inspiring success

AUSTRALIAN COMPUTER SOCIETY

Parliamentary Joint Committee on Intelligence and Security

(PJCIS)

Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

Response by the

Australian Computer Society Inc

19 January 2015

TABLE OF CONTENTS

1. INTRODUCTION

The Australian Computer Society (ACS) welcomes this opportunity to provide input to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, ("the Bill") introduced into the House of Representatives on 30 October 2014.

On 21 November, the Attorney-General, Senator The Hon George Brandis, asked the Committee to inquire into, and report on the Bill, which follows the National Security Legislation Amendment Bill (No.1) and Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014 as the Government's third tranche of legislation in response to alleged national security threats.

The proposal to introduce a mandatory data retention scheme was explored in depth in the Committee's 2013 Report of the Inquiry into Potential Reforms of Australia's National Security Legislation. This Report recommended several changes to the original retention scheme, which have been accepted and incorporated into the present Bill.[1]

Since the introduction of the revised Data Retention Bill into the House in October, the Parliamentary Joint Committee on Human Rights (PJCHR) and the Senate Standing Committee for Scrutiny of Bills have both released comprehensive reviews of its provisions in accordance with those Committees' standing terms of reference.

Since 2011, the PJCHR has been reviewing all legislation for its impact on rights and freedoms contained in the seven international covenants to which Australia is signatory. It is important to note that the International Covenant with which the Committee is most concerned (Civil and Political Rights) *allows the right to privacy to be limited* by laws that are "not arbitrary", which seek to achieve a legitimate objective and are '*reasonable, necessary and proportionate'* to that objective.

The Senate Scrutiny of Bills Committee reviews all Bills that are either before the Senate or are yet to be introduced, and considers whether such Bills:

- may trespass unduly on personal rights and liberties;
- make rights, liberties or obligations unduly dependent upon insufficiently defined administrative powers;
- make rights, liberties or obligations unduly dependent upon non-reviewable decisions;
- inappropriately delegate legislative powers; or insufficiently subject the exercise of legislative power to parliamentary scrutiny.

In preparing this submission, the ACS has had regard for, and given due consideration to, the views and findings outlined in each of those Committee reviews.

1 http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm

2. WHO IS ACS?

The ACS was formed in 1966 and is Australia's peak body for ICT professionals with around 22,000 members nationally. A core function of the ACS is the assessment and accreditation of its members as Certified Technologists or Certified Professionals. Assessments are conducted against an internationally accepted framework called Skills Framework for the Information Age (SFIA). To retain professional status ACS requires certified members to undertake ongoing professional development activities.

ACS also conducts research-based advocacy on behalf of members on public policy issues relating to the digital economy and the impact of ICT on productivity growth and standards of living in the Australian economy. As a vendor neutral organisation with no direct commercial interests in particular technology products or services, the ACS is able to provide a genuinely balanced view with a focus on good public policy outcomes.

ACS is a member of a number of international ICT bodies including the International Federation for Information Processing (IFIP) which represents IT Societies from 56 countries or regions, covering all 5 continents with a total membership of over half a million. [2]

For more information about the ACS, please see www.acs.org.au.

3. ACS POSITION ON THE DATA RETENTION BILL

ACS strongly supports initiatives by the Government to assist Australia's law enforcement and security agencies to more effectively address serious criminal behaviour and other activities that threaten Australia's national security. Furthermore, the ACS recognises that in the 35 years since the original Telecommunications (Interception and Access) Act 1979 ("TIA") was enacted, communications technology has advanced significantly. The internet is global and is now a core platform in our daily lives, there is a plethora of new and highly sophisticated communication devices in the market, there are a multitude of communications mediums and platforms, and in general the population has high digital literacy. In combination, these factors undoubtedly make the job of our law enforcement and security agencies much more difficult and complex than at the time of the original TIA. As such, the ACS believes it appropriate that the TIA be updated so that it remains an effective tool for our law security agencies to operate effectively.

However, the Bill does raise two broad areas of concern for the ACS.

First, whilst not an issue within the drafting of the Bill itself, the implementation of such a Bill requires particular care when choosing a workforce suitable for the delivery of key components of the scheme.

2 http://www.ifip.org/index.php?option=com_content&task=view&id=160&Itemid=480

Secondly, in terms of the Bill itself, there are certain elements which we are concerned may have some unintended consequences in relation to preserving appropriate privacy rights.

3.1 Obligations on ICT Professionals

At an operational level, a mandatory data retention scheme will require telecommunications companies and Internet Service Providers (ISPs) to build systems which will capture and store the required metadata and then allow access to and retrieval of that data as and when required. The recipient law enforcement and security organisations will also be required to build and operate similar ICT based systems.

