Submission to Inquiry into the Privacy Amendment (Enhancing Privacy Protection) Bill 2012

Introduction

The Castan Centre for Human Rights thanks the Committee for the opportunity to comment on the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth).

This Bill introduces significant additional protections for personal information, which, as the accompanying Statement of Compatibility notes, are in keeping with the goals of article 17 of the International Covenant on Civil and Political Rights (ICCPR).

The Bill also strengthens the role of the Privacy Commissioner and extends the new, consolidated Australian Privacy Principles (APPs) to cross-border disclosures, which are welcome developments. Overall, the Centre does not demur from the Government's assertion that "[t]he Bill is compatible with human rights because it advances the protection of human rights, primarily protection against arbitrary interference with privacy, and, to the extent that it may also limit other human rights, those limitations are reasonable and proportionate."[1]

However, as the Centre noted in its submission on the Issues Paper *A Statutory Cause of Action for Serious Invasion of Privacy* in October 2011,[2] there is still effectively no enforceable, comprehensive right to privacy in Commonwealth law. The present Bill goes some way towards strengthening the current legislative regime, but our international obligations would be better fulfilled if it went further in accordance with the three recommendations below. The first five recommendations below relate to the scope of the *Privacy Act 1988* (Cth) (the Privacy Act), including problematic exemptions/exceptions, and the sixth relates to remedies.

[1] See Explanatory Memorandum, *Statement of Compatibility with Human Rights*.
[2] See <http://www.law.monash.edu.au/castancentre/publications/privacy-cause-of-action-sub.pdf>.

Scope of Privacy Act

The Bill's objects clause (section 2A) would insert as aims of the Act:

- To promote the protection of the privacy of individuals;
- to provide the basis for nationally consistent regulation of privacy and the handling of personal information, and
- to implement Australia's international obligation[3] in relation to privacy.

Privacy under international human rights law is a relatively broad concept. Article 17 of the ICCPR requires that "every person be protected against arbitrary or unlawful interference with his privacy, family home or correspondence."[4] The UN Human Rights Committee has emphasised that the terms in article 17 are not to be construed narrowly,[5] and that "[t]he obligations imposed by this article require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right."[6]

Act Title

In Australia, this obligation is implemented by a range of state, territory and Commonwealth legislation. The Privacy Act, although it purports to implement Australia's international obligations in relation to privacy and has a title which suggests broad application, is limited to the protection of personal information.

In its comprehensive review of Australia's privacy laws in 2009 entitled *For Your Information* (a report to which this Bill forms part of the Government response), the Australian Law Reform Commission (ALRC) found that most Australians incorrectly assume that intrusive practices such as surveillance, tracking and monitoring of correspondence, whether done by private or Government actors, are regulated by the Act,[7] whereas in fact they are mainly regulated under state and territory legislation. The ALRC recommended the Privacy Act be renamed the *Privacy and Personal Information Act* to reflect its ambit better.[8] In Victoria, the equivalent law is entitled the *Information Privacy Act,*[9] a title which would perhaps give a more accurate impression of the content of the Commonwealth legislation.

---

[3] The use of the singular here may be an error, as the Explanatory Memorandum speaks of 'international obligations' (at 217).
[4] This obligation is also reflected in article 16 of the Convention on the Rights of the Child.
[5] See eg UN Human Rights Committee, General Comment 16, UN Doc Ref. CCPR/C/GC/16, available at: <http://www2.ohchr.org/english/bodies/hrc/comments.htm> [1].
[6] Ibid.
[7] See *For Your Information: Australian Privacy Law and Practice*, ALRC Report 108: <http://www.alrc.gov.au/publications/report-108>, *Executive Summary,* 106-107.
[8] Ibid.
[9] Full title: *Information Privacy Act 2000* (Vic).

Recommendation 1: The Centre recommends the Committee consider whether the title and objects clause of the Privacy Act accurately reflect the fact that it implements only some of the Australian Government's international obligations in respect of privacy protection.

Definitions

Australians' privacy is under threat from a number of social and legal developments, including inadvertent exposure by the media or on the internet, as well as security and law enforcement measures such as telecommunications interception powers.

The Explanatory Memorandum to the Bill states that "[t]he proposed definition does not significantly change the scope of what is considered to be personal information."

