Submission No 140

Inquiry into potential reforms of National Security Legislation

Organisation: Human Rights Law Centre

Inquiry into Potential Reforms of Australia's National Security Legislation

Submission to the Joint Parliamentary Committee on Intelligence and Security

20 August 2012

www.hrlc.org.au

Freedom. Respect. Equality. Dignity. Action.

Contact

Ben Schokman
Human Rights Law Centre Ltd
Level 17, 461 Bourke Street
Melbourne VIC 3000

W: www.hrlc.org.au

About the Human Rights Law Centre

The Human Rights Law Centre is an independent, non-profit, non-government organisation which protects and promotes human rights.

We contribute to the protection of human dignity, the alleviation of disadvantage, and the attainment of equality through a strategic combination of research, advocacy, litigation and education.

The HRLC is a registered charity and has been endorsed by the Australian Taxation Office as a public benefit institution. All donations are tax deductible.

Follow us at http://twitter.com/rightsagenda
Join us at www.facebook.com/pages/HumanRightsLawResourceCentre

The HRLC would like to thank Richard Concha and Daniel Webb for their assistance with the preparation of this submission.

Contents

1. INTRODUCTION 1
   - 1.1 Background 1
   - 1.2 Scope of this submission 1
2. A HUMAN RIGHTS FRAMEWORK 1
   - 2.1 Community Protection and Human Rights: Complementary Goals 1
   - 2.2 Relevant Human Rights 2
   - 2.3 Permissible Limits on Human Rights: The "Proportionality Test" 2
   - 2.4 Right to Privacy 4
3. PROPOSED REFORMS 5
   - 3.1 Proposed Expansion of ASIO Warrant Powers 5
   - 3.2 Protection from Liability during the Course of Operations 6
   - 3.3 Coverage of 'Ancillary Service Providers' 7
   - 3.4 Data Retention 7
   - 3.5 Ministerial Authorisation Powers 7
   - 3.6 Expanding ASIO's Use of Force Powers 8
4. OTHER HUMAN RIGHTS CONCERNS 9
5. COMPARATIVE LESSONS 10
   - 5.1 United Kingdom: Compulsory Data Retention 10
   - 5.2 European Union Data Retention Directive 11

1. Introduction

1.1 Background

1. This is a submission by the Human Rights Law Centre (HRLC) to the Parliamentary Joint Committee on Intelligence and Security. The Parliamentary Joint Committee has been asked to examine a package of national security ideas comprising proposals for telecommunications interception reform, telecommunications sector security reform and Australian intelligence community legislation reform. The reform proposals relate to the *Telecommunications (Interception and Access) Act 1979* (TIA Act), the *Telecommunications Act 1997* (TA Act), the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Intelligence Services Act 2001* (IS Act).

2. The HRLC is concerned that many of the mooted reforms to national security legislation raise issues of compliance with Australia's international human rights obligations.

1.2 Scope of this submission

3. This submission:

   (a) provides an overview of Australia's international legal obligations and those human rights principles most relevant to the proposed reforms;

   (b) addresses a number of the specific proposals contained in the Government's Discussion Paper; and

   (c) briefly considers similar proposals in other jurisdictions, including the United Kingdom and the European Union.

4. The HRLC is concerned to ensure that any reforms to Australia's national security legislation are closely monitored by reference to international legal obligations and that any limitations on relevant human rights are consistent with the accepted international human rights law principles of proportionality, necessity and reasonableness.

2. A Human Rights Framework

2.1 Community Protection and Human Rights: Complementary Goals

5. The HRLC recognises that the Commonwealth Government has a duty to protect its citizens from national security threats. Australian law enforcement and intelligence agencies should be given sufficient powers to investigate, prevent and prosecute terrorist acts and those engaged in terrorist activities. Likewise, the objective of protecting human rights – such as the rights to life, liberty and security of person enshrined in the *International Covenant on Civil and Political*

Rights (ICCPR) – is consistent with the objective of protecting Australian communities. Both objectives are fundamentally concerned with protecting the community and individuals from harm.

