Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

10 February 2015

Mr David Kaye
Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression and Opinion
Office of the United Nations High Commissioner for Human Rights

Dear Mr Kaye,

Re: THE USE OF ENCRYPTION AND ANONYMITY IN DIGITAL COMMUNICATIONS

The Australian Privacy Foundation (APF) is Australia's leading privacy advocacy organisation. A brief backgrounder is attached.

This submission by the Australian Privacy Foundation responds to the Call for Submissions of Information regarding national legal frameworks governing the relationship between freedom of expression and the use of encryption to secure transactions and communications, and other technologies to transact and communicate anonymously online.

This submission will present the APF's assessment of laws and policies in Australia which concern the use of encryption and the ability to communicate anonymously. We will firstly present an overview of the protection of free expression and privacy in Australia, since both encryption and anonymity techniques may be considered to be expressions of individuals utilising their freedom of expression and/or protecting their privacy. As will be seen below in more detail, compared to other developed democratic jurisdictions, Australia has a much weaker protection of free expression and no constitutional protection of privacy.

Then, we present and discuss specific Australian legislation with a direct effect on encryption and anonymity, namely:

- *Privacy Act 1988* (Cth),
- *Cybercrime Act 2001* (Cth) and
- *Defence Trade Controls Act 2012* (Cth).

We also present other developments, in particular Australia's participation in the 'Five Eyes' intelligence-sharing partnership and the current proposals to introduce mandatory data retention laws in Australia. These developments provide evidence of the lack of human rights protection, particularly of privacy, in Australia and also contribute to the deterioration of individuals' ability to remain anonymous online.

Finally we give APF's assessment of the current situation in Australia for encryption and anonymity.

1. The protection of free expression and privacy in Australia

Since encryption and anonymity, as mentioned above, may be conceptualised as means of securing individuals' free expression and protecting their privacy, in this section we present an overview of the protection of these rights in Australia.

Firstly, Australia is unique among developed liberal democracies in not possessing a constitutional or statutory charter of rights at the national level. While the Australian Constitution provides express protection for certain specific rights such as the right to vote and freedom of religion, there is no comprehensive set of human rights guarantees.

During the 1990s, Australia's High Court implied a right to free speech into the Constitution.[1] Yet this implied right is very limited in its application i.e. to 'political' communication about government or political matters, based the system of representative and responsible government established by the Australian Constitution – and so does not constitute a general right to free speech or expression as constituted in other jurisdictions. The jurisprudence has also conceived of this implied freedom as not conferring personal rights on individuals, and as being more of a freedom *from* laws which perturb political communications rather than a freedom *to* communicate – a shield against excesses of legislative and executive power rather than a sword to assert an individual right.

Australia has no constitutional right to privacy, whether express or implied. The Australian High Court in *Lenah Game Meats* left open the possibility of the judiciary introducing a tort of invasion of privacy given the right circumstances, but did not do so based on the facts at hand on which it was found that there had been no invasion of privacy.[2] Privacy protection in Australia is currently based on a patchwork of different statutes protecting different aspects of privacy rather than an overarching enforceable principle. The most prominent among these statutes is the *Privacy Act 1988* (Cth) which provides some protection of data privacy and its application to anonymity and encryption will be discussed in the next section. However, the *Privacy Act* is limited in various respects, not in the least the fact that individuals cannot bring actions before the courts of their own accord, and instead must make a complaint to the Australian Information Commissioner. While a tort action for serious invasions of privacy has been proposed by the Australian Law Reform Commission which *inter alia* would allow individuals to initiate actions in the courts themselves,[3] at the time of writing it has not been implemented into Australian law.

Some stronger protection than the Constitution's implied right to free expression and lack of privacy protection exists at the State level in certain jurisdictions. Both Victoria and the Australian Capital Territory have enacted statutory charters of rights based on the UK and New Zealand models.[4] Both of these charters, which serve as binding on the state-level public bodies in those two jurisdictions, contain rights to free expression and privacy.

At the international level, Australia is a signatory to the International Covenant on Civil and Political Rights 1966 (ICCPR) which it ratified in 1980. While these provide Australian with international obligations as a signatory state, the rights contained in the ICCPR are not directly enforceable in Australian domestic law.

