Cyberspace Law and Policy Centre
A Centre for the Public Interest in Networked Transactions

Distinguishing PETs from PITs: Developing technology with privacy in mind

Submission to the Australian Law Reform Commission
on the Review of Australian Privacy Laws Discussion Paper 72 (DP72)

Abi Paramaguru
Research Assistant, Interpreting Privacy Principles Project
Cyberspace Law & Policy Centre, UNSW Faculty of Law

David Vaile
Executive Director
Cyberspace Law and Policy Centre, UNSW Faculty of Law

Nigel Waters
Principal Researcher, Interpreting Privacy Principles Project
Cyberspace Law & Policy Centre, UNSW Faculty of Law

Graham Greenleaf
Professor of Law
University of New South Wales

7 March 2008

Note: submissions in this document number consecutively following on those in our separate submission on the Unified Privacy Principles; on Promotion and Enforcement; on Credit Reporting Provisions; on Exemptions and on a Statutory Privacy Action in Australia.

Research for this submission is part of the Interpreting Privacy Principles Project, an Australian Research Council Discovery Project

Table of Contents

Introduction

Structure of Submission

This submission responds to Part B 'Developing Technology' of the Australian Law Reform Commission's Discussion Paper 72 *Review of Australian Privacy Law*, September 2007, which deals with the relationships between developing technologies and the *Privacy Act* 1988. We draw attention to differing issues arising from 'privacy-invasive technologies' (PITs) and privacy-enhancing technologies (PETs).

We have made separate submissions on Part D – the proposed Unified Privacy Principles (UPPs); Part F - the promotion and enforcement of the principles, Part G - the Credit Reporting Provisions, Part E – exemptions from the *Privacy Act* and Chapter 5 - protection of a right to personal privacy.

Background – the iPP Project

Research for this submission has been undertaken as part of a Discovery project funded by the Australian Research Council, 'Interpreting Privacy Principles' (iPP). The home page for the project, and other publications relating to the project, are at <http://www.cyberlawcentre.org/ipp/>. The iPP Project is based at the Cyberspace Law and Policy Centre at UNSW Law Faculty.

The principal objective of this research is to conduct over the course of the project (2006-09) a comprehensive Australian study of:

(i) the interpretation of information privacy principles (IPPs) and 'core concepts' in Australia's various privacy laws, particularly by Courts, Tribunals and privacy regulators;

(ii) the extent of current statutory uniformity between jurisdictions and types of laws, and

(iii) proposals for reforms, in order to help obtain better uniformity, certainty, and protection of privacy.

ALRC Chapter 6. Overview - Impact of Developing Technology on Privacy

The development of new technologies has the potential both to create new privacy intrusions and obstacles to preserving privacy never previously envisaged as well as address privacy concerns, by enabling control, monitoring and permission revocation by individuals.

Technology often seems to lead to the erosion of our ability to perform everyday activities anonymously. The development of biometrics, RFID and the pervasiveness of data matching are all examples of technologies that cause this concern.

Privacy law should be both robust enough to address the technological concerns we face today, and adaptive enough to tackle new and unforseen hurdles.

Questions of technological neutrality are also critical: how to both offer guidance specific enough to apply to any practical technology, but to also focus on principles that are not undermined by the practicalities of a different 'platform'.

Other Technologies

The ALRC notes that it is interested in hearing about technologies other than those that they have addressed in Chapter 6 that may impact on privacy (DP 72, [6.97]).

It is not feasible to enumerate 'developing technologies' that will have an impact on privacy into the future, because the functionality, categories and scope of technologies with privacy impact is vast. Hence the need arises for a regulatory framework that can readily be applied to as yet unthought-of innovations.

Aspects of developing technologies that warrant closer inspection, but generally receive relatively little attention from the ALRC, include:

- targeted advertising (for example Google AdSense, mobile phone Bluetooth advertising, or websites advertising to children such as Neopets.com)
- automatic number plate recognition
- automatic face recognition
- sensor miniaturisation and nano-technology
- DNA sampling, sequencing and analysis
- Biological sensors and instrumentation
- New models for pattern analysis of massive data sets of all sorts
- ubiquitous surveillance models being built into networking tools, and driven by law enforcement seeking ubiquitous surveillance as a panacea
- geo-location functionality in everyday devices
- ubiquitous network nodes: household appliances on the net and talking
- 'virtual worlds' and simulated avatar based communication
- 'root kits' and other virus-like software, whether hostile or allegedly friendly, which usurp user control over personal computers

- instant video publishing by phone or other personal devices
- increasing capacity for routine inter-database communication and data-matching, without the need for specific new functionality and expensive custom interfaces to be added on; this can apply across international boundaries, or between companies or agencies
- social networking technologies and virtual communities.[1]

There is a tendency to instrumentalise privacy concerns as merely technical "personal information security" matters, potentially diminishing the scope of privacy protection and policy.

Some technologies which have yet to be fully developed have potential implications for privacy. For example, it has been noted that nanotechnology could lead to new and unprecedented surveillance power:

> Developments in nanotechnology may both facilitate surveillance and increase the power to process information obtained through surveillance. These developments in technology may have an effect on traditional notions of privacy: if it becomes easier and less expensive to gather and use information about people, it may become more common, and eventually, more generally accepted. The evolution of pervasive computing, with various information networks connected to many — and possibly invisible — sensors, suggests that traditional notions of privacy and private and public spaces may need to be re-defined. (Campbell, 2007)

This comment identifies issues common to many of the new technologies.

We have not addressed all of the different technologies discussed by the ALRC, but consider that RFID and biometrics warrant further consideration from the ALRC, so we make specific comments on those two technologies.

