Submission No 109

Inquiry into potential reforms of National Security Legislation

Organisation: Office of the Victorian Privacy Commissioner

Office of the
Victorian Privacy
Commissioner

Office of the Victorian Privacy Commissioner

Submission to the Joint Parliamentary Committee on Intelligence and Security

on the

Inquiry into potential reforms of the National Security Legislation

20 August 2012

Office of the Victorian Privacy Commissioner (Privacy Victoria)
GPO Box 5057
10-16 Queen Street
Melbourne Victoria 3000
Australia
Phone: 1300-666-444
Fax: +61-3-8619-8700
Email: enquiries@privacy.vic.gov.au
Website: www.privacy.vic.gov.au

Introduction

1 Privacy is not an absolute right. A balance must be struck between privacy and other rights, including the public interest in protecting the safety and security of Australians. This balancing act is a central tenet to privacy legislation around the world, and at times privacy must give way to other public and private interests.[1] There is no doubt that national security is in the public interest; however, most security operations – such as searches, interceptions or warrants – are by their nature privacy invasive. Any extension of such invasions requires careful scrutiny and deliberation. Since 2001, the enactment of multiple terrorism laws has progressively stripped away many civil rights formerly built up under the common law for hundreds of years. Preserving these rights – such as the right to privacy – is essential to maintaining a democratic and free society.

2 Where the state seeks to encroach into privacy and other civil liberties through the exercise of intrusive powers, such powers should be:

- exercised for *legitimate* purposes and not for improper reasons;
- used only when *necessary* and not arbitrarily or without reasonable cause;
- carried out in a way *proportionate* to their need and not in a manner that is excessively intrusive or to an extent that is overly broad; and
- shown to be *effective* in achieving their legitimate aims, with appropriate transparency in reporting outcomes and periodic review to ensure ineffective practices are modified or ceased.[2]

3 The Australian Government's Discussion Paper proposes amendments to existing legislation and additional proposals, both of which threaten to have an adverse and significant effect on the privacy rights of individuals across Australia. This submission considers that, in general, the introduction of intrusive powers suggested in the Discussion Paper fails to achieve those tests of legitimacy, necessity, proportionality and effectiveness.

4 In 2003, the first Victorian Privacy Commissioner, Paul Chadwick, made a submission to the Victorian Parliament Scrutiny of Acts and Regulations Committee in relation to the proposed *Terrorism (Community Protection) Bill 2003* (Vic), which proposed to extend investigatory powers to prevent or respond to potential threats of terrorism.[3] In that submission, he made comments regarding the erosion of civil liberties – including privacy – which bear repeating in the context of the Discussion Paper:

> Where government seeks to introduce measures that restrict civil liberties, of which privacy is a slice, it must do so only to the extent that is necessary to achieve the legitimate aim underlying the proposals. A democratic nation is not secured by compromising, any more

[1] See, for example, *Information Privacy Act 2000* (Vic) s 5.
[2] As detailed in the submission by the first Victorian Privacy Commissioner, Paul Chadwick, to the Victorian Parliament's Law Reform Committee on its Inquiry for Warrant Powers and Procedures, 2004, p 1, available at http://www.privacy.vic.gov.au.
[3] Available at http://www.privacy.vic.gov.au/privacy/web2.nsf/files/terrorism-community-protection-bill-2003.

> than strictly necessary, the freedoms that allow a democracy to function. Preserving freedoms under law is part of what it means to guard the national security of a democracy. To diminish freedoms unnecessarily or disproportionately makes the nation insecure.
>
> Secret policing, covert searches, surveillance, information that cannot be tested for accuracy, closed decision-making, absence of independent scrutiny of government agencies: these are all hallmarks of systems of government that democratic nations tend to want to secure themselves against.
>
> Where any such measures are adopted by democracies, they are adopted reluctantly because they are an aberration from the norm, which is freedom and democratic governance. The norm is accountable policing; minimal and overt search, seizure and surveillance; and a presumption of open government, with necessary, clearly defined exemptions subject to independent review.
>
> The security of the Australian nation's way of life depends on these norms being preserved. ... Fear can make us welcome what should be only reluctantly and warily tolerated. The measures [in the Bill] are an unwelcome necessity for a democratic society that prizes advocacy, dissent and diversity. They ought to be viewed cautiously, their necessity queried rigorously, and the safeguards against their misuse built carefully and applied scrupulously.