Australia's lack of strong human rights protection, especially of free expression and privacy, may be seen as detrimental to anonymity and the use of encryption. For instance, anonymity guarantees in the USA have been interpreted as stemming from the protection of free expression in the First

---

[1] Starting in *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106 and *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1. Affirmed unanimously by the High Court *in Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520

[2] *ABC v Lenah Game Meats Pty Ltd* (2001) 185 ALR 1.

[3] Australian Law Reform Commission Report 123, *Serious Invasions of Privacy in the Digital Era* (3 September 2014) <http://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123> accessed 6 February 2015

[4] Respectively: *Human Rights Act (ACT)* 2005; *Charter of Human Rights and Responsibilities Act (Vic)* 2006.

Amendment to the American Constitution.[5] Given a lack of strong free expression guarantees in Australia, it would seem less likely that the protection of anonymity could be established in a similar way to the US. The European Court of Human Rights has also provided some practical protection of anonymity through its interpretation of Article 8 of the European Convention on Human Rights,[6] again a situation that would seem difficult to replicate in the Australian context.

2. Anonymity and encryption in Australian law

In this section, we discuss specific laws and policies in Australia which concern encryption and anonymity.

2.1 Australian Privacy Principles

As mentioned above, the *Privacy Act* regulates the handling of personal information about individuals which includes the collection, use, storage and disclosure of the information, as well as access to and correction of the information. The *Privacy Act* contains the Australian Privacy Principles (APPs) which govern how this personal information is handled by Australian federal government agencies and private sector organisations with an annual turnover of at least AU$3 million. Essentially, entities which are bound by the APPs must adhere to the obligations contained therein.

Of relevance to this submission on encryption and anonymity in Australia is APP 2 on anonymity and pseudonymity:

> 2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.
>
> 2.2 Subclause 2.1 does not apply if, in relation to that matter:
>
> a. the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or
> b. it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

The *Privacy Act* was updated in 2014 to introduce these APPs, which replaced the Information Privacy Principles (IPPs – which applied to federal government agencies) and the National Privacy Principles (NPPs – which applied to private sector organisations). The predecessor to APP 2 was NPP 8:

> Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

At the time that these reforms to Australian privacy law were being considered, the APF welcomed the expansion of the anonymity principle to include pseudonymity but criticised what we saw as the undermining of anonymity in the proposed APP since it gave entities the option of only offering pseudonymity as a substitute for anonymity, with no obligation to offer anonymity where legal and practicable as NPP 8 previously provided.[7]

---

[5] *McIntyre v Ohio Elections Commission,* 514 U.S. 334 (1995); *Watchtower Bible & Tract Society of New York v Village of Stratton* 536 U.S. 150 (2002)

[6] *Peck v UK* (2003) 36 EHRR 41; [2003] EMLR 287

[7] Nigel Waters and Graham Greenleaf, 'A Critique of Australia's Proposed Privacy Amendment (Enhancing Privacy Protection) Bill 2012' (2012) UNSW Law Research Paper No. 2012-35, <http://ssrn.com/abstract=2134838> accessed 7 February 2015, at p. 13

We also welcomed the application of the anonymity principle via APP 2 to Australian federal government agencies but criticised the exceptions in 2.2 (since 'every government department must surely be so *authorised* by implication of one law or another?'), and instead suggested that exceptions to the anonymity principle only be provided where identification is expressly required by law or impracticable.[8]

Since our concerns were not addressed in the final text of APP 2, the APF does not find this guarantee of anonymity vis-à-vis data privacy particularly strong given the possibilities for APP entities, especially public bodies, to find themselves authorised to deal with individuals who have identified themselves, and the wide interpretation that may be given to situations in which it is 'impracticable' for APP entities to deal with anonymous or pseudonymous individuals.

2.2 Cybercrime legislation

The main law in Australia which addresses 'cybercrime' is the *Cybercrime Act 2001* (Cth). The provisions of this legislation are based on the Council of Europe Convention on Cyber-Crime, although Australia only signed and ratified this Convention more than ten years later in 2013 (and passed the *Cybercrime Legislation Amendment Act 2011* (Cth) in order to accede to this treaty).

