Cyberspace Law and Policy Centre, University of New South Wales

Symposium

Meeting Privacy Challenges – the ALRC and NSLRC Privacy Reviews

Thursday 2 October

Panel Session 3: How do the ALRC and NSWLRC proposals contribute to providing a set of global best practice Privacy Principles which also adequately address the privacy threats and opportunities from emerging technologies?

Paper by Nigel Waters and Graham Greenleaf, Principal Researcher and Chief Investigator respectively on the *Interpreting Privacy Principles* (iPP) project – an ARC funded research project at the Cyberspace Law & Policy Centre. We acknowledge the assistance of Abi Paramaguru, Research Assistant, Anna Johnston, Research Associate, and David Vaile, Centre Director.

References to the ALRC and NSWLRC are respectively to ALRC Report 108, *For Your Information: Australian Privacy Law and Practice*, May 2008 and NSWLRC Consultation Paper 3: *Privacy Legislation in New South Wales*, June 2008.

Coverage of Federal privacy law

Better coverage, but danger of levelling down

The ALRC's preference is for intergovernmental agreement to implement and maintain uniform privacy laws in all jurisdictions (Recs 3-4 & 5) and this objective is supported by the NSWLRC (Proposals 1 & 2). This is a desirable goal, but only if the uniform principles and other provisions reach an adequate standard. States and Territories will be understandably reluctant to 'trade off' any higher level of protection for the sake of national uniformity. As we submit in this and other papers on the proposals from the various Law Reform Commissions, it is not yet clear either that the Commonwealth's 'baseline' offer (once it has digested and responded to the ALRC Report) will be of a sufficiently high level of protection, or that the other jurisdictions will agree to that level. It is therefore premature to endorse the ALRC's proposed model, and we will consequently focus instead on analysis of the detailed recommendations for the content of a federal, and potentially national, privacy law.

The proposal for the Commonwealth privacy law to generally 'cover the field', initially in relation to the private sector (Rec 3-1), but potentially also for State and Territory public sectors has another potential downside, which is recognised by the ALRC, but not, expressly, by the NSWLRC (Proposal 3). It would be essential that the proposed list of 'preserved matters' that could remain subject to State and Territory laws (Rec 3-3) included those matters currently covered by Surveillance laws[1], as there is no current proposal for Commonwealth laws to do so. Given the importance of the regulation of surveillance devices as a complement to information privacy laws, this should be a non-negotiable condition of any Commonwealth preemption.

1 Such as the *Surveillance Devices Act 2007* (NSW)

The ALRC's recommendations relating to exemptions (Part E) are generally very welcome, in that they propose removal of many of the existing exemptions, such as those for employee records, small business and political parties, acts and practices, and narrowing of the media exemption, and review of many of the arbitrary 'inherited' exemptions for specific government agencies. If adopted, these recommendations would mean a major extension of the coverage of the privacy principles, with privacy obligations and rights applying in many circumstances where they are most necessary. The NSWLRC canvasses some similar proposals for narrowing of the many exemptions in the NSW legislation (various Issues and Proposals in CP3 Chapters 5 and 7).

Structural approach to privacy regulation

Sensible aspirations, but many dependencies

The structural changes suggested by the ALRC are generally welcome – a single set of unified privacy principles applying to both private and public sectors would be simpler for both data users and the public to understand and apply or use. If the ALRC's proposals for removal of several major exemptions are also accepted, and if the States and Territories can be persuaded to adopt the UPPs, then Australia would have much more complete, seamless and simpler privacy protection. We also welcome the NSWLRC's preference (Proposal 4) for a simpler set of privacy principles but incorporating relevant exceptions, along similar lines to the ALRC's UPPs.

Whether the regime resulting from the ALRC's proposals would be 'world's best practice' able to deal effectively with the challenges of new technology and of new models of business and government service delivery depends on the content and effect of the proposed new principles. The effectiveness would also depend in part on the way in which key concepts underlying the principles, such as the definitions of personal information and the meaning of consent, are addressed in the legislation and interpreted in practice. On these scores, the future appears less bright.

Principles

Some improvements, some losses, many missed opportunities

The ALRC recommends a continuation, and in some cases a further strengthening, of the current approach of the Privacy Act – that is for 'high level' principles rather than detailed prescriptive regulation. This approach, characterised by the previous government as 'light touch' regulation, is supposed to ensure a focus on achievement of underlying objectives, leaving scope for flexibility in the means by which these outcomes are achieved. While it is difficult to argue against this approach in principle, applying it in practice in a privacy protection context is fraught with difficulty, particularly because there is no clear consensus what the practical effect of many of the principles should be.

