Internet Society of Australia
A Chapter of the Internet Society
ABN 36 076 406 801

PO Box 1705
North Sydney NSW 2059

23rd April 2014

ISOC-AU Submission

Senate Inquiry into the TIA

Introduction

The Internet Society of Australia (ISOC-AU) welcomes this opportunity to provide comments to the Inquiry into the Telecommunications Interception and Access Act.

ISOC-AU's interest is that of ensuring and promoting the development of an open and sustainable Internet for the benefit of all people. As such, our interest and membership spans users, developers, service providers and researchers in personal, commercial and not-for-profit contexts. Remarks will therefore be restricted to that affecting Internet services only, and not the broader telephony service context, except where its regulation affects Internet services. The Internet Society of Australia is the Australian Chapter of the worldwide Internet Society, the organisation which homes the Internet standards body, the Internet Engineering Task Force, and participates actively around the world in many Internet governance and policy discussions. Our expertise is in providing neutral, technically informed advice across jurisdictions.

By way of introduction to me -I am the President of the Australian Chapter, and I am also a member of the Internet Society's Board of Trustees. I have tertiary qualifications in Physics, Engineering and management including a masters degree in Engineering specialising in telecommunications as well 20 years experience designing, building and managing telecom and Internet networks. My current day job is with the Australian Communications Consumer Action Network, but I must make it clear that I am not speaking purely on behalf of the Internet Society of Australia.

ISOC-AU believes that the principles which apply in the physical world should continue to apply in the on-line world and applauds the Australian Government's support of the application of the United Nations Declaration of Human Rights to the Internet.

ISOC-AU, therefore, submits that any legislative change should adopt a technology neutral, principles based approach that would better withstand technological change and couple with a strict preservation of fundamental citizen rights. Any change should at least avoid being unduly technology specific as that cannot readily keep pace with technological change.

ISOC-AU also notes the broader context within which this inquiry is taking place. There is no doubt that Australia has some repairs to undertake on its international reputation as a result of recent revelations of extreme Internet surveillance. As we speak an international forum on Internet governance has been convened in Brazil at which there will be calls for something akin to a *Declaration of Rights for the Internet* or even an *Internet Magna Carta.*

Whether Australia joins such calls, or signs onto any such document, is yet to be seen, however there is a clear sentiment from users within Australia that there should be greater clarity over surveillance and for better online privacy protection. It is of major concern to us that increases in surveillance, by state actors and non-state actors, have a corresponding decrease in trust by users of the Internet – a vital and essential infrastructure for modern society.

Over recent times, also, much discussion has taken place on the concept of access to so-called metadata, with assertions that metadata does not include the content of a communication. We contend that without appropriate technological standards – defined by an independent standards body – this claim is inherently untrue. The existing mechanisms for gaining information about the material that transits across a telecommunications network, for example by using the web page addresses visited by a user, inherently contain specific addresses for many, many elements within the page, even third party elements in turn requested by the page, such as advertising. Thus the amount revealed about an individual, their family, workmates and broader community is potentially very large. In many cases also this data is dynamic and changes from moment to moment, and often today even depends on the types of other sites visited by uses with the advent of 'cookie correlation'. None of which under any control by the individual user. This is further complicated by the emergence of mobile device 'Apps' where users have extremely little awareness or control of background activity.

We further note that the European Court of Justice recently ruled against the retention of metadata and said: "By requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data."

The court was particularly concerned that: it "does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences."

The Joint Committee on Intelligence and Security's recent inquiry revealed that an astonishing number of parties have been granted access to metadata with extremely little oversight, no guarantees over destruction of the material after its acquisition, and certainly no right for redress by consumers when it is misused or exposed. We contend that this is an extremely disturbing situation as the potential for damage by misuse of this data is extremely high.

