

Protecting Privacy while Responding to Terrorism



Issue

Governments have a duty to protect the rights, lives and safety of people within their territory from legitimate threats of terrorist attacks. However, protecting the community from terrorism and protecting human rights are not mutually exclusive. The Counter Terrorism White Paper makes this point clearly.¹ Both have the ultimate objective of protecting and promoting the inherent dignity and safety of human beings.

In its 2010 Counter-Terrorism White Paper,² the Government stated its intention to use or expand the use of certain national security measures such as a biometric-based visa system (using fingerprints and facial images), increased sharing of biometric data between government agencies and internationally, and increased border security measures, including body scanners at international airports.

In his December 2009 report to the UN Human Rights Council, the Special Rapporteur on Human Rights and Counter-Terrorism highlighted the erosion of the right to privacy that has occurred in the global fight against terrorism (the **Special Rapporteur's report**).³ The Special Rapporteur identified certain measures as being potentially incompatible with the right to privacy, many of which are the very surveillance and border control measures proposed in the Australian Government's White Paper.⁴

The Special Rapporteur provides a framework for protecting Australia from terrorism while simultaneously protecting the community from undue violations of privacy rights. In short, the Special Rapporteur urges States to assess how counter-terror laws, policies and practices that intrude on privacy are necessary and proportionate by implementing the following principles:

- **Minimal intrusiveness:** public authorities should exhaust the least intrusive techniques before resorting to others;
- **Restrictions on secondary use:** public authorities should only use information for the purpose for which it was obtained, and should provide a legal basis for any reuse of information;
- **Oversight and regulated authorisation of access:** states should establish independent scrutiny of surveillance practices and techniques to ensure accountability and proportionality;
- **Transparency and integrity:** public authorities must be open about surveillance practices; and
- **Effective modernisation:** public authorities should use tools such as privacy impact assessments to ensure that new technologies are utilised appropriately and effectively.

Opportunity and Imperative for Action

The Special Rapporteur's report is an opportunity for Australia to take the lead both nationally and internationally on national security and privacy issues.

- The Special Rapporteur recommends that the Human Rights Council take measures to create a new declaration on data protection and data privacy in light of the impacts of counter-terrorism measures.⁵ Australia has the opportunity to play an international leadership role in the development of a new international instrument for the protection of privacy.⁶
- Leadership by Australia on protection of privacy in the counter-terrorism context would reinforce two pillars of Australia's bid for a seat on the UN Security Council, namely: building a secure

future; and respecting human rights.⁷ It would also underline Australia's commitment to the UN counter-terrorism conventions and protocols.⁸

- Protecting human rights and privacy in accordance with the Special Rapporteur's report would bolster and enhance the Government's aims and objectives as set out in the Counter-Terrorism White Paper, in particular:
 - pursuing a principled and proportionate response to terrorism that promotes the values we seek to protect⁹ and ensuring that, in responding to terrorism, Australia meets its obligations under the ICCPR;¹⁰
 - building resilience in our community by maintaining our open democratic society and supporting and protecting the values and freedoms from which all Australians benefit;¹¹ and
 - ensuring that domestic efforts to counter terrorism are informed by best practice models internationally.¹²

It is imperative that Australia act now because:

- There is growing concern about the privacy implications of the development and use of new technologies, such as the collection of biometric data and the use of body scanners at airports.¹³ The measures proposed in the Counter-Terrorism White Paper have already raised concerns in the community about the impact on privacy.¹⁴
- The legal safeguards of privacy in Australia remain limited. Neither the Australian Constitution nor any state or territory constitutions contain any express provisions relating to privacy. The unauthorised collection and disclosure of private information is only protected in a limited way, and intelligence agencies are generally exempt from these laws.¹⁵
- Australia is bound by its international obligations to take all legislative, policy and other measures to properly respect the right to privacy in Australia.¹⁶
- Over the last decade, the Australian Government has enacted almost 50 pieces of anti-terrorism legislation and the intelligence gathering and surveillance powers of intelligence agencies have been broadened significantly. In the absence of any comprehensive human rights framework there has been insufficient parliamentary or other scrutiny of the human rights impacts of these laws, including the right to privacy.¹⁷