5 I reiterate these comments and highlight their relevance in the context of the Discussion Paper.

6 Privacy laws in Australia were passed in part to ensure that individuals can use technological systems while maintaining personal privacy. For instance, in the second reading speech for the *Information Privacy Act 2000* (Vic),[4] it was recognised that privacy laws increase the trust and willingness of citizens to embrace and take full advantage of information systems. The laws – based on the OECD Privacy Principles – were drafted to be technologically neutral.

7 It is axiomatic that technology has advanced to such an extent that the telecommunications laws drafted in the 1970s can be considered outdated. However, when revising these laws, the goal should not be to lower protections contained within, but rather to standardise and enhance existing protections irrespective of the method of communication (that is, to make the laws technologically neutral). The terms of reference in the Discussion Paper state that this is one aim of the proposals. To that end, I support changes to accomplish this.

8 However, many of the suggested amendments go far beyond this approach. The terms of reference note that the Committee should have regard to whether the proposed responses contain appropriate safeguards for protecting the human rights and privacy of individuals and are proportionate to any threat to national security. While I acknowledge that many of the proposals in their current format are only considerations, it is my view that many of the proposed changes in the Discussion Paper exceed what is

[4] Victorian Parliament, *Hansard*, House of Representatives, 26 May 2000.

necessary to achieve appropriate balance between national security and other human rights such as privacy.

9 The Discussion Paper notes that at least four terrorist attacks have been thwarted since 2001. It therefore stands to reason that the current legislative regime has been at least somewhat effective in achieving its primary goal: protecting the national security of Australians. But while these threats are to an extent 'real', increasing powers of search and surveillance must be met with caution and circumspection.

10 This submission focuses on some of the proposals in the Discussion Paper that have significant impacts upon the privacy of individuals.

Privacy protections and objects clause in the TIA Act

11 The Discussion Paper explains that reforms may be developed to strengthen the safeguards and privacy protections of the interception regime in line with "contemporary community expectations". In general terms, I recognise that the telecommunications environment has shifted from simple telephony to the internet, mobile phones and social media. Accordingly, there are parts of the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**) which are no longer aligned with current technological standards. I acknowledge that some of the proposed changes to the TIA Act are simply to clarify and simplify.

12 However, it is important that we consider what "contemporary community expectations" regarding privacy actually are. For example, in 2007 the Office of the Privacy Commissioner commissioned a survey into community attitudes to privacy.[5] This survey was undertaken at the cusp of the social media boom. In the survey, 86% of respondents felt that it was a serious breach of privacy where a government department monitors an individual's activities on the internet, recording information on sites visited without the individual's knowledge. Similarly, 50% were more concerned than two years previous (2005) about providing information over the internet. I consider that these numbers would be greater today, given the mass of information collected by electronic means.

13 This matches my experience at this Office. I consider that, while people may share personal information about themselves and their friends to a greater extent, in general people are more concerned about privacy in the 'information age' than previously was the case. It is therefore incumbent upon legislators that terrorism legislation does *not* reduce privacy protections but rather should afford more protections and safeguards.

14 I support the inclusion of a 'privacy focused objects clause', but note that it would not be completely effective to mitigate proposed privacy intrusions. An objects clause alone does not provide sufficient protection to privacy. Privacy, as a human right, needs to be protected in the substantive legislation, not merely given lip-service in an objects clause.

[5] Office of the Australian Privacy Commissioner, 'Community Attitudes to Privacy', 2007, available at: http://www.privacy.gov.au/aboutprivacy/attitudes.

In my view, while the Discussion Paper discusses strengthening safeguards and privacy protections, the substance of the reforms do not achieve this.

Variation and duration of warrants

15 The Discussion Paper states that currently, the *Australian Security Intelligence Organisation Act 1979* (Cth) (**ASIO Act**) does not specifically provide for a warrant to be varied if the circumstances "justify" such a variation. The Discussion Paper proposes that a variation provision may be appropriate to ensure there is sufficient "operational flexibility" while maintaining appropriate accountability.

16 This is concerning given the breadth of the term "operational flexibility". In my view, the level of variation required needs to be carefully considered and should be extremely limited. Courts are (rightly) vested with authority to grant warrants; allowing "operational flexibility" to vary a warrant could potentially allow extension of a warrant beyond what was authorised by a court.