Biometrics

While this chapter touches on biometrics, the possible privacy-intrusive character of all biometric systems warrants more substantial analysis (and more than we can offer here). There are a number of concerns relating to biometric technologies that have been neglected. Roger Clarke noted that (after Clarke, 2001):

1. Some individuals may find the process of providing biometric data invasive.
2. Biometrics can lead to unprecedented consolidation of personal data.
3. It becomes much easier to monitor personal behaviour and form judgements as a result of this.
4. Since biometrics systems are expensive to implement it is more likely that they will be utilised for multiple purposes. Multiple uses of an identifier increase the likelihood and ease of data sharing.

[1] See generally, Geist, M. "Technology's challenge to privacy", BBC News, 4 October 2007, at `http://news.bbc.co.uk/2/hi/technology/7026641.stm`

5. Since biometrics is intrinsically linked to identity the individual may be denied the opportunity to transact anonymously or pseudonymously.
6. It is still possible to trick biometric readers, and once your biometric identity is lost in this manner it may be impossible to regain – the extra difficulty of revocation of a compromised biometric. Remedial action may be extremely difficult.
7. Biometric technologies are likely to lead to automated denial of identity and consequently of access/services, without easy opportunity for individuals to challenge or defend themselves.
8. Since biometrics build on a substantial set of surveillance mechanisms, an environment is created where organisations have significant power over individuals. This could increase the chilling effect on freedom and democracy by ubiquitous surveillance.
9. There is a danger that use of biometric technologies could increase dehumanisation (where humans are treated in a similar manner to manufactured goods), because of the increase of human/machine interaction in circumstances where the human subject has little control over the process.

Biometrics can also be discriminatory in some circumstances (for example a small minority of individuals have no readable fingerprints, for a variety of reasons).

Biometric information can be particularly dangerous when the use of collected information is expanded beyond the initial reasons for collection due to 'emergency' situations (for example terrorist attacks). Since "governments have historically had a difficult time using personal information contained in databases under their stewardship for only the purposes for which it was originally intended" (Sherman, 2005, p. 36), reactive usage of essentially untested technology could have dangerous and unforseen consequences (Sherman, 2005, p. 26). The danger is present with all data collection; however, the unique and fixed nature of biometric information may lead to more devastating consequences.

Further, the potential value of the information held in a biometric database, both as identifiers and perhaps also as encoded biological traits not related to identity, means that this information will be aggressively targeted by third parties.

The threats associated with biometric information and technology have been characterised by some as so large that self regulatory guidelines will be largely insufficient (Sherman, 2005, p. 32). This is in part because the technology is currently neither reliable nor mature: its error rates are high (often unacceptably so), and the necessary constraints and limits of use are neither well understood nor necessarily accepted by those planning adoption.

The existing biometrics Code under the *Privacy Act* should be reviewed in light of all the dangers that biometrics can pose. It needs to be considered both by the ALRC, and also on an ongoing basis, perhaps every three years, on the expectation that the rapid rate of change of biometric technologies and business practices will make such a technology-specific code regularly obsolete and ineffective.

(We are not now in a position to give proper attention to a further suggestion, namely to consider the need for more stringent controls over biometric systems, with

increased external regulatory scrutiny of privacy hazards and protections in specific applications. Hence we do not make a formal submission, but observe that this may warrant further attention.)

> ***Submission DP72-250: The ALRC needs to more closely analyse the hazards posed by biometric technologies, and recognise the extent to which the benefits of biometrics are often over-claimed without sufficient evidence, and consequent introduction of biometric systems without adequate justification under the Collection Principles and other UPPs. Recommendations to ensure that privacy protection is designed into biometric systems need priority. Consideration should be given to the imposition of mechanisms to impose external standards of justification before biometric technologies are implemented.***
>
> ***The adequacy and viability of the existing biometrics Code under the Privacy Act should be reviewed by the ALRC, and required to be reviewed periodically.***

RFID

RFID technology has certain intrinsic risks. They can be invisible and ubiquitous (hence hard to object to), with long data lives and inadequately controlled access to data. But there are ways in which RFID technology can be implemented with less risk to privacy. For example, encryption or password protection can help prevent RFID tags being read by unauthorised devices (Weinberg, 2004, p. 14). Rather than using a unique ID, RFID tags could emit random pseudonyms or alternatively, generic descriptors could be used (Weinberg, 2004, p. 14). However, without being legally compelled to do so, businesses are unlikely to adopt such measures, in part because of the perceived costs involved. In addition there are privacy issues raised by how RFID tag information will be used by authorised readers. RFID can lead to profiling, surveillance and the potential to direct action against an individual (e.g. arrest, targeted advertising etc) (Weinberg, 2004, pp. 17-18).

Wienberg notes:

> My ability to disclose or withhold information has social meaning: it demonstrates that I am the owner of my own self and my own relationships. It attests that I am not someone else's data, not a specimen belonging to those who would investigate me.
>
> The profiling, surveillance and action threats posed by privacy-invasive RFID implementations put these values in jeopardy. By promiscuously broadcasting a wide range of information about me to all comers and facilitating the creation of a large-scale profile possibly tied to my name, they deny my autonomy to decide for myself to whom I'll disclose that information. […] By locating me in space, impressing my digital profile on my physical body, privacy-invasive RFID implementations magnify that privacy threat. By allowing strangers to take actions regarding me based on my constellation of tags, they further suppress my ability to make my own choices in a zone of "relative insulation". (Weinberg, 2004, p. 20)

Certain protections should be considered for mandatory inclusion when implementing RFID systems:

1. Do not link tag IDs to personally identifying information (or if linked, disclose the link and obtain written consent). Such a linkage cannot be disclosed to an unaffiliated third party (Weinberg, 2004, p. 23).
2. Impose restrictions on tag data collection (for example, warnings have to be present if tag readers are used) (Weinberg, 2004, p. 24).
3. RFID tags attached to individual retail items are clearly labelled and easily removable (Weinberg, 2004, p. 24).
4. Tags de-activated at store exits or shortly thereafter. (Spiekermann and Ziekow, 2005, 3.1)
5. Minimise retention period of tracking data (Spiekermann and Ziekow, 2005, 4.1) .
6. Turn off or disable RFID tags by default, to be turned on only with individuals' consent using a personal password (Spiekermann and Ziekow, 2005, 4.1).