Recommendations for Action

The Australian Government should become a world leader in protecting the rights of its people to be safe from both terrorism and from undue interference with privacy. The Australian Government should implement the report of the Special Rapporteur in the following ways:

International Action

1. Australia should adopt the best practices and recommendations set out in the Special Rapporteur's report as the underlying principles of Australian policy in relation to counter-terrorism and privacy protection.

2. Australia should champion the development of a new global declaration on data protection and privacy, working through the Human Rights Council, and in consultation with like-minded States.¹⁸
3. As an aspect of Australia's candidacy for the UN Security Council, it should commit to further mainstreaming human rights considerations, including the right to privacy, in the work of the UN Security Council Counter Terror Committee.
4. Australia should support the development of a programme for global capacity building on privacy protection, with the intention of counterbalancing the global trend of counter-terrorism laws that infringe on privacy.¹⁹

Domestic Action

For Australia to have credibility in its international position, it must ensure that its own house is in order. To that end, Australia should take the following steps to improve the protection of the right to privacy in domestic laws and policies:

1. The National Security Legislation Monitor should immediately review all counter-terrorism, intelligence gathering and surveillance laws to ensure that they are precise and proportionate to the security threat and contain appropriate safeguards against abuse.²⁰ The NSL Monitor should specifically use the Special Rapporteur's framework to analyse the impact of counter-terror laws on the right to privacy.
2. The Australian Government should strengthen privacy protection in Australian law, by ensuring that the law provides not only comprehensive data protection, but broader personal privacy protection, in a manner that reflects international human rights standards. Such a law could regulate, for example, the use of intrusive border control measures such as body scanners, and apply the principles of necessity and minimal intrusiveness. To the extent it does not do so currently, the law should:
 - ensure that there are clear legal protections for individuals that prevent excessive collection of personal information;
 - impose restrictions on secondary use of information and regulate the storage and sharing of information;
 - require individuals to be notified of how information is used; and
 - provide rights of access and remedies for improper violations of privacy.

The Government might either expand the scope and function of the *Privacy Act* (Cth) or create a new stand alone privacy law.

3. In relation to Australia's intelligence and defence intelligence agencies, the Government should implement the Australian Law Reform Commission's (**ALRC**) recent recommendations by:
 - requiring that the privacy rules and guidelines applicable to Australia's intelligence and defence intelligence agencies be updated to include rules that deal with the incorrect use and disclosure by those agencies of all personal information, the accuracy of records and the storage and security of personal information;

- requiring that the National Security Legislation Monitor, the Inspector General of Intelligence and Security, the Privacy Commissioner and the Minister responsible be consulted in the process of making the privacy rules and guidelines; and
 - ensuring that the privacy rules and guidelines governing Australia's intelligence and defence intelligence agencies be made accessible to the public.²¹
4. All current and new Government policies, including the policies contained in the Counter-Terrorism White Paper, should be subject to Privacy Impact Assessments (**PIAs**). The Government should implement the ALRC's recommendation that the Privacy Commissioner be empowered to request and oversee PIAs and that the Privacy Commissioner produce guidelines to assist departments and agencies in the preparation of PIAs.²² PIAs would:
- consider how the policy and any technologies used create privacy risks;
 - contain an assessment of the principles of proportionality and necessity in accordance with human rights standards, and
 - state measures taken to guard against abuse of privacy in the policy.
- Assessments at policy development stage would also ensure that privacy is considered at the earliest stage of policy formulation.²³
5. The policies and practices of Australia's security and intelligence agencies should be subject to particularly strong oversight given those agencies' use of intrusive surveillance techniques and the processing of personal information. The oversight should take specific account of the proportionality of any intrusive measures and whether the intrusion on rights is the minimum necessary to achieve the security or intelligence outcome. Oversight should be as transparent as possible and should be conducted by an independent body that is properly resourced and has appropriate human rights and privacy expertise. Appropriate bodies to conduct this function may include the Inspector-General of Intelligence and Security, the Privacy Commissioner, the Information Commissioner or the Australian Human Rights Commission. Any decision made by that body should be subject to merits review in the Administrative Appeals Tribunal, with rights to appeal questions of law to the Federal Court.
6. Given that new technologies both enhance the ability of Australia to protect its people from terrorism but also threaten to violate privacy, the Government should invest in any features of new surveillance or other technologies that make the technologies less restrictive on the right to privacy.