6. There may be instances where human rights may need to be limited to some extent for the purpose of community protection. However, as explained further below, this should only take place if it is absolutely necessary and only to the extent that the limitation on rights is proportionate, evidence-based and rationally connected to the threat posed. A human rights approach explicitly takes the balancing of competing concerns into account.

2.2 Relevant Human Rights

7. Many of the proposed reforms to national security legislation raise concerns regarding a number of Australia's international law obligations to respect, protect and fulfil human rights, in particular the rights set out in the ICCPR. The following rights, among others, are relevant to the proposed reforms:

   (a) equality and non-discrimination (article 2(1) of the ICCPR);

   (b) access to appropriate remedies (article 2(3));

   (c) the right to life (article 6);

   (d) the right to liberty and security of person (article 9);

   (e) the right to privacy (article 17);

   (f) freedom of opinion and expression (article 19); and

   (g) the rights of minorities (article 27).

8. None of the rights set out above are absolute. Under the ICCPR, each of the rights can be limited, but only in particular circumstances and to the extent necessary. A proportionality analysis is used to determine whether a right can be limited and the extent to which a limitation is lawful.

2.3 Permissible Limits on Human Rights: The "Proportionality Test"

9. The proportionality test for limitation of ICCPR rights can be stated in general terms (although strictly speaking under the ICCPR each of these rights is limited by words contained within the articulation of the right itself).[1] Put broadly, general provisions setting out a proportionality

[1] As Bell J stated in *Kracke v Mental Health Review Board* [2009] VCAT 646, [105], the internal limitations provisions in ICCPR rights "call up a proportionality analysis in various ways".

analysis require that any limitation of rights be reasonable and demonstrably justified in a free and democratic society.[2] The proportionality test is a two stage process.

10. First, the purpose of the limitation on the right must be of sufficient importance to a free and democratic society to justify limiting the right.[3] This might also be described as requiring a "pressing and substantial" objective,[4] reflecting a need to balance the interests of society with those of individuals and groups. Examples of purposes for limitations that might accord with a free and democratic society include protection of public security, public order, public safety or public health.[5]

11. Secondly, the means used by the State to limit rights must be proportionate to the purpose of the limitation. The most widely accepted test of proportionality is derived from the Canadian case *R v Oakes.*[6] In that case the Supreme Court of Canada set out the three components of a proportionality test:

> There are three important components of a proportionality test. First, the measures adopted must be carefully designed to achieve the objective in question. They must not be arbitrary, unfair or based on irrational considerations. In short, they must be rationally connected to the objective. Second, the means, even if rationally connected to the objective in this first sense, should impair "as little as possible" the right or freedom in question ... Third, there must be a proportionality between the effects of the measures which are responsible for limiting the Charter right or freedom, and the objective which has been identified as of "sufficient importance.[7]

12. The onus of establishing that a limitation is reasonable and demonstrably justified rests on the party seeking to rely on the limitation, which will usually be the government.[8] The standard of proof is generally the balance of probabilities, although it may change in given circumstances, requiring "a degree of probability which is commensurate with the occasion".[9] That is, the more serious the infringement of rights, the more important the objective of the limitation of those rights must be to a free and democratic society, and the higher the standard of proof will

[2] Words to this effect are used in section 7 of the Victorian Charter of Human Rights and Responsibilities Act, section 1 of the Canadian Charter of Rights and Freedoms, section 5 of the New Zealand Bill of Rights Act and section 36 of the South African Constitution.

[3] *R v Oakes* [1986] 1 SCR 103, [69]-[71] (Dickson CJ).

[4] *The Supreme Court in Canada (Attorney-General) v Hislop* [2007] 1 SCR 429, [44]. See also R v Oakes [1986] 1 SCR 103, cited with approval in *Kracke v Mental Health Review Board* [2009] VCAT 646, [145] and in *R v Momcilovic* [2010] VSCA 50.