While the encryption of files is not prohibited by this Act or other legislation in Australia,[9] the *Cybercrime Act* does include, in its modification of the *Crimes Act 1914* (Cth) through the insertion of section 3LA, a provision which permits law enforcement agencies to apply to a magistrate for an order requiring a specified individual to disclose encryption keys, passwords and any other details necessary to obtain evidence which is stored in a protected or encrypted fashion. A person who does not comply with such an order to decrypt can face penalties including 6 months' imprisonment. Prior to this, an individual could refuse to provide encryption keys if doing so would be self-incriminating. Similar provisions in the form of section 201A were introduced into the *Customs Act 1901* (Cth), compelling assistance with enforcement officers at points of entry into Australia.

The APF (at the time named the Australian Privacy Charter Council) criticised these extended powers to compel disclosure and cooperation at the time the *Cybercrime Bill* was being considered by the Australian Houses of Parliament in 2001, for the reasons that adequate evidence had not been provided to demonstrate that these extended powers to force cooperation were necessary, and the potential to misuse these powers to manipulate computer data.[10]

Australian digital rights organisation Electronic frontiers Australia (EFA - with which APF often works closely) was also highly critical of the *Cybercrime Bill*[11]. EFA pointed to the legitimate reasons why an encryption key should not be provided to a law enforcement agency, and the 'major and quite legitimate concern' of users of encryption being jailed despite having genuinely lost their keys. The lack of distinction that the legislation makes between 'the inability to provide assistance and an unwillingness to provide assistance' was also criticised by Chan *et al*.[12] EFA also pointed to the

---

[8] *ibid*

[9] Although the exportation of encryption technology from Australia is regulated by the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* as a dual-use technology, adopted into Australian law via the *Customs Act 1901* and the *Customs (Prohibited Exports) Regulations*. See: Nickolas John James, 'Handing Over the Keys: Contingency, Power and Resistance in the Context of Section 3LA of the Australian Crimes Act 1914' (2004) 23 *The University of Queensland Law Journal* 7, at p. 10

[10] Australian Privacy Charter Council, *Submission to the Senate Legal & Constitutional Committee on the Cybercrime Bill 2011 (*July 2011) <https://www.privacy.org.au/Papers/SenCybercrime0107.html> accessed 7 February 2015

[11] Electronic Frontiers Australia, *Commentary on the Cybercrime Bill 2001* (23 July 2001) <https://www.efa.org.au/Publish/cybercrime_bill.html> accessed 7 February 2015

[12] Nelson Chan, Simon Coronel and Yik Chiat Ong, 'The Threat of the Cybercrime Act 2001 to Australian IT Professionals', *Proceedings of the First Australian Undergraduate Students' Computing Conference 2003*, at p. 28

1997 OECD cryptography guidelines, which Australia also adopted, which recognise the fundamental right of privacy in relation to encrypted data.

APF still considers that these powers to force cooperation in decrypting data have not been justified as necessary, and also shares concerns that the provisions are too broadly-worded to include individuals who are unable rather than unwilling to assist law enforcement.

2.3 Cryptography research

At the time of writing, the coming into force of certain provisions of the *Defence Trade Controls Act 2012* (Cth) (DTCA) in May 2015 has sparked debate regarding, among other concerns, the lack of safeguards contained in the legislation for academic research into cryptography in Australia. A public consultation closed on 30 January 2015.

DTCA is Australian legislation intended to control the export, transfer and brokering of defence and strategic goods and technologies which are listed on the Defence and Strategic Goods List, maintained by the Minister of Defence. The Act creates criminal offences for the 'intangible' transfer or supply and publication of goods and technologies contained in this list, and this includes supply via email, scan and fax and publication including academic journal articles, conference papers and blogposts. These criminal offences apply to the supply and publication of research into 'dual use' technologies. Given the absence of an exclusion for academia, university researchers may require prior permission from an official at the Department of Defence to communicate new research to foreign nationals or publish in academic journals, etc if this research relates to an item listed on the Defence and Strategic Goods List.

Cryptography would appear to be a dual use technology that might be subject to DTCA's restrictions, along with other computing research.[13] APF is concerned that these overly broad provisions and lack of exclusions for e.g. academic researchers as well as civic open access initiatives may unduly impede research into encryption techniques in Australia and the public communication of such research.

