



Submission No 220

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

Supplementary Submission to the
Joint Parliamentary Committee on
Intelligence and Security

on the

*Inquiry into potential reforms of the
National Security Legislation*

10 October 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 I thank the Committee for the opportunity to make a supplementary submission to the Inquiry.
- 2 As I stated in my previous submission to the Committee, I do not support a data retention scheme, which I consider goes against the basic tenets of privacy law: that information is collected only where it is necessary,¹ and is destroyed or de-identified when it is no longer needed for any purpose.²
- 3 I recognise that the Committee has before it a difficult balancing act between the right of individuals to privacy and the right not to be placed under arbitrary surveillance, against the protection of national security and the remote (but possible) risk of a terrorist act. Where the line of this balancing act lies is imprecise. There is great difficulty in comparing the right of individuals not to be monitored or tracked against the potential effects of a terrorist attack (or similar). Australia does not have a constitutional right to privacy, unlike in European Union countries such as Germany, Romania and the Czech Republic, where similar data retention schemes based on the European Data Retention Directive 2006/24/EC have been ruled unconstitutional.³
- 4 As such, it is fundamental that the right to privacy (particularly the right not to be surveilled) is given sufficient value so that the dichotomy between privacy and the other interest (in this case, the protection of individuals from terrorist attacks) is comparable. Otherwise, where any countervailing interest exists, privacy rights will always fall away in the face of that other interest.

Metadata

- 5 Many of the submissions to the Committee assumed (and, in my view, were entitled to based on the lack of detail) that a data retention scheme would mean the collection of all data and traffic by an individual across a telecommunication network. My submission was also based on this assumption.
- 6 However, in its submission to the Committee ASIO stated that “agencies are not seeking access to the content of communications”,⁴ but rather are seeking ‘metadata’. The Attorney-General has also clarified that the scheme is intended to capture

¹ For example, *Privacy Act 1988* (Cth), National Privacy Principle 1.1; *Information Privacy Act 2000* (Vic), Information Privacy Principle 1.1.

² For example, *Privacy Act 1988* (Cth), National Privacy Principle 4.2; *Information Privacy Act 2000* (Vic), Information Privacy Principle 4.2.

³ See for instance the German Federal Constitutional Court 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.

⁴ Submission by ASIO to Parliamentary Joint Committee on Intelligence and Security, Potential reforms of national security legislation, available at www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs/sub%202009.pdf.

“telecommunications data”.⁵ The Attorney-General defined “telecommunications data” as “information about a process of communication as distinct from its content.”⁶ The Attorney-General noted that:

The Government does not propose that a data retention scheme would apply to the content of communications. ... Access to the content of communication is only ever carried out under warrants issued in accordance with the *Telecommunications (Interception and Access) Act 1979*. There is no intention to alter the requirement for warranted access to the contents of communication.⁷

- 7 Metadata/telecommunications data might include collecting information about web sites a user visits, which Internet Protocol (IP) addresses the user accesses, the location of the access, and the time, date and duration of such access. The proposal now appears to be similar to the European Union Data Retention Directive 2006/24/EC.⁸
- 8 With respect, clarifying that the data is collected is merely “telecommunications data” and suggesting that it is significantly less invasive is disingenuous. Collecting metadata is still privacy intrusive. Even if “only” IP addresses are collected, it could effectively show a profile of an individual that could be, in some cases, akin to collecting the content of communications. For example, some website addresses may have logins and passwords in the URL. Content may also be determined where information is collected about to whom the person is speaking and the context of that communication.
- 9 I also query the effectiveness of collecting metadata in order to achieve the objectives of the scheme. In countries where data retention has been introduced (such as Germany), there has not been evidence of an increase in the prevention of crime.⁹ It is very difficult to see how collecting IP addresses and other related data could prevent a terrorist act.
- 10 The Committee received evidence from Australian law enforcement agencies that preferred an indefinite rather than two-year retention period. I consider the two-year period excessive, and that the suggestion of a desire for indefinite retention by a law enforcement agency is evidence that, should this scheme be introduced, ‘function creep’ will be inevitable.

Safeguards

- 11 However, should Parliament decide otherwise and legislate such a scheme, it is important that the most stringent oversight and safeguards are placed upon it. The

⁵ Letter from the Hon Nicola Roxon MP, Attorney-General, to Anthony Byrne MP, Chair, Parliamentary Joint Committee on Intelligence and Security, 19 September 2012, available at: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/additional/letter%20from%20ag%20to%20pjcis%20clarifying%20tor.pdf.

⁶ Ibid.

⁷ Ibid.

⁸ Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>.

⁹ See Arbeitskreis Vorratdatenspeicherung, Data Retention Effectiveness Report, 26 January 2011 (updated 19 February 2011, available at http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf).

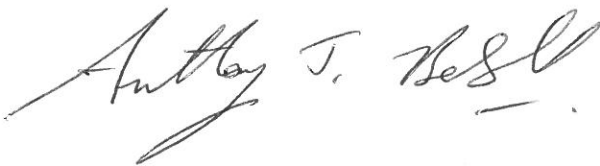
Committee invited me to address what I would consider minimum “safeguards” for data retention. Such “safeguards” might include:

- access only occurring on judicial oversight and requiring a warrant, with a prima facie case being established for access (that is, a restriction on data mining);
- access only permitted for prescribed law enforcement agencies and only for the most serious of terrorism offences;
- strict data security requirements that are audited on a regular basis;
- a requirement that law enforcement agencies be required to regularly and publicly report statistics on issues such as the amount and level of access and interceptions; the number of warrants granted and refused; the number of investigations undertaken; statistics regarding the efficacy of the scheme (such as the number of false positives and false negatives); and number of arrests or prosecutions resulting from such access or interception;
- the ability for a special investigations monitor to monitor compliance of law enforcement agencies with the specific data retention regime;
- serious offences for unlawful access and misuse by individuals;
- a mandatory requirement for agencies, carriers/carriage service providers (C/CSPs) and internet service providers (ISPs) (or any other organisation that stores data collected from the scheme) to notify appropriate bodies and/or individuals should any of the information be accessed without authorisation;
- fines or similar punitive measures for C/CSPs and ISPs for failure to secure data; and
- a requirement for the government to reassess the scheme after a period of time/sunset clause.

12 For the sake of transparency, these safeguards must be legislated and not left to administrative regulation. They should be enforced strictly and with appropriate oversight.

13 As I noted to the Committee, the lack of detail in the Discussion Paper has made only a broad brush response to the proposal possible.

14 Again, I urge the Committee to carefully re-consider the proposals in the Discussion Paper, particularly the nature and operation of any proposed data retention scheme.



DR ANTHONY BENDALL
Acting Victorian Privacy Commissioner