[5] The Hon Rob Hulls MP, Victoria, Parliamentary Debates, *Legislative Assembly*, 4 May 2006, 1291 (Rob Hulls).

[6] [1986] 1 SCR, [103].

[7] [1986] 1 SCR 103, [43].

[8] [1986] 1 SCR 103, [66]. *Kracke v Mental Health Review Board* [2009] VCAT 646, [108].

[9] See Warren CJ in Re an application under the Major Crime (Investigative Powers) Act 2004 [2009] VSC 381 (7 September 2009), [147] citing *Bater v Bater* [1950] 2 All ER 458, 459 (Lord Denning).

be for the State.[10] This approach has been approved in Victorian Court of Appeal decision of *R v Momcilovic*,[11] in which the Court endorsed the *R v Oakes* requirement for clear, cogent and persuasive evidence in order to demonstrably justify a human rights infringement.[12]

13. As discussed throughout this submission, many of the proposed reforms to national security legislation engage in particular the right to privacy. Accordingly, set out below are relevant standards and principles relating to the right to privacy. Considerations relating to other relevant human rights are set out in the discussion of each of the specific mooted reforms.

2.4 Right to Privacy

14. The right to privacy is enshrined in article 17 of the ICCPR:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks.

15. Interferences with the right to privacy may be lawful and permitted where legislation is precise and circumscribed.[13] States must ensure that decision makers do not possess overly wide discretion in authorizing interferences with the right to privacy.[14] In *Toonen v Australia*,[15] the UN Human Rights Committee commented that any non-arbitrary interference with privacy must be proportionate to the end sought, and must also be reasonable and necessary in the circumstances of any given case.

16. If the Government wishes to limit the right to privacy, it must state the overriding public interest in limiting the right and establish that the means used are reasonable, necessary and proportionate. Such considerations are all the more important when individuals have no right to seek judicial review of a warrant's validity or terms or be brought before any judicial body (other than a prescribed authority appointed by the Minister).

---

[10] See See Warren CJ in *Re an application under the Major Crime (Investigative Powers) Act 2004* [2009] VSC 381 (7 September 2009), [150].

[11] [2010] VSCA 50 (17 March 2010).

[12] *R v Momcilovic* [2010] VSCA 50 (17 March 2010), [143] (Maxwell P and Ashley and Neave JJA).

[13] *Duinhoff and Duif v Netherlands* (1984) 13 EHRR 478, [8]. See also the Committee's Concluding Observations on the Russian Federation where it expressed concerns in relation to existing mechanisms to intrude into private telephone communications. Legislation setting out the conditions of legitimate interferences with privacy and providing for safeguards against unlawful interferences lacked sufficient clarity.

[14] *Duinhoff and Duif v Netherlands* (1984) 13 EHRR 478, [8]. See also Sarah Joseph, Jenny Schultz and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary* (Second Edition, 2004), p 480-481.

[15] (488/92).

3. Proposed Reforms

3.1 Proposed Expansion of ASIO Warrant Powers

17. The Discussion Paper released by the Attorney-General's Department indicates that the Government wishes to progress proposals to:

    (a) simplify the renewal of the warrants process; and

    (b) extend the duration for warrants.

18. Those proposals the Government is considering whether to progress are:

    (a) to establish a single warrant with multiple telecommunications interception powers;

    (b) to establish a single warrant authorising multiple (existing) powers against a single target instead of requesting multiple warrants against a single target;

    (c) to establish classes of persons able to execute warrants instead of listing specific officers; and

    (d) to allow disruption of a target computer for the purposes of a computer access warrant.

19. Those proposals the Government is seeking views on are:

    (a) an incidental power in the search warrant provision to authorise access to third party premises to execute a warrant;

    (b) using third party computers and communications in transit to access a target computer under a computer access warrant;

    (c) reforming the Lawful Access Regime; and

    (d) expanding the basis of interception activities.

