An overview of the ALRC privacy recommendations* - Best and worst aspects

*_For Your Information_, Report 108, Australian Law Reform Commission, May 2008

Graham Greenleaf, Professor of Law
Nigel Waters, Principal Researcher
Interpreting Privacy Principles Project

Cyberspace Law & Policy Centre, UNSW Faculty of Law

7 September 2008

Working notes only - for more detailed analysis which is under development. Most sectoral aspects (other than credit) not covered as yet. Please check with one of us before quoting or using. [graham@austlii.edu.au; nigelwaters@iprimus.com.au]

Best aspects of recommendations

Privacy Principles

- Unified Privacy Principles - Government agencies to be subject to same principles as private sector organisations – will generally result in enhanced protection (some exceptions)
- Recipients of unsolicited information must either destroy it or handle it according to UPPs (clarifies that unsolicited receipt can be 'collection').
- Notification of corrections to previous third-party recipients of incorrect information can be required.
- Clarification of anonymity principle to expressly include 'pseudonymity'.
- Openness principle improved by requirement to make privacy policies available electronically (but questionable whether 'reasonable steps' will require maximum accessibility).
- Direct marketing principle strengthened overall (but failure to define 'direct marketing' leaves loopholes).
- Data quality principle strengthened to relate to all stages of information life cycle.
- Third-party intermediary access to records where direct access by individual exempted.
- Access and correction principle 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).

- Extension of identifiers principle to identifiers issued by State and Territory agencies (but the principle should apply to Commonwealth agencies as well as organisations).
- Requirement to disclose overseas transfer practices in privacy policies (but weakened by not also requiring in specific collection notices or on request)
- The principle of a data breach disclosure requirement (but not its implementation).

Enforcement

- Appeals to the Courts against decisions of the Privacy Commissioner.
- A (limited) right to insist the Commissioner make a determination.
- Statutory action for privacy breaches ('privacy tort').
- Privacy impact assessments (PIAs) may be required for public sector proposals, and specifically for multi-purpose identifiers.
- Commissioner to be able to seek civil penalties for 'serious or repeated' breaches.

Exemptions and interactions

- Removal of unjustifiable exemptions ('small' business; employment records; political matters), and review of need for specific agency exemptions.
- Journalism exemption significantly improved and probably a reasonable compromise.
- Public intergovernmental framework for sharing of personal information by law enforcement and intelligence agencies and MoUs (though not public).
- Review of secrecy provisions in federal legislation to consider interaction with Privacy Act (already given to ALRC).
- Review of electoral roll issues.
- Statutory review of AML-CTF law to include specific privacy issues.
- State privacy legislation including complaint handling regulators, and consideration of federal override if no action by States.

Credit reporting

- Limited endorsement of more information for credit reporting with firm recommendation that further extension of more comprehensive reporting to include repayment history should be conditional on responsible lending legislation.
- Prohibition on credit reporting on minors (<18) and minimum loan amount threshold.
- Prohibition on use of credit reporting information for direct marketing, including pre-screening of direct marketing lists.
- Right of access to credit information files free of charge at least annually.

- Improved complaint handling obligations on credit providers including mandatory membership of an approved EDR scheme.

Worst aspects of recommendations

Privacy Principles

- Regulations can weaken (or strengthen) UPPs, with no requirements of public hearings or even consultation with Privacy Commissioner. Opportunity (but no guarantee) of Parliamentary scrutiny of regulations and requirement for consistency with objects are inadequate safeguards. The core of the Act can be destroyed by executive action.

- No attempt (despite claims) to 'future proof' the Act against technological changes, because core definitions such as 'personal information' remain unchanged and can be easily avoided by new technologies that invade privacy without identification. Proposed privacy tort is not a sufficient response.

- The data breach disclosure requirement is not a UPP (and so enforceable by individuals), but only enforceable by the State, via a civil penalty.

