Responses to Questions on Notice

"Find a way to convince me that the ACTU is not…happy with access to information that might otherwise be regarded as private when it is aimed at protecting the rights of employees versus doing something else" [Senator Fisher (Chair) @ p. 36]

We have nothing further to add to the responses provided by Mr Fetter and Mr Clarke at pp 36-37.

"How common would you say that it is for employers to monitor the online activites of employees? Would you say that it is very common, occurs sometimes, is not common or occurs never?" [Senator Troeth @ p.42]

Notwithstanding a growing body of evidence that electronic monitoring comes at the expense of job satisfaction,[i] we would say that it is very common, and refer to our comments at pages 42-43 of the proof Hansard. Statistics as to the use of monitoring are difficult to obtain, particularly in the Australian context. Further US based data we have located is generally consistent with that to which we have already referred: 74% of employers monitoring incoming and outgoing e-mails, 60% monitoring internet connections and two in three doing so with employee knowledge or consent.[ii] Perhaps an anecdotal indicator of the prevalence of employee monitoring is the ubiquitous "Google search", where the ratio of the number of advertisements for employee monitoring software as compared to studies of the ethics of doing so is astounding, even when the search results are limited to Australia.

"In relation to international experience, what is the international best practice on this- either bargaining outcomes or legislative outcomes?" [Senator Cameron @ p.45]

To the best of our knowledge, other jurisdictions regulate employee privacy through legislation, rather than bargaining. Although bargaining may have a role to play in supplementing strong minimum legislative standards, it is clear that leaving questions of privacy to be dealt with exclusively through bargaining is inadequate, particularly if bargaining occurs solely at the individual or enterprise level. This is because employees are unlikely to have sufficient bargaining power to succeed in negotiating adequate standards, especially in non-unionised workplaces.

We note that in many other legal systems, the right to privacy is given express legal (or even constitutional/quasi-constitutional) recognition. For example, article 8 of the Council of Europe's *Convention for the protection of Human Rights and Fundamental Freedoms* of 1950 provides:

> *"(1) Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

For the member states of the Council of Europe[iii] whose national laws are civil code based (as opposed to common law), the terms of the *Convention* are self executing once it is ratified. Subject to exhausting remedies under national laws, the *Convention* may be enforced in the European Court of Human Rights. Decisions of that Court have interpreted the reference to "private life" and "correspondence" in Article 8(1) as applicable to business relations such as e-mail and telephone communications, even where the content thereof is personal.[iv]

The *Treaty of the European Union* and the *Charter of Fundamental Rights of the European Union* provide recognition of the *Convention* in the European Union. The latter now has the status of an EU Treaty, meaning that all EU Regulations must be consistent with it and it can be called into aid in interpreting EU Treaties.[v]

The operation of the Convention is supplemented by various other instruments, including the *Data Protection Directive* and the *Directive on Privacy and Electronic Communication*. Each member state of the E.U. is required to implement E.U. Directives in its national laws. As an example, the French Penal Code permits fines of up to €45,000 or imprisonment for up to 3 years for employers for covert electronic monitoring of employees.[vi] Similarly, French National laws protect the right of employees to engage in some personal use of employer computer networks including storing personal files thereon.[vii]

Question Re provision to Committee of a submission previously prepared for the Standing Committee of Attorneys General and provided to the Department of Justice, Victoria [Senators Cameron & Fisher,@ pp45-46]

The Department of Justice, Victoria, has requested that we not provide a copy of our submission to the Committee. It has however indicated it would not object to us advising the Committee of the general nature of the feedback we provided in that submission. We attach a paper entitled 'Privacy at Work' which sets out some of the material which we put to the Department.

"In respect of your contention that private activities by employees in their private time on their private equipment should remain private….is it possible to apply that in practice? How do you draw the line?" [Senator Fisher @ p.46]

We recognise that employees' activities in their private time might come to the attention of their employer through means other than the employer actively seeking the information. This might include persons bringing information existing in the public domain (whether true or not) to the attention of the employer. What, if anything, happens next must involve a genuine assessment of whether the information impinges on the employment relationship in any meaningful way. This might include whether the "public" commentary identifies the employer, and whether, notwithstanding that it is "public", the real potential audience is at all significant.

A further objection is to employers investigating such activities in advance of any genuine assessment of whether, even if the alleged "activities" were proven to have taken place, they would justify taking disciplinary action. We see such knee-jerk investigations as oppressive and as a serious violation of privacy.

References:

[i] Lee, S.M., Yoon, S.N.& Kim, J. "The Role of Pluaralistic Ignorance in Internet Abuse", Journal of Computer Information Systems 1/4/08; Young, K.K & Case, C.J., "Internet Abuse in the workplace: New trends in risk management", CyberPsychology and Behaviour ,(2004) 7(1), 105.; Arnesen, D.W. & Weis, W.L., "Developing an effective company policy for employee internet and e-mail use", Journal of Organizational Culture, Communications and Conflict, (2007) 11(2), 53; Nebeker, D.M. & Tatum, B.C. "The effects of computer monitoring, standards and rewards on work performance, job satisfaction and stress", Journal of Applied Social Psychology, (1993) 23(7), cited in NSW Council for Civil Liberties, "Workplace Surveillance", November 2004.

[ii] Rustard, M.L. & Paulsson, S.R., "Monitoring Employee E-mail and Internet Usage-Avoiding the electronic sweat shop: Insights from Europe", University of Pennsylvania Journal of Labor and Employment Law (2005) 7:4.

[iii] There are 46 member states, approximately half of which are also EU members.

[iv] See in particular *Halford v. United Kingdom* 39 Eur. Ct. H.R.1004 (1997)

[v] It achieved this status 9 years after its proclamation as a charter.

[vi] Rustad & Paulsson *Op. Cit.*

[vii] *Ibid.*