20. The HRLC is extremely concerned about the proposals to significantly broaden powers available to ASIO under warrants. In particular, no relevant evidence has been provided that such extended powers are required to protect public safety. The Government's stated rationale for the proposals, which is to "modernise and streamline ASIO's warrant provisions", is not directly related to the protection of public safety, but is rather administrative or operational in nature. Mere administrative convenience should not be used to justify serious violations of human rights.

21. Accordingly, the proposals to reform warrant provisions under the TIA Act and under the ASIO Act raise concerns with the right to privacy protected by article 17 of the ICCPR. As discussed above, if the Government wishes to limit the right to privacy, it must state the overriding public interest in limiting the right and establish that the means used in each instance are reasonable, necessary and proportionate.

22. In this instance, the Government has not provided a sufficient explanation as to why such extraordinary powers are necessary to justify the potential limitations on the right to privacy, and the HRLC recommends that the proposed reforms to warrant provisions be either demonstrably justified or rejected.

3.2 Protection from Liability during the Course of Operations

23. The Government is considering the creation of an authorised intelligence operations scheme that would provide protection for ASIO from criminal and civil liability for certain conduct in the course of authorised intelligence operations. The proposed authorised intelligence operations scheme aims to support covert intelligence operations by providing immunity to ASIO officers from criminal and civil liability for certain conduct performed in the course of authorised intelligence operations.

24. The HRLC welcomes the safeguards contained in the proposal, such as:

(a) oversight and inspection by the Inspector-General of Intelligence and Security (IGIS), including notifying the IGIS once an authorised intelligence operation has been approved by the Director-General;

(b) specifying conduct which cannot be authorised (such as intentionally inducing a person to commit a criminal offence that the person would not otherwise have intended to commit and conduct that is likely to cause the death of or serious injury to a person or involves the commission of a sexual offence against any person); and

(c) independent review of the operation, effectiveness and implications of any such scheme, which could be conducted five years after the scheme's commencement.

25. However, the proposal to provide legal protection from criminal and civil liability for certain conduct in the course of authorised operations raises significant human rights concerns, since such a scheme would potentially authorise acts that may infringe human rights. Furthermore, the scheme does not provide any additional avenues for individuals to lodge complaints about the conduct of an intelligence agency during the course of operations, which raises concerns with the right to an effective remedy.

26. The proposed authorised intelligence operations scheme would need to clearly enumerate what specific conduct may be authorised (and not merely what conduct is prohibited), under what circumstances conduct would be authorised, and also provide avenues for redress. Additionally, the role of the IGIS should be extended so that the IGIS is included in the process of authorising an intelligence operation under the scheme to ensure that potential abuses under the protection from liability are minimised.

3.3 Coverage of 'Ancillary Service Providers'

27. The Government is considering the extension of the regulatory regime to cover ancillary service providers not currently covered by the TIA Act, such as social networking and cloud storage websites. Such websites and online services contain a large amount of personal and private information, both stored and in-transit. Allowing access to such data raises serious concerns with the right to privacy, particularly given that the Government has not provided any relevant information or evidence to show that there is an overriding public interest in extending the regulatory regime to cover ancillary providers.

3.4 Data Retention

28. The Government is seeking views on a proposal to tailor data retention periods for up to two years for parts of a data set with specific timeframes taking into account agency priorities, and privacy and cost impacts. This proposal poses a particular concern to the right to privacy because of the vast quantity of private data that could be stored and accessed. The combination of data retention and the proposal to extend the regulatory regime to cover ancillary providers has the potential to severely limit the right to privacy. The proposal also creates the possibility for the potential misuse of stored data, both by the Government and non-government entities.

