Submission No 241

Inquiry into potential reforms of National Security Legislation

Name: K Selvarajah

Organisation: Private capacity

Submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS)

Supplementary Submission

Kidnapillai Selvarajah (Selva)

Introduction

This Supplementary submission clarifies and expands on some of the issues that I have discussed in my original submission No: 236 in response to the Inquiry into Potential Reforms of National Security Legislation undertaken by the Parliamentary Joint Committee on Intelligence and Security (PJCIS).

Most importantly, it incorporates the email response that I have received from the European Commission Cabinet Member responsible for Data Retention, on various concerns discussed relating to the EU Data Retention Directive: 2006/24/EC in my original submission.

Violation of Basic Human Rights

We need greater transparency and proportionality around any communications surveillance legislations in order to safeguard our basic human rights enshrined in various international conventions that are ratified by Australia. The implementation of the AG's mandatory data retention proposal would violate:

- **Article 12 of The Universal Declaration of Human Rights** (*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks)*
- **Article 17 of the International Covenant on Civil and Political Rights** (*No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*)

I wonder why the Australian Human Rights Commission has not pointed out the above short comings to the members of PJCIS.

The main concern with the AG's data retention proposal is that it affects all Australians in whom government or law enforcement agencies such as ASIO and AFP have no prior interest. In other words, it would include those not suspected or convicted of any crimes.

If we go ahead of implementing the proposed mandatory data retention, Australia would become the first country in the world violating the basic norm of the presumption of innocence.

Alternatives to Mandatory Data Retention

There is no evidence whatsoever that the increased communications surveillance has had any beneficial effect. A study of German police statistical data published by the Arbeitskreis Vorratsdatenspeicherung on 26 January 2011, finds that telecommunication data retention as required by EU Directive: 2006/24/EC is ineffective in the prosecution of serious crimes. Please refer to the following URL for more information, if required

http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf)

Being a person worked in the Telecom Industry over 20 years, the beneficial usage of communications data retained under any retention scheme does not mean that data would otherwise have been lacking, considering the required commercial billing data stored and also extra data stored complying with any judicial orders. I strongly believe even in the relatively rare cases where extra data is disclosed under retention schemes, it often has no influence on the outcome of the investigation.

Data Preservation is a viable alternative to data retention and also proportionate measure assisting government law enforcement agencies while minimizing the violation of human rights. Under the data preservation regime, law enforcement agencies can demand that telecommunications service providers **begin storing, or rather preserving** data relevant to a **specified** investigation. Typically, the telecommunication service providers are required to continue preserving these data up to a maximum period of time, such as 90 days, while government law enforcement agencies obtain the necessary authority to compel disclosure. Furthermore, under the data preservation, only data about the tiny fraction of individuals who might fall under criminal suspicion is stored. Both the USA and Japan have data preservation schemes implemented but not data retention laws.

There are many forms of data preservation schemes such as Expedited Data Preservation and Targeted Collection of Traffic Data and they are good alternatives. The targeted data preservation is the internationally recognized standard procedure in investigating cybercrimes, having been agreed upon in the Council of Europe's 2001 EU Convention on Cybercrime. This convention, which also provides for an international exchange of communications data, has been signed by EU Member States as well as, by Norway, Canada, Japan, and the USA. Australia is expected to sign this convention on the 1st March,2013.

I strongly believe proposed mandatory data retention takes disproportionate measures to fight crimes in Australia. Any increased communication surveillance mechanisms like data retention does intrude upon the privacy of innocents fostering surveillance society. By implementing mandatory data retention scheme, Australia would become the pioneer of introducing the **FIRST WORLD SURVEILLANCE SOCIETY**.

Current Status on the EU Directive 2006/24/EC

The below is the email response I have received from on behalf of Soren Schonberg, a member of the European Commission Cabinet relating to the current status on the EU data retention directive 2006/24/EC.

From:
To:
CC:
Subject: RE: Data Retention->EU Directive 2006/24/EC
Date: Wed, 19 Dec 2012 16:40:03 +0000

Dear Selva

Soren Schonberg has asked me to thank you for your email, which has been passed to me to reply. I've answered your questions below in the order you presented them. I hope this is helpful

Christian

Christian D'Cunha

Unit A3 Police cooperation and access to information

DG Home Affairs

European Commission

http://ec.europa.eu/home-affairs/policies/police/police_data_en.htm

1. *How many EU countries have already transposed the EU directive?*

Twenty-five countries have notified the Commission of transposition of the Data Retention Directive (Directive 2006/24/EC).

2. *Have these countries modified the EU directive to comply with the domestic law requirements before transposing it?*

Romania and Czech Republic each recently adopted legislation, which is due to enter into force on 21 December 2012 (in Romania) and on 1 January 2013 (in Czech Republic). The Commission is currently examining the legislation to verify whether it fully transposes the Directive. The other (23) Member States have each transposed the Directive in different ways; for more detail, you may like to refer to the evaluation report published by the Commission in April 2011 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF)

3. *How many EU countries yet to transpose the directive?*

One Member State has not transposed (Germany) and another (Belgium) has only partially transposed.

4. *Is EU planning to replace/modify the current directive?*

The Commission intends to present a proposal for amending the data retention framework in due course, though there is no precise timetable at present. This has been announced most recently in Commissioner Malmström's response to the oral questions in the European Parliament in October 2012 http://www.europarl.europa.eu/ep-live/en/plenary/video?debate=1351018911944).

5. *If so, will you able to share at least any latest information as why the current the EU directive needs to be replaced/modified?*

The areas which need improvement are explained clearly in the evaluation report: a lower and more harmonised retention period, clarity on the types of data which are inside and outside scope, a clearer purpose limitation, stronger data protection and data security safeguards, a consistent approach to cost reimbursement and a proper mechanism for monitoring and evaluation.

Furthermore, any revision of the Directive must ensure that retained data are used exclusively for the purposes foreseen in this Directive, and not for other purposes as currently allowed by another EU law (Directive 2002/58/EC, known as the 'e-Privacy Directive') . The Commission therefore aims to propose a revision of the Data Retention Directive, to be presented at the same time as a future revision of the E-Privacy Directive. Any proposal reforming the E-Privacy Directive will take into account the result of the negotiations on the reform of the EU data protection regime, which is under the responsibility of the Commissioner for Justice, Fundamental Rights and Citizenship.

6. *Has UK transposed the EU directive, if not, any specific reasons for that?*

Yes. See the Data Retention (EC Directive) Regulations 2009 (2009 No. 859) (http://www.legislation.gov.uk/ukdsi/2009/9780111473894/contents).

Conclusion:

Privacy is a basic human right, and it is the main ingredient of any democratic society. It is a sin quo non to human dignity and self-respect. It reinforces other basic human rights, such as freedom of expression and association, and is recognised under various international laws and conventions. Activities that infringe on the right to privacy, including the surveillance of personal communications data by public authorities, can only be justified **where they are necessary for a legitimate aim, strictly proportionate, and prescribed by legislations.**

I strongly believe members of the PJCIS do not have any fancy of ignoring the Principle of the Presumption of Innocence, the Key Principle of Law. Personally, I wish Australia would NOT become the pioneer of introducing the **FIRST WORLD SURVEILLANCE SOCIETY** due to ignorance of Government Policy Making Mechanism.

I wonder whilst Australia strongly promoting and supporting an OPEN and INCLUSIVE Internet Governance mechanism around the world and at the same time trying to deny its own citizens the ***RIGHT of INFORMATIONAL SELF-DETERMINATION***. I hope we are NOT going back again to the year, 1788, the year of first European settlement in our beautiful OZland.