Submission No 236

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)

EQUIPPING AUSTRALIA AGAINST EMERGING AND EVOLVING THREATS

Kidnapillai Selvarajah (Selva)

Introduction

During the last three decades, I have personally witnessed unprecedented revolution in communications technology. This technological revolution has brought far reaching changes to our daily life. It has introduced new challenges to protect individual privacy and many opportunities to curb privacy violations. However, many studies seem to indicate that we, as human beings, feel an increased sense of intrusion and loss of privacy due to this rapid technological revolution.

Throughout history, whenever there have been national emergencies, the rights and civil liberties of the public have been curtailed, and in many instances revoked completely. Having said that, I would like to point out here that we have been witnessing an uneasy tension between privacy advocates and law enforcement agencies since 9/11 disaster. Civil libertarians say the USA Patriot Act was enacted in haste following the 9/11 tragedy in New York. We should not enact laws that narrow the scope of various fundamental rights such as individual privacy. However, drafting laws satisfying both the privacy advocates and law enforcement agencies is a delicate balancing act.

With this background, I have reviewed the consultation document "Equipping Australia against Emerging and Evolving Threats" and the proposed reforms, with particular reference to the Data Retention Proposal for a period of 2 years.

Paradox of Privacy versus National Security

Advances in communications technology, including the internet access, have dramatically changed the way we collect and use our personal information. Our personal data can be transferred universally and more rapidly now than ever before. This has influenced the way we perceive about our individual privacy and the protection of our personal records. The expectations relating to individual privacy have exponentially increased. It is the duties of any responsible government to seriously look into this aspect of enhanced expectations of safeguarding individual privacy.

We understand that law enforcement agencies such as ASIO and AFP are pushing for insidious laws that force Telecom Operators and Internet Service Providers to continuously collect and store data, documenting the communications and online activities of millions of ordinary Australian customers to deal with various crimes. These laws need to be paired with provisions that allow our law enforcement agencies to obtain these stored personal data for investigation purposes.

By expanding the ability of such law enforcement agencies to monitor various forms of communications activities including online internet access would harm individual privacy, anonymity, and free expression. According to Article 17 of the United Nation's International Covenant on Civil and Political Rights, everyone has the right to privacy and protection of the privacy by law. It would become a hindrance for us to use the various technologies to

undertake our legitimate tasks on a daily basis. Before I detail my personal views about the proposed reforms, I would like to pose a few thoughts to the members of the Parliamentary Joint Committee on Intelligence and Security:

- Can the imperatives of Individual Privacy and National Security be reconciled?
- Have we made tangible progress in the balancing act of individual privacy and national security since 9/11 debacle?
- Will it be possible to enhance national security by regulating online information flows?
- Are we ready to override our civil liberties in favour of national security?
- Will the proposed reform supposed to protect our democratic values end up eroding the civil liberties that are part of any democratic society?

Many of our measures (such as internet filtering) intended to protect our community could end up tarnishing the image of our beautiful nation. It is common to view the problem as one of striking the appropriate trade-off between the concerns of privacy advocates and the needs of the law enforcement agencies. Let us discuss as how we could strike a balance, if it is possible.

The Proposed Reform Package:

The proposal in the discussion paper appears to be vague and does not contain enough information for vibrant discussion by the stakeholders. First of all, I wonder what the rationale behind this reform is. The proposed reform seems to me not putting up a strong case for mandatory data retention by communications service providers. Did we carry out any substantial ex-post analysis of the existing legislations? I have been informed that the Telecommunications (Interception and Access) Act 1979 has been amended more than 60 times since the enactment of this piece of legislation. Further, it does not spell out the details of deficiencies in the existing legislations?.

Overall, it does not clearly stipulate a specific data retention model. I have read from various media, both print and electronic, that the Attorney General (AG) Hon Nicola Roxon MP has given assurance that the data retention proposals would only cover Metadata. Being a person directly involved in many capacities in the communications technology revolution, it is very difficult for me to infer from the discussion paper what is referred to as Metadata. I wish to state here that the AG's letter to the Chair of the Committee has given examples of Metadata taken from the EU directive. It is vital we should define the types of data sets that need to be collected and retained for a healthy discussion.