There are drawbacks and advantages to each of the avenues above, however, without appropriate incentive to spend time and money exploring these options; it is likely that businesses and organisations will neglect to design such safeguards into RFID systems.

These are all also issues that need to be addressed in the standards-making process, and the issuing of guidelines as proposed by the ALRC.

> ***Submission DP72-251: The ALRC needs to more closely analyse RFID technologies and canvass options to tackle privacy problems. Ensuring privacy protection is designed into RFID systems should be a priority. The same restrictions as imposed on biometric technologies should be considered for any uses of RFID.***

ALRC Chapter 7. Accommodating Developing Technology in a Regulatory Framework

This chapter explores various ways in which developing technology can be accommodated in a regulatory framework.

Technological Neutrality

Proposal 7–1 *The Privacy Act should be technologically neutral.*

We support the proposal that the *Privacy Act* should be technologically neutral (or artefact neutral), but with some modification. The Office of the Privacy Commissioner is of the view that the Act should also be 'technologically relevant'. We adhere to a similar view and believe it is important for the Act to be 'technologically aware'.

Checks and balances need to be in place to avoid technological blindness in the privacy framework. Proposals by the ALRC in the following chapters may not go far enough to ensure this. We therefore favour an explicit requirement for the Office of the Privacy Commissioner to review the Act in light of technological developments on a periodic basis. The ALRC, while noting that the Commissioner could do this, does not propose to require it, but we consider it should be required, or it is unlikely to obtain the priority it deserves, due to its 'over the horizon' nature. The review could be as frequent as each Annual Report by the Commissioner, which could be required to include a section on whether any particular technological changes now warranted amendments to privacy legislation. Giving the Commissioner a specific obligation to make such comments helps justify the Commissioner intervening in the political process in this way, and is a valuable way of strengthening the Commissioner's mandate.

> ***Submission DP72-252: While the Privacy Act should be generally 'technology neutral', it should also be sufficiently 'technology aware' as to impose explicit regulations on some technologies, consistent with the general approach of the UPPs. In addition, the Office of the Privacy Commissioner should also be explicitly required to review and report on the changing adequacy of the Privacy Act in light of specific technological developments on a specified periodic basis.***

The definition of 'personal information'

One area where 'technological awareness' is crucial is the definition of 'personal information' (discussed by the ALRC at [7.48]). We have previously submitted that the current definition is inadequate in light of new technologies and should be broadened.

> ***Submission DP72-253: Ensuring technological awareness will require a revised definition of 'personal information,' as we submitted in DP 72-1.***
>
> *[The definition of 'personal information', or the explanatory memorandum in relation thereto, should state that it covers those situations where information is sufficient to allow interaction*

*with persons on an individualised basis, or the imparting of consequences on an individualised basis. This should not include information which merely allows an individual to be contacted without conveying anything about the individual's identity or characteristics.**]***

Standards

***Proposal 7–2** The Privacy Act should be amended to empower the Minister responsible for the Privacy Act, in consultation with the Office of the Privacy Commissioner, to determine which privacy and security standards for relevant technologies should be mandated by legislative instrument.*

As the ALRC notes (DP 72, [7.65]), incorporating privacy protections into technical standards provides a good opportunity to have such protections 'built in' at the design stage of processes and products. The ALRC is proposing that some standards relevant to privacy could be made mandatory by delegated legislation (DP 72, [7.68]). We support these two approaches as being of potential value, but have concerns about various aspects of implementation.

The ALRC is proposing guidelines, binding codes, regulations and legislation to tackle assorted privacy issues so the addition of mandated 'standards' adds another layer of complexity to an already complex regime. It also potentially moves the regulatory process into a venue which has a poor track record of broad consultation, as opposed to technical expertise.

The main concern we have is that standards emerge 'bottom up' and are then adopted by the legislative regime. If the processes at the bottom of the standards making and adoption process are not sufficiently representative and open, then this cannot be remedied by the democratic controls involved in the delegated legislative processes. The only check that is available at that level is refusal to adopt the standard. The danger then becomes that the presumed legitimacy of the standards-making process could lead to the adoption of standards that are not adequately protective of privacy.

The success and effectiveness of such a proposal will therefore largely depend on the standards-making process. The parties involved in the standards process and the interests that these parties represent will determine the appropriateness of a standard.

The history of standards development in Australia – for instance through Standards Australia, the obvious body to be involved in standards making, and through sectoral bodies such as the Communications Alliance – has not in our view been satisfactory: there is a clear 'democratic deficit'. Consumer interests have consistently been under-represented, compared with business, technical and professional interests, and there has been a lack of transparency about the processes.[2]

Recent experience with and statements by Standards Australia, suggest that they are not adequately established to deal with matters of a controversial nature, or where

[2] Consumers Federation of Australia submission to the Productivity Commission review of Standards and Accreditation, June 2007 at `http://www.consumersfederation.org.au/submissions.htm`

there are a wide range of disputed interests and positions.[3] There may however be an emerging push to invite government to devolve regulation down to this new quasi-regulatory level.[4] While this may be appropriate in some circumstances or for some subjects, it is by no means clear that the current standards-making process is adequate for dealing with the complex interplay of technology and privacy issues. The attention of standards bodies is intrinsically likely to focus on technical rather than broader issues, and there is a clear risk of an industry-driven rather than an individual citizen focus, in both the consultative methods and the scope of analysis.