A consequence of granting a range of authorities permission to collect, manage and view private data is an increased risk of data security breaches. Furthermore breaches of professional and ethical standards could potentially undermine public confidence in and support for the scheme which, by its very nature, creates heightened concerns about some potential loss of privacy. Responsibility for delivery and maintenance of these systems will be with the ICT community of professionals. Given the sensitivity of the data, the risk that the scheme potentially represents to the right to privacy, and the consequences if the captured data becomes available to inappropriate people or organisations, it is critical that the ICT professionals involved work with the highest standard of professionalism and ethics. This is an important and generally overlooked issue in the current debate. This is understandable to some extent since Parliament does not and cannot legislate to modify behaviour. However it is an important operational issue which will need to be addressed as part of the broader task of ensuring the legislation delivers the outcomes intended.

What then should be done to help minimise the risk of unprofessional behaviour?

In other long established professions such as medicine, law, engineering and accounting, achieving appropriate levels of professionalism and ethics is generally pursued via some combination of:

1. The professional body assessing and accrediting members, including a requirement that they must comply with a code of ethics. The latter is generally enforced and overseen by a Professional Ethics Board.
2. Governments legislating that certain professional minimum requirements must be met - including those relating to ethical behaviour - before a person can legally work in a particular field of professional practice. The rationale is that the consequences of those minimum standards not being achieved are potentially so significant that a legislated approach is required to help reduce risk.

ICT professionals however, in part because ICT is relatively young compared to disciplines such as law, medicine and engineering, are not yet recognised as a highly-skilled workforce that applies standards and ethics as part of their profession. Professional bodies such as the ACS exist in many countries, and most have well-established assessment, accreditation and professional development procedures which are built on a Code of Ethics. Until recent years, the community, and Governments in particular, have not understood or acknowledged that there are areas of ICT practice and/or ICT deployment that require “professional” characteristics similar to law, medicine and other skilled professions. A senior ICT practitioner has a specialist knowledge and skill so far in excess of the client that the client must have absolute trust that the practitioner will operate in a competent and ethical manner. This asymmetry of knowledge between the

practitioner and the client essentially defines a profession. So there are risks in ICT environments where incompetent and/or unethical behaviour can have very serious financial or personal consequences. Breaches of personal privacy information have the potential for serious consequences and should be considered part of this category.

The ACS is, however, now starting to see a change in how ICT is viewed particularly in those mission-critical areas of ICT practice. Globally there is an emerging discussion about areas of ICT practice or deployment needing to be regarded as a "profession" subject to similar types of accreditation and licensing arrangements as apply to other long-established professions. The rationale is well summed up by IFIP, the global body for the ICT profession, which notes that:

"The most important reason to examine and build ICT professionalism stems from the extent to which the increasing pervasiveness of ICT has the potential to harm our economy and society. The extent to which ICT is embedded in our lives is inevitably growing. If we fail to take steps to mature the ICT profession, it is likely that the risks to society from ICT will grow to unacceptable levels."[3]

The ACS' view, therefore, is that Governments (as well as private sector organisations) should start giving more serious consideration to whether these is case for mandating certain minimum standards of professionalism and perhaps even licencing requirements for people working on ICT systems in high-risk, mission-critical areas. The mandatory data retention arrangements being proposed by this Bill highlight one possible area – the handling of, and accessing to, personal information by third parties (other areas could include ICT systems in critical functions within fields such as defence, transport, medicine and security).

For its part, the ACS is taking action on a number of fronts to strengthen the awareness of and emphasis on professionalism and ethics within its own membership. In particular:

- We have an existing Code of Professional Conduct, administered by a Professional Standards Board, which must be adhered to by accredited ACS members.
- We are currently developing an online ethics course, which we are considering making a mandatory element of both the initial assessment/accreditation process as well as the annual professional development requirements for accredited members.
- The ACS President is Chair of the International Professional Practice Partnership, a sub-committee of IFIP, which is leading international efforts to define minimum standards of professionalism and to establish the supporting infrastructure.

However, where it is deemed important to achieve this outcome across all those working within the ICT profession, Government support and assistance would be needed. At one level it could involve Government, as an employer, requiring that those people working on ICT systems in mission critical areas being firstly independently assessed and accredited by the professional society. The next level up would be Government legislating that licensing arrangements are in place for

3 http://ipthree.org

anyone wanting to work on systems deemed as mission critical. The licensing process would require assessment, accreditation and ongoing professional development via an independent body and/or professional society.