The Centre understands that certain telecommunications metadata, such as visited IP addresses and geolocation data, do not come within the definition of 'personal information' under the Act. This, along with broad exemptions (see further below), may be a contributing factor the explosion in access to such data for law enforcement (both civil and criminal) under the *Telecommunications (Interception and Access) Act 1979*.[10]

If surveillance powers are expanded as proposed in the Government's recent *Equipping Australia against Emerging and Evolving Threats* Discussion Paper,[11] it will only increase the need for strong privacy protection (in addition to any safeguards incorporated into the interception legislation itself). The broad exceptions in proposed APP 3.4 (relating to the collection of sensitive personal information) should also be considered in this context.

Telstra recently admitted to sending customers' browsing habits to Canadian internet censorship specialist NetSweeper.[12] Once uncovered, this practice was widely condemned and prompted alarm amongst the corporation's customers.[13] Telstra's immediate reaction was to deny the information contained any personal identifiers (which would bring it within the purview of the *Privacy Act*).[14] Nevertheless Telstra ended the practice due to the negative publicity it had attracted.[15] An investigation into this affair by the Privacy

[10] See *Report on the Implementation of the Act for Year Ending 30 June 2011*: <http://www.ag.gov.au/Documents/Final+TIA+Act+Annual+Report+2010-11+-+amended+after+publication+-+v5+(3).pdf>, Chapter 6.
[11] See <http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/additional/discussion%20paper.pdf>.
[12] See Stilgherrian, '"It's how we connect:" Telstra and the spy sites mystery,' *Crikey*, 27 June 2012: <http://www.crikey.com.au/2012/06/27/its-how-we-connect-telstra-and-the-spy-sites-mystery>.
[13] See <http://exchange.telstra.com.au/2012/06/27/update-on-telstras-mobile-cyber-safety-tool>.
[14] Ibid.
[15] See <http://exchange.telstra.com.au/2012/06/28/further-update-telstra-smart-controls-cyber-safety-tool>.

Commissioner will be the third investigation of Telstra in a year,[16] which strongly suggests that stronger regulation is required to prevent this kind of repeat offending.[17]

Apart from a narrow definition of 'personal information,' the proposed APP8 does not include a requirement to notify customers of cross-border disclosures – this would be a good measure to address situations such as the latest Telstra controversy.

Recommendation 2: The Centre recommends the Committee consider whether the scope of the Privacy Act (as amended), including the definitions of 'personal information' and 'record,' is broad enough to cover new and emerging threats to Australians' privacy.

Recommendation 3: The Act should require companies to notify customers when their data is to be sent offshore, even if the potential for this to happen is covered in the company's privacy policy.

Small Business Exemption

Despite the intention "to ensure that the Privacy Act is given the widest possible operation consistent with Commonwealth constitutional legislative power,"[18] the Bill does not alter the fact that small businesses, political parties and law enforcement bodies are exempt from the operation of the Act (with the exception of some credit reporting obligations and foreign businesses). These exemptions were criticised by the ALRC in *For Your Information*.[19] Given the definition of small business as an organisation with a turnover of less than $3 million per year,[20] statistics suggest that more than 94% of Australian businesses are exempt from the federal privacy regime,[21] which severely limits its reach.

A prominent example of technological advances intruding into the private sphere in the business world is the use of scanners upon entry to certain premises. Clubs in Canberra have begun scanning drivers' licences to 'streamline' identification processes, reportedly with the intention of retaining the information gathered for up to seven years.[22] Identification scanners are openly marketed not just as security devices, but also integral components of customer databases which present marketing and screening opportunities (checking

[16] See 'Telstra privacy bungle "must not happen again,"' *iTnews,* 6 July 2012: <http://www.itnews.com.au/News/307846,telstra-privacy-bungle-must-not-happen-again.aspx>.
[17] The Commissioner found Telstra had breached the National Privacy Principles in July 2011 (<http://oaic.gov.au/publications/reports/own_motion_telstra_May_2011.html>) and in June (<http://www.theaustralian.com.au/australian-it/telecommunications/privacy-commissioner-timothy-pilgrim-will-probe-telstras-culture-in-light-of-privacy-breach/story-fn4iyzsr-1226412092746>).
[18] See Explanatory Memorandum, 222.
[19] See ALRC 108, *Executive Summary*, above n 7, 113-115. See also Recommendations 39-1 and 41-1.
[20] *Privacy Act 1988*, s 6D.
[21] According to the Australian Bureau of Statistics *8165.0 - Counts of Australian Businesses, including Entries and Exits, Jun 2007 to Jun 2011,* only 5.9% of Australian businesses have a turnover of more than $2 million.
[22] See Knaus, 'ACT Clubs Scanning Your Licence,' *The Canberra Times*, 23 July 2012: <http://www.canberratimes.com.au/act-news/act-clubs-scanning-your-licence-20120723-22j5l.html>.