Other questions emerge over what happens when a consensus cannot be reached regarding a standard. Creating standards for developing technologies can be a very complex process. If experts in the field cannot decide on an appropriate standard, it begs the question: will the relevant minister and the Office of the Privacy Commissioner be able to reach an appropriate conclusion? It is also relevant to consider what mechanisms are in place to update a standard where necessary.

We also share the Office of the Privacy Commissioner's concern that the relationship between the proposed instrument and other regulations and principles is unclear (OPC, 2007, Chapter 7, [12]). Questions also arise about how the standards process would operate in these particular circumstances.

In our view, no standard should be able to reduce the protections provided by the UPPs.

We support proposal 7-2 in principle, subject to a thorough prior review of the operation of the standards-making process, especially the adequacy of wide stakeholder representation and consultation, clear and explicit limits on the regulatory topics which can be devolved to standards, and mechanisms for avoiding an overly technical and 'industry convenience' focus to the detriment of less industrially organised interests, and less technical values such as individual privacy, dignity and wellbeing.

As a further necessary precaution, where the Minister proposes to adopt a standard, there should be a requirement for prior public consultation and the involvement of the Privacy Commissioner.

> ***Submission DP72-254: There is currently no adequate stakeholder representation in standards-making, and the current Australian process is not well developed enough to deal fairly with matters where there are real divergences of interest, especially as between industry and consumer or community sectors. We support proposal 7-2 in principle, but only subject to (i) a thorough prior review of the operation of the standards-making process, especially the adequacy of wide stakeholder representation and consultation; (ii) provision for public consultation by the Minister, and involving the Privacy Commissioner, before any standard is adopted; and a***

[3] For instance, they acknowledged in September 2007 that their process was inadequate and immature for dealing with the issues arising from the OOXML Draft Specification for file formats. See http://www.cyberlawcentre.org/2007/ooxml/

[4] Personal communication with one of the authors.

requirement that a standard cannot reduce the protections provided by the UPPs.

It is also important that privacy-enhancing technologies (PETs) are taken into account when formulating mandated standards (see discussion regarding PETs below). They are a desirable foundation for privacy protection, as the ALRC recognises.

Submission DP72-255: The standards-making process should start from an assumption that there should be integration of privacy-enhancing technologies (PETs).

Oversight Functions of the Regulator re technologies

Proposal 7–3 *In exercising its research and monitoring functions, the Office of the Privacy Commissioner should consider technologies that can be deployed in a privacy enhancing way by individuals, agencies and organisations.*

We support this proposal to consider PETs.

We also suggest that the inverse, 'privacy-invasive technologies' (PITs), should also be given careful consideration. Research and monitoring of such technology will help assist in identifying PITs and minimise the harm caused by this technology.

The Office of the Privacy Commissioner should pay special attention to technologies that appear to be privacy enhancing, however only offer minimal protection. For example, 'privacy seals' have been used as an example of technology utilised mainly to offer the illusion of privacy rather than true privacy protection (Clarke, 2007). The Platform for Privacy Preferences (P3P) was also once lauded as a PET, but has been criticised widely and does not seem to have advanced (Clarke, 2001a).

Submission DP72-256: The Office of the Privacy Commissioner should be required to actively and regularly research and monitor privacy invasive technologies. In particular, these inquiries should be directed to whether technologies claimed to have privacy enhancing characteristics do so, or are themselves a hazard in practice.

The New Zealand Law Commission (NZLC) in their privacy study paper noted that law reform should address ways in which law and policy can protect privacy through the promotion of PETs. The NZLC continues by offering the following examples (NZLC, 2008, [6.113]):

- Promoting and supporting research into and development of PETs.
- Adopting PET-friendly policies within government departments and agencies. This can include using PETs in the government's own information systems and other technologies that may have implications for privacy, ensuring that privacy is designed in to new systems, and carrying out privacy impact assessments of systems during and after development.
- Requiring the incorporation and use of PETs in the provision of particular products and services.
- Intervening directly in the design of systems by private companies. While this is unlikely to happen often, one significant example is the European Union's successful attempt to get Microsoft to modify its 'Passport' system[…]

- Removing legal and other obstacles to the use of PETs by consumers, so long as these PETs do not protect privacy at the expense of other public interests (some restrictions on the use of encryption and anonymisation may be needed for security and law enforcement purposes, for example).
- Raising consumer awareness of PETs through provision of information and education.
- Facilitating informed choice by consumers through the development of privacy standards for technologies and associated certification programmes such as privacy seals.

It appears that there are more avenues to create incentives to use PETs than have been canvassed by the ALRC.

> ***Submission DP72-257: The ALRC should develop recommendations addressing ways in which law and policy can protect privacy through the promotion of privacy enhancing technologies (PETs).***

> ***Proposal 7–4*** *The Office of the Privacy Commissioner should educate individuals, agencies and organisations about specific privacy enhancing technologies and the privacy enhancing ways in which technologies can be deployed.*

We support this proposal.

In keeping with our comment above, the Office of the Privacy Commissioner should also educate individuals, agencies and organisations about the potential harm of PITs, why such technologies should be avoided and how to identify these technologies.

The Office of the Privacy Commissioner should also educate individuals, agencies and organisations about the various degrees of protection that can be provided by PETs. In particular, identifying poor PETs that only provide a minimal degree of privacy protection.

We support the Office of the Privacy Commissioner's proposal to expressly acknowledge the promotion of an understanding of technology and privacy in its education function under section 27 of the *Privacy Act* (OPC, 2007, proposal 7-4).

> ***Submission DP72-258: Proposal 7-4 should be embodied in section 27 of the Privacy Act under the education function of the Office of the Privacy Commissioner. It should be extended to also cover privacy invasive technologies, particularly those that are not obviously privacy invasive.***

Guidance on Particular Technologies

> ***Proposal 7–5*** *The Office of the Privacy Commissioner should provide guidance in relation to technologies that impact on privacy (including, for example, guidance for use of RFID or data collecting software such as 'cookies'). Where appropriate, this guidance should incorporate relevant local and international standards. The guidance should address:*

We note at this stage our general comments on OPC guidance contained in our other submission (see 3.3, CLPC submissions to part F), and our comments on the incorporation of technical standards (above).