3.2 Privacy Concern within the Legislation

As noted in earlier comments, the ACS strongly supports the draft Bill to the extent that it seeks to assist Australia's law enforcement and security agencies tackle serious criminal behaviour and other activities that threaten Australia's national security.

However, whilst ACS' area of expertise is certainly not privacy law, we do have some concerns that the legislation, as currently drafted, could have some intended consequences for important privacy principles.

Drawing particularly on the considerations of this draft Bill by the Parliamentary Joint Committee on Human Rights (PJCHR)[4], the ACS has concerns about the following elements:

3.2.1 Data Collected - Regulation or Legislation

The Bill does not contain a clear outline of the specific types of data that are to be covered by the retention scheme. Those data types are to be specified by a regulation made under paragraph 187A(1)(a) of the substantive Bill. In addition, paragraph 187A(3)(b)(iii) enables the regulations to prescribe services *beyond those specified* in subsection 187A(3), to which retention obligations will apply. Those specified are essentially carrier and internet services. This means, in effect, there will be a regulation-making power that can be used to expand the operation of the scheme.

The ACS understands that the argument for defining the detail of the data types in regulation rather than legislation is that it allows for more flexibility and agility. This can be particularly important in the fast-moving communications technology space. However, defining the detail of the data sets in the legislation provides more certainty and transparency for both the communication providers who must build the systems to capture the data, as well as individuals and the public generally whose personal data might be captured. The ACS believes the latter issues are of greater significance and therefore supports the PJCHR view that the Bill be amended to define the types of data that are to be retained, or alternatively, the Government release for consultation, a draft exposé of the regulation specifying the types of data to be retained for the purposes of the scheme.

3.2.2 Content is Undefined

The Bill specifically excludes 'content' from the scheme but 'content' is undefined. The ACS is concerned that in their efforts to comply with the scheme, telecommunications providers may unwittingly include elements of content in the data retained. An example used by the PJCHR is the use of meta-tags by website developers to allow search engines to rank

4 http://www.aph.gov.au/~/media/Committees/Senate/committee/humanrights_ctte/reports/2014/15_44/Chapter%201.pdf

sites. Such tags may contain details about a site's content or aspects of its content. The ACS therefore suggests that the Bill provide an exclusive definition of 'content'.

3.2.3 Access to Information

The TIA Act permits an 'authorised officer' of an 'enforcement agency' to authorise a service provider to disclose existing telecommunications data where it is 'reasonably necessary' for the enforcement of, 'a law imposing a pecuniary penalty or the protection of the public revenue'. ACS believes the concept of 'reasonably necessary' as it is assumed under the Bill is too imprecise. As presently drafted, it can be argued that the Bill may allow access to data where it is reasonably necessary for a minor offence. There needs to be a clearer and proportionate link made between the data to be collected and the seriousness of the crime. Otherwise there could be unnecessary and unjustified intrusion into the individual's right to privacy. A possible precedent provided by the PJCHR is the threshold of 'major indictable offence', currently required to trigger the option of trial by jury. The ACS therefore supports the PJCHR suggestion that the Bill be amended to limit disclosure of data to "instances where it is 'necessary' for the investigation of specified serious crimes, or categories of serious crimes."

3.2.4 Potential Use for Unrelated Purposes

ACS is concerned that the Bill creates a potential for retained data to be accessed and then used by parties other than the original requesting agency, under sharing arrangements between government agencies. There is also no limitation on how the accessed data can be used; while it may be disclosed for an authorised purpose, it may then be used for an unauthorised purpose or by an unauthorised person or agency.

ACS recommends the Bill be amended to restrict access to retained data where it is necessary for specific investigations of serious criminal activity, and used only by the requesting agency.

3.2.5 Agency Access

The Bill would allow metadata to be accessed by 'enforcement agencies'. The Bill defines these as including the Australian Federal Police, State Police forces, and other investigative bodies such as the Australian Crime Commission and Independent Commission Against Corruption. However the Bill also allows for "*any other authority or body declared by the Minister to be an enforcement agency*." Under this provision, the Attorney-General must consider a range of factors, including whether the agency enforces the criminal law, imposes pecuniary penalties or protects the public revenue. As these are not limiting factors, it is possible that a range of bodies beyond those outlined in the Bill could be declared as "enforcement agencies". In addition those bodies will only become clear after the relevant declarations are made. ACS' view is that it is not appropriate that a key element of the proposed data retention regime, such as who can access the metadata is, to some degree, open-ended and lacks transparency. ACS suggest means be explored to tighten the Bill up in this area, be that by defining 'enforcement agency' more specifically or perhaps by defining the categories or types of authorities which will have access.