- The data breach disclosure requirement is incoherent and circular. It allows avoidance of disclosure of breaches, even to the Privacy Commissioner, on the basis of subjective judgments by the party in breach.

- Anonymity/pseudonymity principle does not apply to the design stage of information systems, only their subsequent implementation, thus allowing what is 'practicable' to be dictated by previous bad decisions.

- Notification requirements of disclosure practices remain too weak, including no obligation to give more detail on request.

- Failure to limit 'authorised by law' exception to use and disclosure and other principles with 'specifically' leaves it open (as now) to abuse.

- Identifiers principle does not apply to agencies, despite ALRC accepting that the objective of the principle is relevant to agencies.

- No overseas transfer of data can be a breach *per se*, no matter if the receiving country has no privacy laws at all. The onus (unfairly) shifts to the complainant to prove harm has occurred in some foreign location. Jurisdiction-based *prima facie* prohibitions on overseas transfers should be retained.

- The Privacy Commissioner plays no role in the proposed 'whitelist' of overseas jurisdictions. Unless the 'whitelist' is a legislative instrument, there will be no opportunity for parliamentary scrutiny. Even then, parliamentary scrutiny of regulations is inadequate with no guarantee of Privacy Commissioner and public input.

- Otherwise desirable requirement to disclose overseas transfer practices is limited to privacy policies, and does not apply to individual notices.

Enforcement

- Appeals structure is fundamentally flawed: Privacy Commissioner to retain right to dismiss complaints when Commissioner thinks respondent has dealt adequately with complaint, even if respondent does not; Extended discretion for Commissioner to not investigate 'when not warranted'; No right to insist on a determination where Commissioner dismisses complaint; No appeal against the Privacy Commissioner unless there is a determination. Commissioner can therefore avoid appeals, cover up mistakes.

- No requirement that PIAs be made public.

- Nothing recommended on increasing the transparency of the Commissioner's complaint reporting practices, which are at present discretionary, self-serving and inadequate.

Exemptions and interactions

- Exclusion of State/Territory laws dealing with 'the handling of personal information', without any recommendation of 'preserved matters'. This risks State/Territory surveillance control laws being eliminated with nothing to replace them.

- Unacceptable concession that data linkage arrangements with a third party intermediary holding the identification key amounts to 'non-identified', thereby removing any application of privacy principles.

Credit reporting

- Allows possibility that 'positive reporting' can be introduced by executive action with only inadequate opportunity, and no guarantee, of parliamentary scrutiny, without any requirement for an independent report concluding that credit granting practices really have changed.

- Recommendation for amendment of AML-CTF Act to allow use of credit reporting information for electronic identity verification purposes is inappropriate, going beyond terms of reference – needs debate in wider identity management context.

- Inadequate treatment of how credit reporting agencies should deal with identity crime.

- Failure to address issue of third parties requiring individuals to apply for access to their credit information files for purposes unrelated to credit assessment – continues to allow 'back-door' access to credit reports by parties who are prohibited from direct use of the credit reporting system.

General weaknesses / omissions

- Reliance on Parliamentary Counsel to deal with some wording issues which are significant enough to deserve specific recommendations.

- Excessive reliance on the Privacy Commissioner to provide 'guidance' on numerous crucial and difficult issues, when the Commissioner has a poor track record of giving effective guidance and non-binding guidance is too often not followed in any case.

- Failure to deal in any adequate way with:
    - the critical issues of consent, including 'bundled' consent and consent which is not free and revocable;
    - the exemption for 'generally available publications';
    - the regulation of automated decision making;
    - the regulation of data-matching and sharing;
    - personal information generated internally;
    - potential for abuse of 'serious threat' exception once additional 'imminent' test is removed;
    - the definition of 'transfer' for the purposes of the cross-border data flow principle; and
    - the timing of notification of proposed default listing with credit reporting agencies.
- Narrow definition of biometric information to be included in 'sensitive information'.
- Failure to support urgent intergovernmental action on residential tenancy databases.