> *(a) when the use of a certain technology to collect personal information is not done by 'fair means' and is done 'in an unreasonably intrusive way';*

We support this proposal (subject to our general comments on OPC guidance).

> *(b) when the use of a certain technology will require, under the proposed 'Specific Notification' principle, agencies and organisations to notify individuals at or before the time of collection of personal information;*

The Office of the Privacy Commissioner proposes that technology-specific notices should only be provided where there is a demonstrated need for technology-specific notice requirements (OPC, 2007, Chapter 7, [23]). While this has some merit, there is a risk that this criterion will be used to drastically limit the scope of the guidance given on notices. It is not clear how such a need would be demonstrated, or who would demonstrate it. One of the core issues with emerging technology is that its effects are secret, invisible or otherwise hidden from attention. Promoters have an incentive to keep it so, and this may result in a lack of awareness of something that, if known, may well be a cause for wide concern. The OPC should therefore in matters of emerging technology, err on the side of encouraging notice, rather than seeking loopholes to avoid it. We consider it should be sufficient for non-binding guidelines if the Commissioner considers that notice would be 'desirable'.

The Office of the Privacy Commissioner further submits that where there is a demonstrated technology specific need to provide guidance that these requirements be incorporated in technologically specific binding guidelines and industry codes (OPC, 2007, Chapter 7, [24]).

> ***Submission DP72-259: The Office of the Privacy Commissioner should be required to develop either guidelines or codes where he or she has identified specific circumstances in which notification in the context of particular technological developments should be required.***

In our other submission we discuss technology constraints on notification (See CLPC Submission, Pt D, p. 32). We note that guidance is required relating to what limited circumstances notification can occur 'after the event' (CLPC DP 72, 2007, p. 31). This guidance is critical in the context of developing technologies, mobile phone advertising being one such example.

> ***Submission DP72-260: In relation to recommendation 7–5(b), it should be sufficient for non-binding guidelines if the Commissioner considers that notice would be 'desirable'. The requirement that notice be demonstrated to be 'necessary' should be limited to binding requirements.***

> *(c) when agencies and organisations should notify individuals of certain features of a technology used to collect information (for example, how to*

> *remove an RFID tag contained in clothing; or error rates of biometrics systems);*

We have already discussed some ways in which privacy issues associated with RFID can be at least partially addressed, such as clearly labelling and allowing easy removal of RFID tags.

We also indicate that these are all considerations that need to be taken into account when designing a RFID system. The Office of the Privacy Commissioner notes that there should be basic privacy principles which should be followed when designing RFID systems (OPC, 2007, Chapter 7, [26]). We agree with this position, however, feel that guidelines will not go far enough to highlight the importance of privacy considerations in the design phases of developing technologies. We propose in one of our other submissions that the anonymity and pseudonymity principle should:

> Expressly state that the obligation on organisations/agencies applies at the stage when an information system is being designed, not only 'after the event' when a person wishes to enter a transaction with a data user. This is to mean that where it is practicable, without excessive cost, to design anonymity/pseudonymity options into a system, they must be designed in. The judgements as to practicability and as to whether any cost is excessive must not be left to the organisation/agency – they must be able to be tested by an independent party (CLPC DP 72, 2007, Submission DP72-12).

The importance that the design phase plays in reinforcing privacy is already evident. Privacy considerations during the design phase should be a critical factor when assessing developing technologies that are satisfactory under our current framework.

> ***Submission DP72-261: The Office of the Privacy Commissioner should provide guidance on how privacy protection, addressing current and future community expectations and the intrinsic hazards of the system, must be designed into systems from their earliest feasibility stages, and how it is critical to implement privacy protections in the design phase.***

> *(d) the type of information that an agency or organisation should make available to an individual when it is not practicable to provide access to information held in an intelligible form (for example, what biometric information is held about an individual when the information is held as an algorithm); and*

The Office of the Privacy Commissioner queries whether the proposed access and correction principle implies that access to personal information should be given in an intelligible form where practicable (OPC, 2007, Chapter 7, [28]). It is critical that the principle expressly states that access should be provided in an intelligible form where practical. The Office of the Privacy Commissioner could then provide guidance as to what does not amount to practical circumstances.

> ***Submission DP72-262: In relation to recommendation 7–5(d), we support the Office of the Privacy Commissioner's proposal that express reference to the need to provide access in an intelligible form where practicable should be included in UPP 9.***

> *(e) when it may be appropriate for an agency or organisation to provide human review of a decision made by automated means.*

In our submission responding to Part D of the review we recommend that an organisation or agency should take reasonable steps to avoid making a decision adverse to the interests of an individual based on automated processing, without the prior review of that decision by a human. We submitted that the Data Quality principle (UPP 8) should be amended to achieve this (Submission DP72-124).

The Office of the Privacy Commissioner notes that legislative amendments may be necessary requiring agencies and organisations to have in place appropriate review mechanisms for automated decisions, especially where the decision has an adverse effect on the individual (OPC, 2007, Chapter 7, [32]). However the Office believes that in the interests of technological neutrality it is important for the *Privacy Act* to support fair and reasonable review mechanisms and allow for technological development which allows for effective review via automated systems.

The OPC approach seems to misconstrue the concept of 'technological neutrality': our proposal in relation to UPP 8 was for a right to have a human involved in adverse decisions. It is not somehow 'technologically neutral' to suggest that this be done alternatively without human intervention.