17 Similarly, increasing the duration of a search warrant from 90 days to six months should require judicial authority. Such a change also requires considerable justification given that extensive warrants would likely intrude upon civil and privacy rights.

Authorised intelligence operations scheme

18 One matter the Government is considering is amending the ASIO Act to create an "authorised intelligence operations scheme". Part of this proposal is to allow ASIO officers and human sources operating under the ASIO Act to be issued with a certificate protecting them from criminal and civil liability for specific conduct for a specified period (such as 12 months). The Discussion Paper notes that there will be oversight and inspection regimes, certain conduct which cannot be authorised, and an independent review of the operation, effectiveness and implications of the scheme after five years.

19 In general, I consider this proposal concerning. The proposal needs to be justified on the basis that ASIO officers and human sources have been and continue to be prosecuted or sued civilly for conduct committed while undertaking intelligence operations. Such a justification is not detailed in the Discussion Paper; nor has evidence been put forward to justify the necessity of such an amendment.

20 One particular type of conduct by ASIO officers that may be relevant to terrorism offences is false imprisonment. I am unwilling to give support to a scheme that permits ASIO officers to commit a crime to which they are immune to prosecution and would have significant impacts upon the privacy of an individual (that of arbitrary and illegal detention). In my view, this undermines other protections in legislation and the common law and would permit intrusion into an individual's privacy that may otherwise be illegal.

Named person warrants

21 The Discussion Paper notes that, in approximately one third of cases, more than one ASIO Act warrant type is sought against a particular "target" (an individual). This currently requires multiple applications and re-casting of the case. Accordingly, the proposal is to allow ASIO to apply for a single warrant governing all ASIO Act warrant powers.

22 I consider that this proposal is questionable. Certain warrants are more invasive than others. A court may find that, based on particular circumstances, one type of warrant is justified (eg a search warrant), but another type of warrant unjustified (eg an interception warrant). The proposal presumes that the level of intrusiveness into an individual's privacy and liberty is the same for all warrants, which is not the case. For instance, a search of an individual's premises is entirely different to intercepting all communications that person has over any telecommunications system.

Person searches

23 The ASIO Act currently contains the power to search a premises, including the power to search persons "at or near" the premises. The proposal is to enable ASIO to request a warrant to search a specified person rather than premises (subject to the existing safeguards) so that there would be sufficient "operational flexibility" while maintaining appropriate accountability via the warrant process.

24 While details of whether or not such a change is necessary are not described in the Discussion Paper, this proposal is concerning, as it is a significant departure from the traditional search warrant procedure. I consider an alteration of the warrant procedure in such a fashion to be extraordinarily broad and intrusive. It would have a serious adverse impact on an individual's privacy, may unduly infringe a number of human rights and freedoms (such as the freedom from arbitrary search and seizure), and interfere with the privacy of one's home and family. In particular, despite the safeguards in place, there is a possibility of using a person search to repeatedly harass a target at multiple locations (eg work, home, in a public space etc).

Use of third party computers and communications in transit

25 The Discussion Paper notes that advancements in technology have made it increasingly difficult for ASIO to execute its computer access warrants due to "security conscious" targets. The proposal is to amend the ASIO Act to enable a third party computer or communication in transit to be used by ASIO to "lawfully access a target computer". The Discussion Paper notes that this would have "privacy implications", and that appropriate safeguards and accountability mechanisms would need to be incorporated into such a scheme.

26 In my view, this proposal is completely unjustified. To access a third party's computer which has no connection with the target is extraordinarily broad and intrusive. These are powers usually characteristic of a police state. Adversely impacting the privacy of an individual (the third party) should only be permitted in the most extreme circumstances as a 'last resort' when all other methods have been exhausted. Furthermore, the power to alter (rather than 'access') a third party computer should not be permitted.

27 Even with such safeguards and accountability mechanisms (which are not detailed in the Discussion Paper), I cannot support a measure that could severely diminish the privacy of individuals and could cause a chilling effect on the way that individuals communicate and use technology.

Incidental entry

28 ASIO are seeking "clarification of the scope of the incidental power" to assist it in executing search and computer warrants, including "entry into a third party's premises for the purpose of installing a surveillance device".