29. Considering the wide implications of such a data retention scheme, the Government has not provided any detailed information regarding the proposal, except to say that the rationale for the proposed scheme is to streamline and reduce complexity in the law. As discussed above, if the Government wishes to limit the right to privacy, it must state the overriding public interest in limiting the right and establish that the means used are reasonable, necessary and proportionate. In this instance, the Government has not provided any significant information to show that there is an overriding public interest in implementing a data-retention system.

3.5 Ministerial Authorisation Powers

30. The Government is seeking views on a proposal to enable the Minister of an agency established under the IS Act to authorise the production of intelligence on an Australian person or persons where the Agency is cooperating with ASIO. This proposal has wide reaching implications for intelligence activities and raises significant human rights concerns, especially in regard to the right to privacy.

31. The intelligence agencies established under the IS Act, such as the Australian Secret Intelligence Service (ASIS), the Defence Imagery and Geospatial Organisation (DIGO) and the Defence Signals Directorate (DSD), are mandated only to produce intelligence on persons or organisations *outside* of Australia. Section 9 of the IS Act provides an exception by allowing the Minister of an agency to provide authorisation under certain conditions, but only to the point where it is in fulfilment of an agency's function. ASIO, on the other hand, is not limited by

geography but by its function of "security intelligence" as defined in the ASIO Act. ASIO is therefore able to produce intelligence on Australian persons and organisations.

32. The proposal to amend the Ministerial Authorisation provision contained in Section 9 of the IS Act would result in the removal of the limitation that Australia's foreign intelligence agency act only in fulfilment of *its* functions. The proposal would provide a greater avenue for Australia's foreign intelligence agencies to collect information on Australian citizens and organisations by allowing them to cooperate with ASIO in the performance of an ASIO function. This would enable an agency to potentially act outside of its mandate under the IS Act.

33. The proposal to amend Section 9 of the IS Act raises a significant human rights concern in relation to privacy because it would give Australia's foreign intelligence agencies a broader avenue to produce intelligence on Australian persons without any corresponding oversight or accountability of such powers. The Government has not stated an overriding public interest in limiting the right to privacy and has not established that the proposal is reasonable, necessary and proportionate.

3.6 Expanding ASIO's Use of Force Powers

34. The Government is seeking views on proposals to:

(a) allow reasonable force to be used at any time during the execution of a warrant, not just on entry; and

(b) enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.

35. The Government's proposal to allow ASIO to use reasonable force at any time during the execution of a warrant, not just on entry, may raise concerns in relation to the right of liberty and security of person, which is enshrined in article 9 of the ICCPR. The HRLC is also concerned that the proposal to enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS, may pose risks to right to life contained in article 6 of the ICCPR. These proposals should have regard to human rights standards on the use of force.

36. A human rights-based approach to the use of force can be characterised as requiring the state to act in the three stages involved in the use of force:

(a) before the use of force – putting in place systems to protect human rights and avoid or minimise resort to force, such as proper policies and training;

(b) during the use of force – requiring that force be used in a proportionate way; and

(c) after the use of force – ensuring that there are accountability mechanisms in place to hold agents of the state to account for their use of force.

37. Human rights standards require that the law and policies governing the use of force protect life to the greatest extent possible. Lethal force must be strictly regulated and must only be used when absolutely necessary.[16] In short, a human rights-based approach requires:

(a) clear laws - state agents should be guided by clear and detailed laws on the use of lethal and non-lethal force which strictly regulates its use in accordance with the right to life and other human rights.

(b) training - state agents should be appropriately qualified, trained and monitored in order to safeguard life, including in a range of non-violent and non-lethal responses, such as communication and negotiation. Agents should be trained to protect life by assessing whether there is an absolute necessity to use firearms, not only on the basis of the relevant regulations, but also with due regard to the pre-eminence of respect for human life as a fundamental value.

(c) range of means - state agents should be equipped with a range of use of force options, including non-lethal or less than lethal weapons.

