July 1998

Privacy and self-regulation: Is there any hope?

Jay Forder  
*Bond University, jay_forder@bond.edu.au*

Follow this and additional works at: [http://epublications.bond.edu.au/law_pubs](http://epublications.bond.edu.au/law_pubs)

**Recommended Citation**  

Privacy and self-regulation

Is there any hope?

by Jay Forder, Consultant Editor

In 1996 the Federal Liberal/National Party coalition made election promises to extend privacy protection to the private sector through legislation. The promise was subsequently described as a "non-core promise" and has not been implemented.¹ The Federal Privacy Commissioner, Moira Scolloy, was asked instead to help develop voluntary codes of conduct. After "broad consultation" she published national privacy principles in February this year.² We note here some of the reactions to these events, and developments elsewhere, including interesting software solutions envisaged by P3P and TRUSTe.

The content of the national principles

The principles published by Ms Scolloy are framed in general terms to be relevant to a wide range of activities. The intention is to establish a "national benchmark" to avoid different standards applying in different industries or across Australian jurisdictions.

Like the Privacy Act 1988 (Cth), the principles "reflect the ideas of the OECD guidelines".³ Thus, some of the main provisions include:⁴

- **Collection:** organisations should collect only what is necessary, and by fair means; they should take reasonable steps to forewarn the subject about who they are and what they intend to do with the information; where practicable they should collect the information directly from the subject; where information is collected from someone else they should at least take reasonable steps to notify the subject.

- **Use and disclosure:** organisations should only disclose information in ways that are reasonable and consistent with the subject’s expectations or are required in the public interest.

- **Data quality and security:** organisations should take reasonable steps to ensure that data is accurate, complete and up to date, and that it is secure.

- **Openness, access and correction:** organisations should be open about the kinds of information they hold and what they do with it; and within certain limits should provide individuals with access to the information about them and the opportunity to correct it.

- **Identifiers:** identifiers originally assigned by government agencies should only be used in certain limited circumstances.

- **Anonymity:** whenever lawful and practicable, subjects should have the option of not identifying themselves.

- **Transborder data flows:** organisations should only transfer personal information outside Australia in limited circumstances and should ensure it will be sufficiently protected.

- **Sensitive information:** highly sensitive information such as race, political opinion, religion, etc should not be collected except in limited circumstances.

Privacy advocates have been lukewarm in their reception of the principles. For example, while recognising that some of its provisions are a positive contribution, Roger Clarke suggests that it is inadequate to focus on data privacy to the exclusion of other concerns, such as privacy in communications. He also suggests that the detail of the use and disclosure self-regulatory regime would show an alarming sympathy for lobby groups such as the direct marketing industry and outdated national security interests.⁵

Perhaps the strongest criticism is that the principles are based on an old and well-worn view of data privacy. They do not take account of modern concerns. How much they reveal about themselves depends on who they are communicating with, the purpose of the communication, and how much trust exists. The suggestion is that we need a model that allows the same discriminating behaviour on the Internet.

The requirements for effective self-regulation

Much will obviously depend on the way in which a self-regulatory model is implemented. Indeed, the Privacy Commissioner herself acknowledges the importance of a number of “implementation issues” to be addressed in a “second stage” in the future. According to Ms Scolloy, these include issues such as which organisations adopt the principles, the mechanisms for dealing with complaints and compliance, whether the principles apply to employees, and whether they apply to information collected before the principles are adopted.⁶

It is interesting to note that the Clinton Administration’s Department of Commerce hosted a national summit in the USA on 23-24 June to discuss this topic. The conference will debate the “Elements of Effective Self-Regulation for Protection of Privacy”, the subject of a brief discussion draft published by the Department in January.⁷ As a starting point for discussion the US paper suggests that an effective self-regulatory regime would need:

- readily available and affordable recourse to dispute resolution procedures for consumers;
- verification of the representations an organisation makes about its privacy practices; and
- meaningful and swift consequences for failure to comply with fair information practices.

We await more detailed suggestions that might come out of the US conference. In the meantime, progress continues to be
made with two interesting industry initiatives.

**The Platform for Privacy Preferences (P3P)**

A working draft of the syntax specification for P3P was made public by the World Wide Web Consortium (W3C) on 19 May 1998. P3P is a protocol or standard that enables:

- the provider of a web site to specify its own personal data and privacy practices;
- a web user to specify their own preferences and expectations; and
- software to be written to use these specifications in working behind the scenes to broker an acceptable agreement between both parties.

The software could be used to provide users with sufficient information to make informed decisions themselves, or it could act as an "intelligent" agent and make decisions automatically based on the specified preferences. It envisages the user being able to specify preferences for multiple personas. This would give the user a lot more control over what information they release and to whom.

**TRUSTe**

The Electronic Frontier Foundation and CommerceNet got together with the support of several major industry sponsors (including Netscape and IBM) and two well-known accounting firms (KPMG and Coopers & Lybrand) to design a program that takes advantage of labelling and certifying privacy practices. TRUSTe issues a Trustmark™ that rates a web site’s privacy practice in three strengths:

(a) no exchange, which means that the site will not capture any personally identifiable information for anything other than billing and transactions initiated by the user;
(b) 1-to-1 exchange, which means that the site will not disclose data to third parties; and
(c) third-party exchange, which means that the site may disclose data to third parties provided it explains what information is being gathered and with whom it will be shared.

The interesting thing about TRUSTe is the lengths to which they will go to verify that their Trustmarks are accurate. For example, they do spot audits, and seed a site with fake data to check how the data is being used. For these reasons, TRUSTe is gaining many converts.12

**Conclusions**

There is certainly cause for concern that not enough is being done by the Federal Government to address privacy issues in Australia. A self-regulatory code of conduct on its own will not suffice. Compliance with the principles needs to be enforced in some way. Hard decisions need to be made about how this will be implemented and what resources will be needed.

---

**Video Surveillance Act**

The use of covert video surveillance in the workplace is now regulated under the Workplace Surveillance Act 1998, (NSW) which was assented to on 29 June 1998. The Act makes it an offence to conduct covert video surveillance of employees unless it has been authorised by a Magistrate. The Magistrate must be satisfied that there are reasonable grounds to suspect that one or more employees are involved in unlawful activities at the workplace before issuing the authority. At the same time, the Magistrate must take into account whether the proposed surveillance would unduly intrude on the privacy of employees or any other person.

**What is covert surveillance?**

The Act defines surveillance as being covert unless:
- the employee has been notified in writing at least 14 days before the intended surveillance is conducted (unless the employee agrees to a lesser period); and
- cameras, or evidence of their existence, are clearly visible at the workplace; and

- clearly visible signs at the entrance to the workplace notify people that they may be under video surveillance.

Despite the above provisions, however, video surveillance will not be covert if a majority of employees has already agreed to video surveillance of the workplace generally, as distinct from surveillance of the activities of employees.

**Conditions of surveillance authority**

The Act provides for a number of conditions relating to the application for an authority, conduct under an authority and the use of video tapes made under an authority. Importantly covert video surveillance of an employee in a toilet facility or shower or other bathing facility, or to monitor work performance, will not be authorised in any circumstances.

For further information on the Act and ongoing commentary on the topic see the CCH loose leaf reporting service, Human Resources Management.