You have been told that there is a need to keep pace with modern technology through a demand for far reaching data logging capacity across public and private networks. We are concerned that this will lead to vast arrays of data being created and retained which will expose the population to greater risk disproportionate and trigger a costly surveillance arms race as serious criminals adopt more and more arcane ways of obfuscating their traffic.

In that same inquiry a request was made for an offence to be created where a person refused to provide encryption keys. We contend that this is an impractical offence due to the fact that in many cases an encryption key is automatically and dynamically created by software for the purpose of that transmission, destroyed after use and is often completely unknown to the user.

Policy Position

Shortcomings within the TIAA

ISOC-AU submits that the overall controls and reporting arrangements for lawful interception has in general been strong, however there is concern that the penalties for lapses in appropriate governance and controls over access to interception mechanisms have not been enforced. Furthermore, there should be clarity over which Act applies where competing legislation exists.

Destruction of Materials

ISOC-AU supports the Australian Law Reform Commission's recommendations with respect to the destruction of materials gathered under an interception warrant.

Clarification of Warrants

Existing provisions do not make it clear as to which specific services are required under a warrant. There should be no level of interpretation required by service providers as to which services to provide.

No Retention of Metadata

Without appropriate technology standards metadata not be retained beyond strict business need. Where metadata is retained there must be the strictest standards around retention and protection.

Reporting and Oversight of Metadata Access

Should access to metadata be granted considerably higher standards of access and oversight of these processes be implemented including penalties for breaches of standards.

Public Interest Monitor

We support the establishment of a public interest monitor (PIM) and ISOC-AU would be happy to assist in the establishment or operation of such.

Clarification of Entitlements to Metadata

Existing provisions do not make it clear as to which agencies have the right to gain access to metadata. Should metadata be defined, then there must be a clear understanding of which agencies are eligible to access communications information, and the proportionality of suspected crime must also be correspondingly high.

Concern Regarding Attribute Based Interception

Attribute based interception is at this stage extremely ill-defined. In practice, it could mean the creation of systems with high levels of complexity and capability, with ad-hoc methods of interrogating dynamic databases through scripts or other tools. Again, this will require a high dependency on logging and filtering, and the scope for error and is high.

No offense for Encryption Keys

No offense be created for the non-provision of encryption keys and any defence of not knowing keys be acceptable should one be created.

Cost to Consumers

Any further imposts on service providers will result in greater costs which ultimately will be directed to consumers. It is essential that these costs be taken into account and avoided wherever possible.

Closing statement

In closing I refer you to a recent statement of the Swedish Foreign Minister Carl Bildt, where he proposed the following principles be observed:
<http://www.regeringen.se/sb/d/17280/a/226590>

1. First, legality.

Surveillance needs to be based on laws.

These laws must be adopted in a transparent manner through a democratic process.

The implementation of these laws should be reviewed periodically to ensure that the expansion of surveillance capabilities due to, for instance, technological advances is properly debated.

2. Second, legitimate aim.

Surveillance must be conducted on the basis of a legitimate and well-defined aim.

Surveillance measures may never be carried out in a discriminatory or discretionary manner and only by specified state authorities.

3. Third, necessity and adequacy.

The law should justify that surveillance is necessary and adequate to achieve the legitimate aim.

4. Fourth, proportionality.

A sound proportionality judgment must be made, to carefully assess whether the benefits of surveillance outweigh its negative consequences.

5. Fifth, judicial authority.

Decisions on the use of communications surveillance should be taken by a competent authority.

As a general rule, an independent court should take such decisions.

6. Sixth, transparency.

States should be as transparent as possible about how they carry out surveillance.

They should provide information on how the surveillance legislation works in practice.

7. Seventh, public oversight of parliamentary or other credible institutions.

We need to scrutinise how the laws work, to create transparency and build trust and legitimacy.

Our obligation as governments is to provide security and to respect human rights - not either or.

Thank you again for this opportunity.

Narelle Clark
President
Internet Society of Australia
Ph: 0412 297 043
www.isoc-au.org.au