As I have stated in my introductory remarks, we clearly witness an uneasy tension between the individual privacy and the law enforcement agencies due to the current nature in communications technology but the proposal has failed to clearly articulate as how it would play the balancing act between individual privacy and national security. Any potential reform needs to be considered diligently with the required level of checks and balances that will minimize the impact on the rights of individual privacy.

I have a curiosity question to ask the members of the Committee, whether law enforcement agencies such as ASIO and AFP really know what they really want from the mandatory data retention. It is to be noted here that German Parliamentary research unit surveyed EU crime data between 2005-2010 and they could not find any evidence to suggest data retention was helping to resolve crimes Are we really trying to discover a pareto-optimising(in a Pareto efficient economic allocation, no one can be made better off without making at least one individual worse off) solution to the tension between the individual privacy and national security? Because of criminals in our society use communications technology to carry out their illegal activities, are we going pass this to all Australians irrespective whether they guilty or not? Do we need to tax all Australians a perceived "fear psycho" in their minds that they are monitored by law enforcement agencies and their private records could be misused?

In summary, the current proposal of mandated data retention for a period 2 years storing metadata will be invasive, intrusive, costly, and damage the right to individual privacy and free expression. It would compel telecom entities to create large databases of information about who communicates with whom via telephone line or smart phone or Internet, the duration of the call, and the location of the users. The proposed regime would also require that our IP addresses be collected and retained for every time we make online activity.

We should recognize that privacy risks increase as these databases become vulnerable to theft and accidental/purposeful disclosure. The telecom service providers, whether they are small or big, must absorb the costs of storing and maintaining these large databases for a period of 2 years and often pass these costs on to consumers. Further, it might lead to closure of many small internet service providers due to this additional cost of mandatory data retention scheme.

EU Directive 2006/24/EC:

According to the consultation document, AG does not have a specific data retention model to propose to the Committee to seek views from the public. However, the AG has cited EU Directive 2006/24/EC in her letter to the Chair of the Committee. The EU Data Retention Directive, adopted by the European Union in March2006 and came into force in May 2006, is the most prominent example of a mandatory data retention framework. It stipulates basic requirements on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. According to the directive, EU member states will have to store customers' telecommunications data for a period of 6 to 24 months. A permission to access the information will be granted only by a court.

The EU Directive compels all telecom and internet service providers storing data relating to a subscriber's incoming and outgoing telephone numbers, IP addresses, location details, and other key telephone and Internet traffic data. It is applicable to all European Community citizens, including those not suspected or convicted of any crime. With a data retention regime in place, sensitive information about social contacts (including business contacts),

movements and the private lives (e.g. contacts with physicians, lawyers, workers councils, psychologists, help lines, etc.) of 500 million Europeans is collected in the absence of any suspicion. It undermines professional confidentiality, creating the permanent risk of data losses and data abuses and deters citizens from making confidential communications via electronic communication networks. It undermines the protection of journalistic sources and thus compromises the freedom of the press. Overall it damages the preconditions of our open, vibrant and democratic society.

Effectiveness of EU Directive 2006/24/EC

Following patchy adoption of the EU directive and the recent publication of a report critical of its effectiveness, the European Data Protection Supervisor (EDPS) has weighed in on the Data Retention Directive. The EDPS has concluded that that the current law does not meet the requirements of fundamental rights to privacy and data protection and called for its revision or replacement. Though the directive has proven useful in criminal investigations, it needed revision and improvements in response to the fact that not every EU member state has adopted it and, in cases where they have, retention requirements vary wildly. Further, an internal review by the EU has highlighted a number of shortcomings with the directive.

The EU Data Retention Directive, which builds on and complements the general EU Data Protection Directive (95/46/EC), mandates that member states should ensure the confidentiality of communications and related traffic data. But the Privacy Directive requires that traffic and location data generated by using electronic communications services must be erased or anonymised when no longer needed for communication or billing purposes. The EDPS also questioned the law's compatibility with privacy rights. "Data retention as regulated in the Data Retention Directive, in any event, goes beyond what is necessary," continued the EDPS opinion, adding: "Data retention could have been regulated in a less privacy-intrusive way."