2.4 Other developments

Although not explicitly related to anonymity and encryption, the APF has been highly concerned with recent developments relating to Australia's participation in the Five Eyes intelligence sharing partnership (along with the US, UK, New Zealand and Canada) and the proposals for mandatory data retention currently under consideration by the Australian Houses of Parliament.[14] We see Australia's lack of effective human rights protection providing a check on executive and parliamentary power as being manifested in these developments which are highly intrusive of Australians' privacy yet which cannot be challenged in Australian courts.[15]

As regards the topic of this submission, we are particularly concerned that if mandatory data retention laws are passed in Australia, then in practice this could entail less *de facto* protection for anonymity - in particular if anonymity requires the de-identification of data as this could conflict with data retention requirements.[16]

---

[13] See: Richard Chirgwin, 'Australia tries to ban crypto research – by ACCIDENT' (*The Register*, 14 January 2015) <http://www.theregister.co.uk/2015/01/14/australia_tries_to_ban_crypto_research_by_accident/> accessed 8 February 2015

[14] See: Australian Privacy Foundation, *Submission to Parliamentary Joint Committee on Intelligence and Security on Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (19 January 2015) <https://www.privacy.org.au/Papers/PJCIS-DataRetention-150119.pdf> accessed 8 February 2015

[15] See: Australian Privacy Foundation, *Human Rights as a Break on Tyranny* (public statement, 4 February 2015) <https://www.privacy.org.au/Media/MR-HumanRts-150204.pdf> accessed 8 February 2015

[16] Graham Greenleaf, 'Transactional anonymity in privacy principles – Australia and elsewhere' (OII AnonEvent, London, 8 December 2011)

The introduction of mandatory data retention laws has been the topic of debate for some years now in Australia.[17] In 2013, in the context of such discussions on the reform of national security laws, the Australian Attorney-General's Department publicly admitted that it wanted powers that would enable it to break the encryption used in services such as Tor in order to gather data on individuals using such services to evade data retention laws.[18]

APF is highly concerned about the extended powers that mandatory data retention may give Australian law enforcement agencies to interfere with encryption, and the general deterioration of the legal landscape for individuals who wish to remain anonymous that these laws will entail.

3. Conclusion

APF considers that the current protection for free expression and privacy in Australia, and accordingly encryption and anonymity, is inadequate. APF would welcome stronger protections of the right to communicate anonymously for individuals either as individual measures or as part of a broader reform of Australian law to honour and give domestic effect to ICCPR obligations in the form of a bill of rights. Such a reform might include rights to anonymity and to use encryption either as subsets of the rights to free expression and privacy or as conceptually separate, standalone rights.

APF is particularly concerned about the effect that mandatory data retention laws could have in practice on Australians' attempts to remain anonymous while using the Internet. In particular, an obligation on service providers to retain information identifying particular users would seem to conflict with, and override, APP 2's (already weak) guarantee of anonymity. APF is highly concerned about the attack on privacy and security that the Australian government's previously-expressed wishes to break encryption on services such as Tor would entail.

APF is also concerned about the current overly broad provisions in the *Cybercrime Act* compelling data decryption and the adverse effect of the *Defence Trade Controls Act* on cryptography research in Australia.

Representatives of the APF would be pleased to discuss this submission with you and address particular aspects in more detail.

Thank you for your consideration.

Yours sincerely

Angela Daly
Board Member
+61 392144420 Angela.Daly@privacy.org.au

[17] See: Angela Daly and Sean Rintel, 'Europe says no to data retention, so why is it still an option in Australia?' (*The Conversation*, 14 April 2014) <https://theconversation.com/europe-says-no-to-data-retention-so-why-is-it-an-option-in-australia-25444> accessed 8 February 2015

[18] Bernard Keane, 'Revealed: Australian spies seek power to break into Tor' (*Crikey*, 30 May 2013) <http://www.crikey.com.au/2013/05/30/revealed-australian-spies-seek-power-to-break-into-tor/> accessed 8 February 2015

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies in Australia. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, SubCommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby AC CMG and The Hon Elizabeth Evatt AC, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90) http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-) http://www.privacy.org.au/Campaigns/Media/