(d) non-discrimination - state agents should respect and protect the human rights of all people without discrimination. The circumstances in which force may be used by state agents, and the policies which guide such use of force, should include consideration of the special position and needs of minority and other groups (e.g. racial and religious groups, people experiencing mental illness and young people).

(e) monitoring and oversight – there must be effective and independent investigation following the use of force. True independence is only achieved when an investigation is hierarchically, institutionally and practically independent of the organisation being investigated.

4. Other Human Rights Concerns

38. The HRLC is also concerned about the disproportionate impact of the Government's national security proposals on particular groups within Australian society. The discussion paper mentions that the proposals are designed to meet the threat posed by terrorism.

39. Similar to past counter-terrorism provisions, the HRLC notes that while many of the current proposal are not discriminatory on their face, in practice the increase in powers and prosecutions under counter-terrorism laws has been felt adversely and disproportionately by Muslim, Kurdish, Tamil and Somali communities in Australia.

[16] *McCann v United Kingdom* (1996) 21 EHRR 97, [148] to [161]; *R (Middleton) v West Somerset Coroner* [2004] 2 AC 182, [2]; *LCB v United Kingdom* (1998) 27 EHRR 212, [36]; *Osman v United Kingdom* (1998) 29 EHRR 245 [115]; *Keenan v United Kingdom* (2001) 33 EHRR 913, [88]-[90]; *Edwards v United Kingdom* (20020) 35 EHRR 487, [54]; *R (Amin) v Secretary of State for the Home Department* [2004] 1 AC 653, [30], *Oneryildiz v Turkey* (2005) 41 EHRR 20, [89]; *Leonidis v Greece* [2009] ECHR 5, [55]-[56]; *Simsek v Turkey* [2005] ECHR 546, [104].

40. One concern is that intelligence gathering agencies use the existence of the laws to coerce co-operation with investigations from particular communities, without needing to resort to actually exercising powers under the laws. The indirect effect of the laws is therefore that intelligence officers reportedly use powers to leverage individuals into informal interviews.[17]

41. Community legal centre lawyers in Melbourne have reported that ASIO officers request an informal chat accompanied by an indication that they could obtain a questioning warrant.

42. Community lawyers in Melbourne have also reported that the Australian Federal Police and ASIO, when investigating instances of political violence, focus disproportionately on Australians with Tamil, Pakistani, Arab and East African ties through their families or countries of origin.[18]

5. Comparative Lessons

5.1 United Kingdom: Compulsory Data Retention

43. The United Kingdom (UK) Government recently released its draft *Communications Data Bill*.[19] The Bill proposes to expand the collection and storage of communications data, such as records of email, texts and phone calls, by communication service providers so that such data may be accessed by state agencies at some later date.[20]

44. Both the Australian and UK proposals require a greater number of communication service providers to store more data for longer. The justification proffered by both governments is that the intelligence collection powers of law enforcement and security agencies needs to evolve to meet developments in communication technology, lest criminal elements be given a "technological upper hand".[21]

45. The draft UK Bill has been met by strong criticism.[22] The HRLC notes that many of the concerns raised have application to the Australian Government's proposals.

46. By imposing onerous requirements on companies providing communication services, the draft UK Bill outsources security and surveillance functions to the private sector, inevitably at some financial cost to consumers. Further, the mass collection and storage of personal information

[17] See, eg, Independent National Security Legislation Monitor, Annual Report, 16 December 2011, p 12, available at http://www.dpmc.gov.au/inslm/docs/INSLM_Annual_Report_20111216.pdf.

[18] Western Suburbs Legal Service, *Is Community A Crime?* (2009), p 7.

[19] *The Queen's Speech 2012*, 2012, Cabinet Office, http://www.cabinetoffice.gov.uk/queens-speech-2012.

[20] *No Snoopers Charter*, Liberty, http://www.liberty-human-rights.org.uk/campaigns/no-snoopers-charter/no-snoopers-charter.php.

[21] *Discussion Paper*, p 3.