Obstacles Faced by EU Directive

The EU Directive has met many obstacles in the process of implementing it across EU member states. It remains highly controversial and has been rejected as unconstitutional in several EU member states. It has been challenged at the European Court of Justice by Digital Rights Ireland on human rights grounds, and the case is due to be heard very soon.

Sweden refused to implement the EU Data Retention Directive for a long period, finally adopting it on 21 March 2011 and came into effect on 1 May 2012. It has been reported in the press that the German Federal Constitution Court has ruled that the German law introduced to implement the directive is not in accordance with privacy rights that are guaranteed by the German Constitution, but the court said that the law can be amended to become constitutionally acceptable. The courts said that there were not enough safeguards to prevent misuse of citizen's personal data, and that the German Data Protection Commissioner should have oversight of the operation. I wish to remind gently to the Members of the Committee that it was a class action suit brought to the court by 35 thousand German citizens, and it was successful. The law as it was passed in 2008 must be amended before it can be put into force again.

UK Voluntary Code of Practice

The United Kingdom operates a voluntary system of data retention of communications traffic data. Although the Code is a voluntary in nature, there was a considerable pressure on the telecom industry to introduce a scheme. The system of voluntary data retention derives from Part 11 of the Anti-Terrorism, Crime and Security Act 2001.

The Anti-Terrorism, Crime & Security Act was passed in December of 2001 (the Act) Part 11 of the Act aims to allow for the retention of communications data to ensure that the UK security, intelligence and law enforcement agencies have sufficient information available to them to assist them in protecting the UK's national security and to investigate terrorism.

Communications data are retained by the communications service providers to enable them to carry out their business effectively. Such information could be divided into three broad categories, these being subscriber information (identifies the user); traffic data (identifies whom was called etc.); and the use made of service (identifies what services are used). The Act recognises that communications data are an essential tool for the security, intelligence and law enforcement agencies in carrying out their work to safeguard United Kingdom's national security. These agencies, which are authorised to acquire communications data under statutory provisions, would be greatly assisted if they could rely on the communications data being available when they required it.

Part 11 of the Act provides only for the retention of data that communication service providers already retain for business purposes**.** Its object is not to enlarge the fields of data which a communication service provider may (or must) retain, but to encourage communication service providers to retain that data for longer than they would otherwise need to do so for their own commercial purposes. The Act identifies that the purpose of the retention period is the safeguarding of national security or for the prevention or detection of crime or the prosecution of offences which relate directly or indirectly to national security.

This Code of Practice relates specifically to the need for communications service providers to retain data for extended periods of time in order to assist the security, intelligence and law enforcement agencies in carrying out their work of safeguarding national security or in the prevention or detection of crime or the prosecution of offences which relate directly or indirectly to national security. This Code of Practice does not address issues relating to disclosure of data; it simply addresses the issues of what types of data can be retained and for how long it will be retained beyond a particular company's existing business practice.

The Data Protection Act 1998 requires that personal data are processed lawfully. In retaining communications data for longer than needed for their own business purposes and for the purposes identified in the Act communication service providers will process personal data. The Information Commissioner's Office (ICO) has accepted that such processing will not, on human rights grounds, contravene this requirement of the Act.

However, individual communication service providers must satisfy themselves that the processing is "necessary" for one of a range of functions. In doing so they are entitled to rely

heavily on the Secretary of State's assurance that the retention of communications data for the periods as specified in this Code is necessary for the government's function of safeguarding national security, and on the fact that the Code has been approved by Parliament. The ICO has though expressed concern about such retained data being acquired for purposes that do not relate to national security.

Data Retention in the United States

The United States does not have any ISPs data retention laws similar to the EU Directive. There have been many attempts to introduce a form of mandatory data retention scheme and all have failed miserably due to vigorous protest from privacy advocates. I have extracted the information below from the ITU ICT Regulation Toolkit for the information of the Members of the Committee.

The Title 18 of the United States Code, Section 2703(f) states that: "A provider of wire or electronic communications services or a remote computing service, upon the request of a government entity, shall take all necessary steps to preserve records in its possession pending the issuance of a court order or other process." The policy of the U.S. Government is based on the belief that investigators and prosecutors need the ability to have service providers preserve (without disclosing) for a limited period of time, any data which already exists within their network architecture and which relates to a specific investigation.