whether someone is on a 'VIP' list, whether they usually pay a cover charge etc).[23] In Victoria[24] and Queensland,[25] nightclubs have begun using biometric scanners to collect facial, fingerprint and even iris data,[26] in some cases storing it in central repositories to create lists of troublesome patrons.[27] Given the increasing use of biometrics to secure other data (including financial data), possession of such data by unaccountable companies presents an emerging fraud risk as well as a privacy risk. It is positive that the definition of 'sensitive information' is being amended to include biometric data.

The stated goals of those using the scanners are improvements in efficiency (compared with manual identification verification procedures) and patron safety. Human rights law allows for limitations on the right to privacy, but if the intrusiveness of the measures outweighs the importance of the goals, they may become arbitrary in breach of article 17 of the ICCPR.[28] To minimise the chances of such a breach, the Privacy Commissioner should be empowered to take direct action against, for example, those who retain data which is not required to carry on their business (see further below). The former Privacy Commissioner, Karen Curtis, released an Information Sheet for pubs and clubs in 2010,[29] but this response was criticised as inadequate by the Privacy Foundation.[30]

In any case, many of these businesses may well be exempt from the operation of the Act. Australian Bureau of Statistics figures for pubs and bars reveal an average turnover of around $3.2 million per year.[31] It is therefore reasonable to infer that a significant proportion of venues make less than the $3 million threshold.

Political Party Exemption

The exemption for political parties may be justified in the name of protecting other rights, including the implied right to freedom of political communication in the Constitution[32]

---

[23] See eg JS Security's 'Clubscan': http://www.jssecurity.com.au/clubscan>.
[24] See eg 'Face recognition technology for clubs,' *ABC PM*, 4 May 2010: <http://www.abc.net.au/pm/content/2010/s2890212.htm>.
[25] See eg 'Brisbane nightclubs to introduce fingerprint scanning,' *The Courier Mail*, 23 November 2009: <http://www.couriermail.com.au/news/queensland/brisbane-nightclubs-to-introduce-fingerprint-scanning/story-e6freoof-1225802718506>.
[26] See eg Norman, 'Stripped of civil liberties for a night on the town,' *The Punch,* 23 January 2012: <http://www.thepunch.com.au/articles/Stripped-of-civil-liberties-for-a-night-on-the-town>.
[27] See 'A Big Night Out: Drinking, Dancing, Fingerprinting,' *The Sydney Morning Herald*, 27 March 2010: <http://www.smh.com.au/technology/technology-news/a-big-night-out-drinking-dancing-fingerprinting-20100326-r31s.html>.
[28] See UN HR Committee, General Comment 16, above n 5, [4]; also eg *Pinkney v Canada* (HR Committee Communication 27 of 1978).
[29] See <http://www.privacy.gov.au/index.php?option=com_icedoc&view=types&element=infosheets&fullsummary=7074&Itemid=1021>.
[30] See 'Face recognition technology for clubs,' *ABC PM,* above n 24.
[31] See <http://www.abs.gov.au/ausstats/abs@.nsf/mf/8687.0>.
[32] See *Australian Capital Television Pty Ltd v Commonwealth* [1992] HCA 45.

(associated with rights in respect of freedom of expression and political participation in the ICCPR[33]). However, the lack of transparency and oversight in this area is a concern given the reported nature of the major parties' voter databases, and has been strenuously criticised.[34] The capacity for such databases to favour incumbent parties over those with fewer data-harvesting resources has also drawn comment, and may undermine the argument that maintenance of these databases has a net positive effect on Australian democracy.[35]

The definition of 'sensitive data' in the Act includes information about a person's political opinions, beliefs and membership of political associations,[36] which places such data in the category most in need of protection. In addition, comparable jurisdictions including the UK and NZ seem to be able to conduct election campaigns effectively without such a broad exemption,[37] which further calls into question claims that the exemption is necessary to "enhance the operation of the electoral and political process in Australia."[38]

Law Enforcement Exceptions

With a few exceptions, Australian law enforcement bodies are covered by the Information Privacy Principles and will continue to be covered by the new APPs. However, a new definition of 'enforcement related activity' in section 6 (to be used in several exceptions to the APPs relating to accessing and sharing personal information[39]) is of concern. The definition encompasses criminal investigations, which is unexceptionable, but it also covers prevention and investigation of 'breaches of a law imposing a penalty or sanction,' with no minimum seriousness requirement.