[22] *No Snoopers Charter*, above n 20.

carries the inherent risks that such information will be misused, fraudulently accessed or inadvertently lost or disclosed.[23]

47. Importantly, the National Council of Civil Liberties ('Liberty') in the UK has observed that the draft Bill represents a shift in the underlying approach to crime prevention and detection.[24] Instead of the targeted monitoring of future communications on the basis of individual suspicion, the draft Bill promotes the indiscriminate stockpiling of private data by private agencies for potential future use by the state. Everyone's communication data is kept, not just those suspected of a crime. Large repositories of private data tempt 'fishing expeditions' – trawling though private data in search of suspicion, not on the basis of it. A nation of citizens thus becomes a nation of suspects.[25]

48. In addition to analogous data retention measures, the HRLC also notes that the Australian Government's proposals include establishing the offence of failing to assist in the decryption of communications. Imposing an obligation on suspects to provide this level of assistance to investigators runs counter to the right to remain silent. Derogation from such a fundamental tenet of due criminal process serves to further underscore the relevance to the Australian context of Liberty's concerns of an underlying shift in the approach to crime investigation.

5.2 European Union Data Retention Directive

49. The European Union Date Retention Directive, adopted in 2006, requires all internet service providers and telecommunication service providers operating in Europe to collect personal communications data and retain it for periods between six months and two years.[26]

50. The Directive has been heavily criticised and the necessity and proportionality, and therefore the legality, of such vast data retention requirements has been questioned. Human rights and privacy organisations have criticised the European Commission's impact assessment of the Directive as failing to examine the necessity of each different category of service provider retaining each different category of personal data.[27] Such groups have also called on more active consideration to be given to less restrictive alternatives, such as targeted (rather than indiscriminate) data retention.[28]

---

[23] See http://www.liberty-human-rights.org.uk/pdfs/policy09/liberty-s-communications-data-consultation-response.pdf, p 19.

[24] Ibid.

[25] *No Snoopers Charter*, above n 20.

[26] For a discussion on the directive, see Electronic Frontier Foundation, https://www.eff.org/issues/mandatory-data-retention/eu.

[27] Andreas Krisch, European Digital Rights, available at http://www.edri.org/files/dr_letter_260911.pdf.

[28] Ibid.

51. Concerns have also been raised that the impact assessment fails to establish that blanket data retention has a demonstrable, statistically significant impact on the prevalence or investigation of serious crime.[29] Further, there has been no analysis of whether any benefits flowing from blanket data retention are sufficient to justify the adverse consequences, such as:

    (a) the risks of data loss and abuse;

    (b) the risks of mistakes in data retrieval;

    (c) damage to peoples' confidence in, and willingness to, communicate freely; and

    (d) the inherent invasion of privacy.[30]

52. Several countries have legislated to implement the Directive domestically. However, such legislation has been struck down by the High Courts and Constitutional Courts of several countries, including Cyprus, Bulgaria, Lithuania and the Czech Republic.[31]

53. In a class action brought by 35,000 people, the German Federal Constitutional Court suspended the operation of German data retention laws on the basis that the data storage was not secure and it was unclear what the data would be used for. The President of the court, Hans-Jürgen Papier, commented that mass data retention can:

> cause a diffusely threatening feeling of being under observation that can diminish an unprejudiced perception of one's basic rights in many areas.[32]

54. The HRLC notes that many of the concerns raised in the European Union context, particularly those relating to the absence of any detailed necessity and proportionality assessment, apply equally to the Australian Government's data retention proposals. Such risky and invasive measures will only be lawful if necessary and proportionate to the ends they achieve.

[29] Ibid.

[30] See http://www.edri.org/files/dr_letter_260911.pdf.

[31] See https://www.eff.org/issues/mandatory-data-retention/eu.

[32] See http://www.spiegel.de/international/germany/defending-privacy-german-high-court-limits-phone-and-e-mail-data-storage-a-681251.html.