29 In my view, should ASIO wish to install a surveillance device, it should be required to obtain a fresh warrant, rather than relying upon an "incidental" power of an existing warrant to do so. ASIO should also be required to notify the third party whose premise is being used except in the most extreme of cases. Similar to the above, where an intrusion into a third party's home is required, substantial justification should be given and a separate warrant issued.

30 Any encroachment into the privacy of a person's domicile should be treated seriously and should only occur when absolutely necessary. This is an essential principle of human rights law, mentioned in the *International Covenant on Civil and Political Rights* (Article 17), which states that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence.

Offence for failure to assist in decryption of communications

31 The Discussion Paper notes that the Government is also seeking the view of the Committee as to whether to establish an offence to fail to assist in the decryption of communications.

32 This is a concerning proposal. Again, the lack of detail around possible penalties to whom they would apply makes it difficult to provide relevant comments. At the very least, any such proposal would need to be subject to a court order.[6]

33 Should the offence be directed against an individual, it is my view that the proposal would seriously undermine the privilege against self-incrimination. Unlike the United

[6] I note that similar a provision (requiring a warrant) exists in the *Cybercrime Act 2001* (Cth).

States' Fifth Amendment,[7] the privilege in Australia mostly stems from common law[8] and has at its crux the principle that an individual should not have to provide evidence against himself or herself. This is an important protection that ensures the right to a fair trial and that the prosecution prove its case.

34 It may also be technologically possible to encrypt transmissions and/or data so that even the user themselves does not know, or the user has forgotten, the decryption key. This could create a situation where a user is ordered to produce a decryption key, but is unable and 'fails' to do so, and is therefore subject to a criminal penalty – which is an undesirable outcome.

The two-year 'data retention scheme'

35 The proposed data retention scheme, on which the Government is "expressly seeking the views of the Committee", is perhaps the most controversial and concerning of the proposals in the Discussion Paper. The scheme would be "tailored" and (presumably) require carriage service providers (CSPs) and internet service providers (ISPs) to retain data from users for use by intelligence agencies to predict crimes and terrorism offences.

36 As noted above, this proposal is characteristic of a police state. It is premised on the assumption that all citizens should be monitored. Not only does this completely remove the presumption of innocence which all persons are afforded, it goes against one of the essential dimensions of human rights and privacy law: freedom from surveillance and arbitrary intrusions into a person's life.

37 While the Government appears to have already withdrawn its support for the proposal,[9] it is necessary to examine the issues. It would appear that public support for this type of proposal is largely absent. As noted in the introduction to this submission, for there to be any extension of intrusive powers, such powers should be legitimate, necessary, proportionate and effective. I fail to see how the proposal achieves any of these. Collecting the data of all Australians does not appear proportionate to the risk of terrorism, nor is it likely to be effective in stopping terrorist acts (described below). Like any information system, would-be criminals and terrorists will either find a way around the technological limits (such as using a Virtual Private Network, encryption services, or an anonymity network such as Tor[10]), or move communications to other non-electronic channels.

---

[7] See the cases of *United States v Fricosu*, US District Ct (Colorado) (2012); cf *United States v Kirschner*, US District Ct (E. Michigan Sth Div) (2010).
[8] Apart from its existence in legislation, such as the *Evidence Act 1958* (Vic) ss 26, 29.
[9] See, for example, *The Age*, 'Roxon puts web surveillance plans on ice', 10 August 2012, http://www.theage.com.au/technology/technology-news/roxon-puts-web-surveillance-plans-on-ice-20120809-23x9l html.
[10] These would not necessarily be "workarounds" to a deep packet inspection scheme, but are merely provided as examples of current technologies that provide users with the ability to (in some way) mask their internet usage.