Automated systems, especially large monolithic ones used by large agencies and corporations, are almost by definition, and certainly by long experience, likely to be flawed in a range of ways, rather than being reliable.[5] IT systems development is still demonstrably in an immature stage of industrial and professional development, despite what promoters may suggest. Developers avoid all liability for the reliability of their systems. It is therefore not possible to have confidence in automated systems, especially where they are new, complex, rapidly-changing, or dependent on new technologies or processes.

> ***Submission DP72-263: We support the Paper's proposal that the OPC may provide guidance as to when it may be appropriate for an agency or organisation to provide human review of a decision made by automated mean. We further recommend that, consistent with our earlier recommendations, the presumption should be that an organisation or agency should take reasonable steps to avoid making a decision adverse to the interests of an individual based on automated processing, without the prior review of that decision by a human.***

> ***Proposal 7–6*** *The Office of the Privacy Commissioner should provide guidance to organisations on the privacy implications of data-matching.*

The ALRC suggests that guidelines governing data-matching should not be made mandatory. In our previous submission we noted that data-matching is an increasingly prevalent technique (CLPC IP31, Submission, p. 39). The Commissioner issued 'voluntary data matching guidelines' in 1992, and subsequently recommended legislation to make them mandatory (to which the government did not respond). The

[5] See for instance the formal demonstration that you cannot prove that any given system is 'not a killer robot', GikII conference, University of Edinburgh, September 2006.

Office of the Privacy Commissioner proposes that the *Privacy Act* should provide for the development of binding industry codes to add specific regulation to data-matching activities that may raise heightened privacy risks (OPC, 2007, Proposal 7-6).

We submit that data-matching guidelines should be made mandatory. The industry self regulatory model does not work in this area, as there is too great a disconnect between possible abuses, mistakes or other privacy invasive aspects and the information that data subjects are likely to be able to find about a given program. This is not an area where industry codes are sufficient, because the temptations and conflict of interest are likely to be too strong, and the likelihood of enforcement or detection of abuses too limited in such a model.

Hidden abuses of data matching represent a major area of concern for future privacy rights. The largest corporate and government bodies are likely to be involved, so it affects large segments of the population. Any parties involved in data matching may be tempted to bypass or avoid the intent of voluntary codes, because data matching is very often an activity that is not visible to those affected by it.

Data-matching is subject to more general mandatory requirements under other countries' privacy laws, including those in Hong Kong and New Zealand, and should generally be subject to mandatory requirements in Australia.

(The content of data matching regulation more generally also warrants further attention, but we are not in a position to offer any formal submission at this point.)

> ***Submission DP72-264: Data-matching in both the public sector and the private sector should be subject to mandatory rules (whether Codes or some other form).***

ALRC Chapter 8. Individuals, the Internet and Generally Available Publications

In this chapter the ALRC examines the handling of personal information by individuals, in particular the publication of information online.

Individuals Acting in a Personal Capacity

> ***Question 8–1*** *Should the online content regulation scheme set out in the Broadcasting Services Act 1992 (Cth), and in particular the ability to issue take down notices, be expanded beyond the National Classification Code and decisions of the Classification Board to cover a wider range of content that may constitute an invasion of an individual's privacy? If so, what criteria should be used to determine when a take down notice should be issued? What is the appropriate body to deal with a complaint and issue the take down notice?*

Extension of the online content scheme is not the appropriate approach to tackling privacy issues. Jurisdictional issues mentioned by the ALRC will become a notable obstacle. The Privacy Commissioner's existing powers are probably sufficient to enable the Commissioner to require content to be removed from a website if its posting breaches the UPPs. Improving the Commissioner's responsiveness to complaints which involve an element of urgency, while preserving rights of hearing and appeal, is the preferable way to deal with issues like this. The proposed statutory cause of action will also provide some assistance to individuals who have had personal information posted about them online. It would be desirable that the exemption from the UPPs for the actions of individuals should be lost wherever a person discloses information about another person under circumstances which are within the proposed cause of action.

The ALRC and/or OPC should also investigate whether providers of relevant Internet services that enable posting could modify their Terms of Use of Internet services in order to give better remedies for persons affected by privacy intrusive posts by other individuals, while being sensitive to the dangers of censorship regimes being instituted by private parties.

> ***Submission DP72-265: Issuing 'take down' notices is not an appropriate method of tackling problems associated with individuals and 'private' information posted on the internet. The exemption from the UPPs for the actions of individuals should be lost wherever a person discloses information about another person under circumstances which are within the proposed statutory cause of action (under consideration by the ALRC and the NSWLRC). If the Privacy Commissioner's powers need to be clarified to ensure that the Commissioner has power to require content removal from the Internet, that should be done. The Privacy Commissioner should develop procedures to deal with such complaints, where such a breach of the UPPs is involved.***
>
> ***ALRC and/or OPC should also investigate whether providers of Internet services that enable posting could amend their Terms of Use of Internet***

services to give better remedies for persons affected by privacy intrusive posts by other individuals.

Proposal 8–1 *The Office of the Privacy Commissioner should provide guidance that relates to generally available publications in an electronic form. This guidance should:*

(a) apply whether or not the agency or organisation is required by law to make the personal information publicly available;

(b) set out certain factors that agencies and organisations should consider before publishing personal information in an electronic form (for example, whether it is in the public interest to publish on a publicly accessible website personal information about an identified or reasonably identifiable individual); and

(c) set out the requirements in the proposed Unified Privacy Principles with which agencies and organisations need to comply when collecting personal information from generally available publications for inclusion in a record or another generally available publication (for example, when a reasonable person would expect to be notified of the fact and circumstances of collection).

We support this proposal subject to general comments on Office of the Privacy Commissioner guidance contained in our other submission (see 3.3, CLPC sub to part F).

The OPC notes that since the *Privacy Act* does not cover state and territory courts a coordinated approach with state, territories and the Commonwealth is required to ensure there is a consistent framework in place for the publication of electronic court records and decisions (OPC, 2007, Chapter 8, [31]). We support this position.