The Attorney-General's Department report on the operation of the *Telecommunications (Interception and Access) Act 1979* for the year ending 30 June 2011[40] revealed that 8,000 "authorisations made for access to existing information or documents in the enforcement of a law imposing a pecuniary penalty or the protection of the public revenue" were issued during 2010-11, up from 6,583 the previous year.[41] These authorisations can be made without external scrutiny[42] and they have been granted to bodies including local councils, Australia Post and even the Victorian Taxi Directorate. Given the relatively minor nature of

[33] See articles 19 and 25.
[34] See eg Van Onselen, 'Political parties face hard questions on how they use our personal data,' *The Australian*, 26 July 2011: <http://www.theaustralian.com.au/national-affairs/political-parties-face-hard-questions-on-how-they-use-our-personal-data/story-fn59niix-1226101670023>.
[35] See eg Van Onselen, Political Databases and Democracy: Incumbency Advantage and Privacy Concerns, Democratic Audit of Australia, October 2004: <http://democratic.audit.anu.edu.au/papers/200410_van_ons_dbases.pdf>.
[36] *Privacy Act 1988* (Cth), s 6.
[37] See ALRC 108, above n 7, *Executive Summary*, 113-114.
[38] See ALRC 108, above n 7, *Political Exemption* (Chapter 41).
[39] The Bill proposes to incorporate these exceptions into some of the most important APPs – 6, 8 and 9.
[40] See *Report on the Implementation of the Act for Year Ending 30 June 2011*, above n 10.
[41] Ibid, Table 58.
[42] See *Telecommunications (Interception and Access) Act 1979,* s 179.

the civil offences which these bodies are likely to be investigating, they should not benefit from a blanket exception from several of the relevant APPs.

Recommendation 4: The Centre recommends that the Committee consider whether Australians' right to privacy can be protected effectively while the Privacy Act covers neither small businesses nor political parties. In the Centre's view, these exemptions create overly large gaps in protection.

Recommendation 5: The Centre recommends that the definition of 'enforcement related activity' be tightened to allow invasions of privacy only for investigating serious breaches of the law.

Powers and Resources of the Privacy Commissioner and Legal Remedies

In *For Your Information*, the ALRC called for the Privacy Commissioner to be able "to seek a civil penalty in the federal courts where there is a serious or repeated interference with the privacy of an individual,"[43] and for Deputy Privacy Commissioners to be appointed to handle the continually-increasing workload.[44] It also called on the Government to develop a statutory cause of action for serious breaches of privacy.[45] The present amendments address the first of these recommendations (through proposed section 13G).

However, the Bill does not clarify the Government's position on a private right of action for serious breaches of privacy, which was the subject of a Government Issues Paper released in September 2011.[46] In a response to this Issues Paper in October 2011,[47] the Centre highlighted the need for statutory remedies for serious breaches of privacy in addition to extra powers for the Information/Privacy Commissioners. The Bill falls short in this respect.

Recommendation 6: In order to improve compliance with article 2(3) of the ICCPR, which requires effective remedies for breaches of other articles including article 17, the Centre recommends that the Bill be amended to include a cause of action for serious breaches of privacy. This cause of action should incorporate a range of remedies as set out in the ALRC's Discussion Paper 72[48] and reiterated in *For Your Information*.[49]

---

[43] See ALRC 108, *Executive Summary*, above n 7, 117. See also Recommendation 50-2.
[44] Ibid.
[45] Ibid, 126-127.
[46] See <http://www.dpmc.gov.au/privacy/causeofaction/docs/issues%20paper_cth_stat_cause_action_serious_invasion_privacy.pdf>.
[47] See above n 2.
[48] See *Review of Australia's Privacy Law:* <http://www.austlii.edu.au/au/other/alrc/publications/dp/72>.
[49] See ALRC 108, above n 7, *Protecting a Right to Personal Privacy* (Chapter 74).