Lack of detail

38 The detail in the Paper is scarce. Accordingly, there are multiple unanswered questions:

a. Why has two years been chosen as the appropriate time period for data retention? Is this time period particularly significant for law enforcement? Two years appears arbitrary and without justification.

b. Will it involve actual collection of raw data or merely data relating to what Internet Protocol/web addresses a user connects to? If the former, how will the data be stored, given it is likely to be prohibitively expensive and arguably technically impossible for internet service providers to do? If it is the latter, which would be far less encompassing and of limited utility in comparison to raw data, how does this achieve the goal of stopping terrorist attacks? (For example, if only web access was recorded, and terrorists were conversing on Facebook – how would knowing a user had visited Facebook stop a terrorist attack?)

c. How will the data be secured? Retaining the data would create a massive security risk if an ISP suffers a breach of security, including a significant risk of identity theft. The immense amount of data would also create an incentive for hackers to view ISPs as a target.[11] Unlawful access of this data could cause extensive privacy concerns, given the data is likely to contain a wealth of personal information, including potential online financial transactions.

d. Who will have access to the data? The proposal clearly anticipates ASIO/law enforcement access; however, the ISPs that collect the data will also have access. How will employees of CSPs/ISPs be prevented from accessing what is likely to be an extremely valuable, if not tempting, data source?

e. Will there be a standard format in which the data is required to be kept? How will each CSP/ISP ensure that the data is consistent across all services so that it can be data-mined?

f. How will the information be 'linked' to a particular person? If multiple people use one computer, how will the system determine which user is which (clearly necessary to determine if a law has been breached)? How will agencies ensure accuracy?

39 These questions need to be both considered and answered before a genuine debate can be entered into.

[11] See, for instance, Anonymous's access of AAPT's servers to demonstrate the 'problems' with data retention schemes. See *The Next Web*, 'Anonymous hacks Australian ISP AAPT to demonstrate data retention problems', 26 July 2012, http://thenextweb.com/au/2012/07/26/anonymous-hacks-australian-isp-aapt-to-demonstrate-data-retention-problems /.

Data mining ineffective in identifying terrorist links

40 There must also be some consideration as to the *purpose* of such a proposal. Assistant Commissioner Neil Gaughan of the Australian Federal Police High Tech Crime Centre has stated publicly that, "If we don't have a data retention regime in place we will not be able to commence an investigation in the first place."[12] The intention is (presumably) for law enforcement to mine this data to identify terrorism links and, as a result, prevent terrorist attacks.

41 However, there has been research to suggest that data mining is not "well suited" to discovering terrorists.[13] Research suggests that it is not *more* information, but *useful* information, which assists in finding terrorist links. The National Research Council noted, as one of its conclusions to the report *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*:[14]

> The utility of pattern-based data mining is found primarily if not exclusively in its role in helping humans make better decisions about how to deploy scarce investigative resources, and action (such as arrest, search, denial of rights) should never be taken solely on the basis of a data mining result. Automated terrorist identification through data mining (or any other known methodology) is neither feasible as an objective nor desirable as a goal of technology development efforts.

42 If raw data of all Australians is stored, even with the world's most powerful supercomputers filtering the data and creating these links, the data will still need to be examined and investigated by a law enforcement officer, resulting in immense resource requirements. The data will not be of sufficient "quality" (a requirement under existing privacy laws)[15] given the amount of information, and the amount of false positives inevitably created by such a system may in fact divert resources from legitimate risks.

Potential for function creep, misuse and unlawful access

43 If such a data retention scheme was introduced, the data should *only* be used for the most serious of terrorism offences, and those offences defined in legislation. Otherwise, the potential for 'function creep' is too great. 'Function creep' refers to situations where information collected for one reason is used later for other purposes.[16] For example, the information may first be collected only for terrorism offences, but then other agencies or individuals are permitted to access it for limited reasons (one can envisage the data being

---

[12] See *The Age*, above n 9.
[13] Jeff Jonas and Jim Harper, 'Effective Counterterrorism and the Limited Role of Predictive Data Mining', *Policy Analysis* No. 584, December 11 2006, available at http://www.cato.org/pubs/pas/pa584.pdf.
[14] United States National Research Council, Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, 78, available at http://www nap.edu/catalog/12452.html.
[15] Organisations must take reasonable steps to make sure that personal information it collects, uses and discloses is accurate, complete and up to do date (*Information Privacy Act 2000* (Vic), Schedule 1, Information Privacy Principle 3).
[16] Office of the Victorian Privacy Commissioner, *Guidelines to the Information Privacy Principles*, Edition 3, November 2011, available at http://www.privacy.vic.gov.au.

used for other non-terrorism offences, civil proceedings, and so forth). I consider it inevitable that, even if safeguards are put in place, the temptation for others to seek access to that data would place great pressure on legislators to amend the scheme to allow other law enforcement agencies and organisations to access the data, and the safeguards upon which the scheme was predicated would be progressively stripped away.