One measure of the effectiveness of privacy laws is the extent to which they increase the level of control that individuals have over the amount of information about them that is collected, and over the way in which it is then used, including the extent of dissemination. This objective is characterised by James Rule as the 'surveillance limitation' function of privacy laws[2]. How do the modifications to privacy principles suggested by the ALRC score on this measure? And do the NSWLRC's provisional views support this function for the NSW law?

2 James Rule et al in *The Politics of Privacy* , Elsevier Books, 1980 - In essence, Rule argued that [privacy] laws rarely attempted to limit the spread of information surveillance, they merely attempted to make surveillance mechanisms operate more ‘fairly

Proposals which give individuals *more* control or otherwise limit surveillance (but in most cases with serious limitations).

- Application of most UPPs to agencies will mean some additional controls although also some losses – specifics mentioned below.
- inclusion of biometric information in the definition of 'sensitive information' (Rec 6-4). (But the value of this is severely limited by the qualification that it only be " biometric information collected *for the purpose of* automated biometric verification or identification" or "a biometric template".)
- addition of 'pseudonymous' to the 'Anonymity' principle (UPP1) and application to agencies. (But this principle remains 'toothless' because the Commissioner can only investigate once a system has failed to offer anonymity or pseudonymity, by which time it will almost always be 'impracticable' to do so! This is a principle than needs to be enforced proactively, and the Act does not provide appppropriate mechanisms for this. Privacy impact assessments would help but the ALRC's recommendations in respect of PIAs are weak (Recs 47-4 & 5).)
- removal of the 'mere awareness' exception to the disclosure principle currently applying to Commonwealth agencies (IPP 11.1(a)) – the proposed UPP 5 contains no such exception. (The NSWLRC asks about this at Issue 40 – an appropriate exception is the 'related purpose within the individual's reasonable expectation' at UPP 5.1(a).)
- strengthening of the Direct marketing principle (UPP6), including by giving individuals an unambiguous right to opt-out from direct marketing without charge. (But a failure to define 'direct marketing' leaves loopholes, and the principle is not applied to agencies.)
- extension of the Identifiers principle (UPP10) to identifiers issued by State and Territory agencies. (But to be really effective, the principle should apply to Commonwealth agencies as well as to organisations. See also NSWLRC Proposal 14 and Issue 44.)
- application of the Cross-border data flow principle (UPP 11) to agencies. (But see our comments below on the weakness of UPP 11.)

Proposals which give individuals *less* control or otherwise increase surveillance

- endorsement of argument that data linkage arrangements where identification keys are held by third parties amounts to de-identification (6.72, 6.83). (This would result, for example, in much sensitive health information being outside the definition of 'personal information' and therefore exempt from even the data quality and data security principles.)
- removal of 'imminent' from the 'harm' exceptions at UPP 2.5(c); UPP 5.1(c) and UPP 9.1(b), (While acceptable in relation to ad hoc uses and disclosures, this opens the door for bulk and/or routine uses and disclosures justified on general public health or safety grounds.)
- increasing the freedom with which organisations are able to transfer personal information overseas, including to countries with weak or non-existent privacy laws (UPP 11). (The NSWLRC suggests following UPP11 (Proposal 14). We draw attention to HPP 14 in HRIPA which is in some ways stronger than both existing NPP 9 and proposed UPP 11. We analyse the Cross-border data flow issue in more detail in a separate paper.)

Missed opportunities to strengthen control or otherwise limit surveillance

- core definitions such as 'personal information' remain unchanged and can be easily avoided by new technologies that invade privacy without identification (see Chapter 6). The NSWLRC discuss related issues but have not yet made firm proposals (CP3 Chapter 5).
- failure to expressly address the complex issues of application of privacy principles to 'publicly available information'. (This is more comprehensively addressed by the NSWLRC at Issues 6 & 7.)
- failure to expressly include obtaining by observation, by extraction from other records, and by internal generation (from transactions) within a definition of collection (21.81) The

NSWLRC proposes the first of these inclusions (Proposal 11).

- failure to impose additional conditions on the collection of 'sensitive' personal information e.g. *express* consent, *specifically* authorised by law, serious *and imminent* threat. (ALRC 22.88, see also NSWLRC Issues 30 & 31.)
- failure to add 'specifically' to the 'authorised by or under law' exceptions at UPP 2.5(b); UPP 5.1(e); UPP 9.1(h); UPP 10.2(b) and UPP 11.1(c). (see Chapter 16)
- failure to recommend key elements of 'consent' which would make many of the principles more effective (e.g. to prevent self serving interpretation of 'bundled' and implied consent) (see Chapter 19).
- failure to recommend any direct regulation of automated decision-making (10.83) or data-matching (10-97) (the latter despite both the Privacy Commissioner and Parliamentary Committees having repeatedly recommended mandatory data-matching controls.)
- failure to extend the security obligation to expressly apply to collection – not addressed by the ALRC but suggested by the NSWLRC (Proposal 12).
- failure to relate the primary purpose(s) in relation to use and disclosure principles to the purpose *of collection* (i.e. not any subsequently defined purposes) – an issue not expressly addressed by the ALRC but canvassed by the NSWLRC (Issue 37).