About the Human Rights Law Resource Centre

The Human Rights Law Resource Centre is a leading national community legal centre. The Centre promotes and protects human rights in Australia. We contribute to the alleviation of poverty and disadvantage, and the promotion of equality and fair treatment.

¹ The Counter-Terrorism White Paper clearly states that in responding to terrorism Australia is committed to meeting its obligations under the ICCPR (56), including the right to privacy (58).

² Department of Prime Minister and Cabinet, *Counter-Terrorism White Paper: Securing Australia, Protecting Our Community* (2010).

³ M Scheinin, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, UN Doc A/HRC/13/37, 28 December 2009.

⁴ The Special Rapporteur pointed to the global increase in stop and search powers; the increasing use of biometric techniques such as facial recognition, fingerprinting and iris scanning; the circulation of secret watch lists; and, increased monitoring, regulation, interference and control of movement at State borders.

⁵ Special Rapporteur's Report, [73].

⁶ A number of countries have expressed positive interest in such a declaration, including China, Norway, France and Finland.

⁷ These are two of four pillars upon which Australia has built its candidacy: www.dfat.gov.au/un/unga.html.

⁸ As expressed in the Counter-Terrorism White Paper: 56.

⁹ Counter-Terrorism White Paper, [3.2.4].

¹⁰ Counter-Terrorism White Paper, 56.

¹¹ Counter-Terrorism White Paper, 20.

¹² Counter-Terrorism White Paper, 21.

¹³ The ALRC stated that 'rapid advances in information, communication and surveillance technologies have created a range of previously unforeseen privacy issues'. The introduction of body scanners created intense media scrutiny in January and February 2010, and drew condemnation from a broad range of stakeholders, including airlines, see www.theaustralian.com.au/travel/backlash-to-airport-body-scans/story-e6frg8f-1225817485755.

¹⁴ See *Herald Sun*, 23 February 2010, www.heraldsun.com.au/news/breaking-news/measures-in-counter-terror-white-paper-are-invasion-of-privacy-say-civil-libertarians/story-e6frf7jx-1225833306737.

¹⁵ The *Privacy Act 1988* (Cth) is the key federal law that protects against unlawful interference with personal information. Australia's intelligence and defence intelligence agencies are either partially or wholly exempt from the operation of the *Privacy Act*. Acts of ASIO, ASIS and the ONA are completely exempt by virtue of sections 7(1)(a)(i)(B) and (2)(a) of the *Privacy Act*.

¹⁶ Australia is a party to the ICCPR. Article 17 of the ICCPR protects the right to privacy.

¹⁷ There is bipartisan recognition of the need to review and possibly recalibrate the relationship between counter-terror measures and privacy: see, eg, the Hon Joe Hockey MP, 'In Defence of Liberty', Address to the Grattan Institute, Melbourne, 11 March 2010 at <http://joehockey.com/useruploads/File/InDefenceOfLiberty.pdf>.

¹⁸ This is the Special Rapporteur's recommendation at [73].

¹⁹ See Special Rapporteur at [72].

²⁰ This reflects the recommendation of the Special Rapporteur at [60].

²¹ See Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008), recommendations 34-1 to 34-4.

²² *Ibid*, recommendations 47-4 and 47-5.

²³ See Special Rapporteur at [63] and [67].