44 There is no information as to how such data will be protected and safeguarded, whether misuse and unlawful access would result in an offence, or whether such powers are subject to a sunset clause. Again, the paucity of information does not allow appropriate examination.

45 Additionally, the extreme risk of a breach of this data (whether accidental or by unlawful access) and the consequential effects is too great. Without the introduction of mandatory data breach notification laws, this risk is exacerbated. One needs only look at breaches of mass datasets that have occurred in the private sector within the last year[17] to recognise that the additional risks created by of an ISP storing every transaction a user makes online is immense. In my view, a breach of some kind is inevitable given the interest in the data from hackers. If ISPs are not required to notify users that their information has been breached, this creates a further risk that users are unable to take steps to protect themselves from damage such as identity theft.

Chilling effects and flow-on economic problems

46 A data retention proposal could create an extreme chilling effect not only on technology but on social interactions, many of which are now conducted solely online. Users may move away from using online services due to the fear that their communications are being monitored. Investment in technology systems may decrease and innovation could be stifled. Depending on cost-sharing arrangements, smaller ISPs, for instance, may not be able to afford the data storage costs, and these costs may be passed on to consumers. I consider that the consequential economic impacts of a data retention scheme are wide-reaching. Simply put, the proposal could mean that individuals, due to concerns about surveillance, revert back to offline transactions. If this occurred, it would affect existing efficiencies of both businesses and government (such as online banking).

47 One is reminded of Professor Zelman Cowen, eminent lawyer and former Governor General of Australia:[18]

> Only those who can sustain an absolute commitment to the ideal of perfection can survive total surveillance, and I do not believe that they exist among ordinary men in ordinary society.

[17] For instance, recent investigations from the Office of the Australia Information Commissioner include Sony (http://www.oaic.gov.au/news/statements/statement_investigation_into_Sony_data_breach.html); Telstra http://www.oaic.gov.au/news/statements/statement_investigation_telstra_Dec_12.html); Vodafone (http://www.oaic.gov.au/news/media_releases/media_release_vodafone.html); AAPT (http://www.oaic.gov.au/news/statements/statement_120806_aapt_melb_it.html); and First State Super (http://www.oaic.gov.au/news/statements/statement_investigation_first_state_super.html).

[18] Professor Zelman Cowen, *The Private Man* – Boyer Lectures, 1969 (ABC Books).

> A man must therefore have some place, some area of "social space" into which he can withdraw in solitude and anonymity. Who among men can know what he thinks and feels if he never has the opportunity to be alone with his acts, thoughts and feelings? A crucial aspect of the autonomy of the individual, therefore, must be his claim to make his independent decision when to "go public". A man's privacy is his safety-valve. He has in it his permissible area of deviation, his opportunity to give vent to what he would not express or do publicly; within these limits he may share confidences and intimacies with those he trusts and he may set boundaries to those confidences.
>
> ...
>
> It is worthwhile stressing the point which emerges from this: the claim to privacy protects the individual's solitude, his intimacy and various groups of his own choosing, his anonymity, his ability to be lost, without identification in a crowd, his reserve, his shutting himself off from unwanted intrusion.
>
> To me, this claim to privacy is clear beyond doubt; I see it as one of the truly profound values of a civilised society. I believe that it is important that it should be so recognised: important because the contemporary political and social organisation, aided by a formidable technology, has forced us to become aware that the privacy which until now we took for granted and even casually presumed as an ingredient of moral action, simply can no longer be presumed but must be specified. What also must be specified are the threats, actual and impending, to that privacy, and the action to be taken to meet those threats.

48 This proposal would invade the privacy of every Australian citizen, erode democratic freedoms in Australia, and remove protections ensconced in human rights law, in the name of identifying and capturing a relatively small number of people.

Conclusion

49 Disproportionate responses to terrorism can do more damage than the terrorist acts themselves. Unfortunately, the Discussion Paper outlines multiple proposals which will have the cumulative effect of significantly eroding civil liberties and the privacy rights of Australians.

50 I strongly urge the Committee to re-consider these proposals.

DR ANTHONY BENDALL
Acting Victorian Privacy Commissioner