We support the promotion of more privacy protective assumptions in such guidelines, such as by requiring agencies, before they publish PI (personal information in full everywhere), to consider both alternative non-PI means of achieving the same ends, and also alternative to full PI, such as partial identifiers that can on request be linked to PI for appropriate reasons, rather than having all the PI accessible; or requiring identification and logging of users of such PI.

We also support the highest level of notification that one's personal information will go on the Internet, and the provision of alternative means to avoid this, or means to easily challenge a decision to post such information prior to its posting.

The harm that can be done by non-essential posting of PI is rapid and potentially devastating. The authors are aware of people who have lost employment as a result. It is often too late to take it down after the fact.

Submission DP72-266: We generally support Proposal 8–1 in relation to guidelines concerning publicly available information. Such guidelines should encourage a presumption that organisational and individual means to avoid posting fully identified PI on websites should be adopted unless all alternatives have been explored and rejected as not feasible, or the competing social interests clearly justify such a level of Internet publication. We also support a presumption of the highest level of notification that one's

PI material will go on the Internet, and the provision of alternative means to avoid this, or means for the subject to easily challenge a decision to post such information, prior to its posting (and also remedies after posting).

We support a separate enquiry into publication of electronic court records and decisions, coordinated between all jurisdictions.

ALRC Chapter 9. Identity Theft

This chapter looks specifically at identity theft and privacy. In our view, 'identity theft' is simply one of the extreme cases of the more general problem of identity fraud, with which it is often wrongly conflated. The ALRC notes that privacy laws including observance of the UPPs can assist in preventing and minimising the harm associated with identity theft. The ALRC cites as potentially performing this function the security and accuracy principles; data breach notification, proposed guidance and proposed take down notice scheme relating to publicly available information in electronic form and credit reporting provisions. We would add that the principle of minimum collection of personal information, coupled with observance of disclosure restrictions, and appropriately strong data export limitations, are also of great importance in minimising identity theft.

> ***Submission DP72-267: We agree that the UPPs and privacy laws generally should be considered as tools to reduce identity fraud and theft. The ALRC should adopt recommendations in relation to all of the UPPs and its other privacy proposals with the specific question in mind of what will best minimise harm caused by identity fraud and theft.***

It also useful to consider the implications of the adoption of biometric technologies and the consequences this will have on identity theft. As discussed above, there is an intrinsic link between biometric data and identity. As a result, if this information is stolen or compromised, revocation of the credentials is much more difficult that with other identifying data.

> ***Submission DP72-268: The ALRC should consider how identity fraud and theft can be minimised in the context of biometric data, and in particular the increased risk that repositories of biometric data poses due to the potential commercial and criminal value of such data.***

References

Australian Law Reform Commission (‘DP 72’) (2007), Discussion Paper 72: *Review of Australian Privacy Law*, September 2007.

Clarke, R. (2007) “Business Case for Privacy Enhancing Technologies”, Preprint of a Chapter in Subramanian R. (Ed.) '*Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions*' IDEA Group, 2007, Version of 12 June 2007 available at
<http://www.anu.edu.au/people/Roger.Clarke/EC/PETsBusCase.html>

Clarke, R. (2001) “Biometrics and Privacy”, 15 April 2001 at
<http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html >

Clarke, R. (2001a) “P3P Revisted”, [2001] *PLPR* 1 at
< http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/PLPR/2001/39.html>

Campbell, L.M. (2007) “Nanotechnology and the United States National Plan for Research and Development In Support of Critical Infrastructure Protection” presented at TERRA INCOGNITA

Privacy Horizons, 9th International Conference of Data Protection and Privacy Commissioners, September 25-28, Montreal, Canada at
<http://www.privacyconference2007.gc.ca/workbooks/Terra_Incognita_workbook2_E.html>

Greenleaf, G., Waters, N, and Bygrave L. (‘CLPC DP 72’) (2007) 'Strengthening uniform privacy principles: an analysis of the ALRC's proposed principles', Submission to the Australian Law Reform Commission on the Review of Australian Privacy Laws Discussion Paper 72, December at
<http://www.cyberlawcentre.org/ipp/publications/papers/ALRC_DP72_UPPs_final.pdf>

Greenleaf, G., Waters, N, and Bygrave L (‘CLPC IP31’) (2007), 'Implementing privacy principles: After 20 years, its time to enforce the *Privacy Act*', Submission to the Australian Law Reform Commission on the Review of Privacy Issues Paper, January
at <http://www.cyberlawcentre.org/ipp/publications/papers/ALRC_IP31_subm.pdf>

New Zealand Law Commission (‘NZLC’) (2008) “Privacy Concepts and Issues: Review of the Law of Privacy Stage 1”, January, at
<http://www.lawcom.govt.nz/UploadFiles/Publications/Publication_129_390_SP19.pdf>

Office of the Federal Privacy Commissioner (‘OPC’) (2007), “Submission to the Australian Law Reform Commission's Review of Privacy - Discussion Paper 72,” 21 December, at <http://www.privacy.gov.au/publications/alrc211207.html>

Sherman, D , "Biometric Technology: The Impact on Privacy" (2005). CLPE Research Paper No. 5 at: <http://ssrn.com/abstract=830049>

Spiekermann, S. and Ziekow, H. (2005) "RFID: A 7-Point Plan to Ensure Privacy" (2005). 13th European Conference on Information Systems, 2005 at SSRN: <http://ssrn.com/abstract=761047>

Weinberg, J. (2004) "RFID and Privacy" (October). at SSRN: <http://ssrn.com/abstract=611625> or DOI: 10.2139/ssrn.611625

Index of Submissions

Introduction

ALRC Chapter 6. Overview - Impact of Developing Technology on Privacy

Submission DP72-250: The ALRC needs to more closely analyse the hazards posed by biometric technologies, and recognise the extent to which the benefits of biometrics are often over-claimed without sufficient evidence, and consequent introduction of biometric systems without adequate justification under the Collection Principles and other UPPs. Recommendations to ensure that privacy protection is designed into biometric systems need priority. Consideration should be given to the imposition of mechanisms to impose external standards of justification before biometric technologies are implemented.

