the *Privacy Act* 1988 is ambiguous as to whether it provides greater protection of employees' personal privacy.

Although there is no "employee records" exemption in respect of an agency under the *Privacy Act*, there are qualifications contained within the Information Privacy Principles ("IPP") applicable to "agencies" that could result in the common law duties referred to above as remaining the baseline test for the reasonableness of monitoring activities. We refer in particular to the "unlawful or unfair means" limitations in IPP 1(2), the "reasonable" and "unreasonable" tests in IPP 3, the relevance test in IPP 9 and the "authorisation by law" test in IPP 10(1)(c).

(d) Other related issues

We note that the Standing Committee of Attorneys-General has decided to produce voluntary guidelines for employers on workplace monitoring and privacy. A draft of these guidelines, prepared by the Victorian Department of Justice in consultation with State, Territory and Commonwealth representatives, was recently circulated for comment to some unions and presumably other stakeholders.

We have concerns that the draft guidelines as circulated present as a "how to" guide for employers to implement invasive monitoring and treat the issue of the appropriateness of introducing monitoring as a secondary issue. Whilst we will be participating in the consultation process regarding these guidelines, we raise it as a matter that the present Committee may wish to investigate further given that the subject matter of the guidelines substantially overlaps with the terms of reference of this Inquiry.

Yours faithfully,

Trevor Clarke
Legal & Industrial Officer
Australian Council of Trade Unions