Proposals relating to other objectives (downstream safeguards, or Rule's 'efficiency' functions of privacy laws) – these proposals would generally improve the level of privacy protection at the margins, but most have significant limitations – again missing the opportunity to further strengthen protection.

- Requirement to either destroy unsolicited information or apply principles (UPP 2.4). (Would ensure no personal information remains in unprotected 'limbo'). The NSWLRC raises the issue of whether unsolicited but retained information should be subject to all of the principles (Issues 38 & 39) – they clearly should.
- Application of the same notification requirements to both direct and indirect collection (UPP 3, and also NSWLRC Proposal 10).
- Data quality principle (UPP 7) strengthened to relate to all stages of information life cycle.
- Access and correction principle (UPP 9) generally strengthened (but the related consideration of interaction with the FOI Act is now in limbo following the government's withdrawal of the FOI reference from the ALRC).
- Third-party intermediary access to records where direct access by individual is exempted (UPP 9.3).
- Notification of corrections to previous third-party recipients of incorrect information (UPP 9.6(b)). (But only if both practicable and requesteded by individual).
- Requirement to disclose overseas transfer practices, and likely destinations, in privacy policies (UPP 4.1(c)). (But weakened by not also requiring any reference to overseas transfers in collection notices or disclosure of specific destinations on request).
- Requirement for disclosure of data breaches (Rec 51-1). (But the proposed implementation of this requirement is seriously flawed e.g. by leaving disclosure in effect to the discretion of the agency or organisation, by not allowing individuals to obtain more detail on request and by not making it a principle, meaning that individuals would be unable to take action to enforce the requirement).
- Openness principle improved by requirement to make privacy policies available electronically (UPP 4.2(a)). (But questionable whether ‘reasonable steps’ will require maximum accessibility).

Prescription vs Guidance

Trust in guidance misplaced in light of experience

The ALRC places far too great a reliance, throughout its report, on 'guidance' to be issued by the Privacy Commissioner. Without the missing upper levels of the 'responsive regulation' pyramid, as explained in Greenleaf & Waters's other paper for this symposium, any such guidance will likely suffer the same fate as the myriad guidelines, information sheets and other educational material issued by successive Commissioners for the last 20 years – that is, to be largely ignored. Commissioner's guidance is not and cannot be binding, and will have limited effect except in those areas in which it supports other imperatives, such as some aspects of quality and security. Where guidance seeks to divert the practices of business and government away from their all too frequent preference for greater privacy intrusion, it will only succeed if backed up by a significant volume of, and awareness of, effective enforcement.

Sectoral regulation

Open invitation for special pleading and weaker protection

In relation to sectoral regulation, the ALRC proposal to replace specific rules for health and credit information, and potentially for tax file numbers with Regulations under the Privacy Act is acceptable in principle, but dangerous without a guarantee, deliberately missing from the ALRC recommendations, that the default standards of the UPPs could only be *strengthened* and *not weakened*, by Regulation. This leaves privacy protection not only in these sectors, but also potentially in any other sector or activity, open to erosion by 'special pleading' from industy or professional lobby groups. While regulations are subject to Parliamentary approval, they inavariably receive less scrutiny, with less opportunity for other stakeholder input, than legislative amendments, and than is currently provided for in relation to the Credit Reporting Code of Conduct and Determinations, the TFN Guidelines and the health information Guidelines issued or approved by the Privacy Commissioner under the Act.

Both the credit reporting regime and the health guidelines can be seen as licences to depart from the normal application of key privacy principles (mainly the presumption of consent) in recognition of competing public interests (efficiency of financial markets and health research respectively). These concessions are balanced by additional procedural safeguards and more specific data quality and security standards. By providing for this balance to be determined in Regulations, the ALRC's proposals invite intensive lobbying by industry stakeholders, with an easier path to weakening of privacy protection in key sectors.

The NSWLRC suggests that there may no longer be a need for health specific privacy regulation in NSW if private sector providers are subject to the federal regime. This is a good example of where we could only agree if the Commonwealth regime was strong enough. In the absence of a clear 'consent' requirement for electronic health records (Health Privacy Principle 15 in the HRIPA) and if the application of the UPPs to health information could be weakened by Regulation, as proposed by the ALRC, this condition would not be met, and NSW should not surrender its higher standard of health privacy protection without insisting that it is replicated in any uniform model, and foregoing the ability to weaken it by Regulation (which, ironically, already exists and has been exercised under the NSW law[3)].

3 The effect of HPP 15 has been removed, by Regulation, in relation to the operation of the Healthelink project.