The adequacy and viability of the existing biometrics Code under the Privacy Act should be reviewed by the ALRC, and required to be reviewed periodically.

Submission DP72-251: The ALRC needs to more closely analyse RFID technologies and canvass options to tackle privacy problems. Ensuring privacy protection is designed into RFID systems should be a priority. The same restrictions as imposed on biometric technologies should be considered for any uses of RFID.

ALRC Chapter 7. Accommodating Developing Technology in a Regulatory Framework

Submission DP72-252: While the Privacy Act should be generally 'technology neutral', it should also be sufficiently 'technology aware' as to impose explicit regulations on some technologies, consistent with the general approach of the UPPs. In addition, the Office of the Privacy Commissioner should also be explicitly required to review and report on the changing adequacy of the Privacy Act in light of specific technological developments on a specified periodic basis.

Submission DP72-253: Ensuring technological awareness will require a revised definition of 'personal information,' as we submitted in DP 72-1.

Submission DP72-254: There is currently no adequate stakeholder representation in standards-making, and the current Australian process is not well developed enough to deal fairly with matters where there are real divergences of interest, especially as between industry and consumer or community sectors. We support proposal 7-2 in principle, but only subject to (i) a thorough prior review of the operation of the standards-making process, especially the adequacy of wide stakeholder representation and consultation; (ii) provision for public consultation by the Minister, and involving the Privacy Commissioner, before any standard is adopted; and a requirement that a standard cannot reduce the protections provided by the UPPs.

Submission DP72-255: The standards-making process should start from an assumption that there should be integration of privacy-enhancing technologies (PETs).

Submission DP72-256: The Office of the Privacy Commissioner should be required to actively and regularly research and monitor privacy invasive technologies. In particular, these inquiries should be directed to whether technologies claimed to have privacy enhancing characteristics do so, or are themselves a hazard in practice.

Submission DP72-257: The ALRC should develop recommendations addressing ways in which law and policy can protect privacy through the promotion of privacy enhancing technologies (PETs).

Submission DP72-258: Proposal 7-4 should be embodied in section 27 of the Privacy Act under the education function of the Office of the Privacy Commissioner. It should be extended to also cover privacy invasive technologies, particularly those that are not obviously privacy invasive.

Submission DP72-259: The Office of the Privacy Commissioner should be required to develop either guidelines or codes where he or she has identified specific circumstances in which notification in the context of particular technological developments should be required.

Submission DP72-260: In relation to recommendation 7–5(b), it should be sufficient for non-binding guidelines if the Commissioner considers that notice would be 'desirable'. The requirement that notice be demonstrated to be 'necessary' should be limited to binding requirements.

Submission DP72-261: The Office of the Privacy Commissioner should provide guidance on how privacy protection, addressing current and future community expectations and the intrinsic hazards of the system, must be designed into systems from their earliest feasibility stages, and how it is critical to implement privacy protections in the design phase.

Submission DP72-262: In relation to recommendation 7–5(d), we support the Office of the Privacy Commissioner's proposal that express reference to the need to provide access in an intelligible form where practicable should be included in UPP 9.

Submission DP72-263: We support the Paper's proposal that the OPC may provide guidance as to when it may be appropriate for an agency or organisation to provide human review of a decision made by automated mean. We further recommend that, consistent with our earlier recommendations, the presumption should be that an organisation or agency should take reasonable steps to avoid making a decision adverse to the interests of an individual based on automated processing, without the prior review of that decision by a human.

Submission DP72-264: Data-matching in both the public sector and the private sector should be subject to mandatory rules (whether Codes or some other form).

ALRC Chapter 8. Individuals, the Internet and Generally Available Publications

Submission DP72-265: Issuing 'take down' notices is not an appropriate method of tackling problems associated with individuals and 'private' information posted on the internet. The exemption from the UPPs for the actions of individuals should be lost wherever a person discloses information about another person under circumstances which are within the proposed statutory cause of action (under consideration by the ALRC and the NSWLRC). If the Privacy Commissioner's powers need to be clarified to ensure that the Commissioner has power to require content removal from the Internet, that should be done. The Privacy Commissioner should develop procedures to deal with such complaints, where such a breach of the UPPs is involved.

ALRC and/or OPC should also investigate whether providers of Internet services that enable posting could amend their Terms of Use of Internet services to give better remedies for persons affected by privacy intrusive posts by other individuals.

Submission DP72-266: We generally support Proposal 8–1 in relation to guidelines concerning publicly available information. Such guidelines should encourage a presumption that organisational and individual means to avoid posting fully identified PI on websites should be adopted unless all alternatives have been explored and rejected as not feasible, or the competing social interests clearly justify such a level of Internet publication. We also support a presumption of the highest level of notification that one's PI material will go on the Internet, and the provision of alternative means to avoid this, or means for the subject to easily challenge a decision to post such information, prior to its posting (and also remedies after posting).

We support a separate enquiry into publication of electronic court records and decisions, coordinated between all jurisdictions.

ALRC Chapter 9. Identity Theft

Submission DP72-267: We agree that the UPPs and privacy laws generally should be considered as tools to reduce identity fraud and theft. The ALRC should adopt recommendations in relation to all of the UPPs and its other privacy proposals with the specific question in mind of what will best minimise harm caused by identity fraud and theft.

Submission DP72-268: The ALRC should consider how identity fraud and theft can be minimised in the context of biometric data, and in particular the increased risk that repositories of biometric data poses due to the potential commercial and criminal value of such data.

References

Index of Submissions