The law requires preservation for 90 days, renewable for another 90 day period. After such period, access to these historical records can be obtained pursuant to a court order or in conformity with other due process protections. For example, the US Privacy Act requires, with some exceptions, that disclosure of any personal information be allowed only pursuant to a written request or prior written consent of the individual to whom the information belongs. The requirement for data preservation does not, however, require a service provider to collect data prospectively, nor does it permit the preservation of everything in a service provider's system – but only the information that related to a specific investigation. The United States also does not require ISPs to routinely destroy or retain communications data. ISPs are free to destroy or retain communications data as they each choose, based upon their own assessments, resources, needs and limitations.

There has been another attempt to introduce a different form of mandatory date retention scheme in the name of Internet Stopping Adults Facilitating the Exploitation of Today's Youth (SAFETY) Act of 2009 also known as H.R. 1076 and S.436 would require providers of "electronic communication or remote computing services" to "retain for a period of at least two years all records or other information pertaining to the identity of a user of a temporarily assigned network address the service assigns to that user. This bill has never become a law in the USA.

Conclusion

Personally I am not a favourite kid for any mandatory data retention scheme. Honestly, I have been puzzled observing the renewed interest and passion shown by Hon Nicola Roxon MP in developing and adopting an Australian version of EU Directive 2006/24/EC that has failed miserably including violating the constitutional provisions of certain EU countries as I

have detailed in my submission above. It is clear that there are many problems with the EU Data Retention Directive. I would like to recall what the European Data Protection Supervisor has called it "***the most privacy invasive instrument ever adopted by the EU,***"

In Summary:

- I do not see a strong case for a mandatory data retention scheme as the consultation document has failed to articulate the rationale and the need for it;
- There would be **enormous costs to the telecom Industry** if we proceed with the mandatory data retention scheme while many small time service providers could not afford to bear the additional cost burden and could be expected to go bankrupt;
- We would create a **"Fear Psyche"** among all Australians giving a perception "You Are Being Watched Continuously" and we should remember that the greatest element in a strong people is a fierce independence of spirit" and we Australians would lose this independence when we have a **"Fear Psyche"** in our minds all the time;
- Mandatory Data retention scheme is an invasion of our individual privacy and a **disproportionate response to the needs of law enforcement agencies**;
- There could be a real possibility that Mandatory Data Retention scheme might be abused by any law enforcement agencies.

Though it is not possible to reconcile the concerns of privacy advocates and needs of the law enforcement agencies, certainly we could look at the possibility of developing a Voluntary Scheme based on a "Code of Practice" developed by legally constituted "Data Retention Forum" alleviating the concerns of privacy advocates whilst trying to satisfy the needs of the law enforcement agencies. It is vital that the cost of adopting such a Code of Practice shall be shared by the Government and Industry; preferably the Code should be Voluntary in nature for a period of 2 years and then review the implementation for in-depth analysis.

If I get a chance to discuss my submission with the Members of the Parliamentary Joint Committee on Intelligence and Security in person, I would certainly consider travelling to Canberra for such a discussion. Further, on the same occasion I wish I could get a chance to question Hon Nicola Roxon MP on the rationale and motives for her proposed reform packages to guide the Members of the Committee to make an informed decision.

Acknowledgements:

I wish to express my sincere thanks to the Members of the Joint Parliamentary Committee on Intelligence and Security providing me an opportunity to make an individual submission to the Inquiry into the potential reforms of National Security Legislation. This submission is purely based on my professional knowledge on the subject for which I have acquired a passion and deep interest, industry experience in many capacities including leading telecom industry working committees in developing Australian National Standards and the interests in telecommunications/wireless, media and internet technologies.

The views expressed here are my own and not necessarily those of my employers both past and present or any organization with which I am affiliated.

References

1. The Code of Practice for Voluntary Retention of Communications Data http://security.homeoffice.gov.uk/news-publications/publication-search/general/5b1.pdf
2. European Union (EU) Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks - http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf
3. Explanatory Memorandum to the Data Retention(EC Directive) Regulations 2009: http://www.legislation.gov.uk/uksi/2009/859/pdfs/uksiem_20090859_en.pdf