Submission No 145

Inquiry into potential reforms of National Security Legislation

Organisation: Internet Society of Australia

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

PO Box 1705
North Sydney NSW 2059

19 august 2012

To: Hon Anthony Byrne MP
Chair
Joint Parliamentary Committee on Intelligence and Security
Parliament House
Canberra ACT 2600
Via email: pjcis@aph.gov.au

ISOC-AU SUBMISSON: in response to the request for comments on the Inquiry into potential reforms of National Security Legislation

Introduction

The Internet Society of Australia (ISOC-AU) welcomes this opportunity to provide comments to the Inquiry into potential reforms of National Security Legislation.

The Internet Society of Australia (ISOC-AU) is a non-profit society founded in 1996 which promotes the Internet development in Australia for the whole community – private, academic and business users: the Internet is for everyone! ISOC-AU is a chapter of the worldwide Internet Society and is a peak body organisation, representing the interests of Internet users in this country. We have a longstanding and ongoing commitment to the effective representation of these interests in legislative and policy review, code development and self-regulatory processes in the telecommunications, domain name and Internet-related services industries.

Policy Position

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

ISOC-AU recognises that the technological basis for which some of the Acts are predicated is dated and does not recognise the flexibility and pervasiveness of modern technology. However, it may also be argued that some of the claims made within the Attorney General's Department (AGD) discussion paper are also flawed such as: "…clear, one-to-one relationship between the target of an interception warrant, telecommunication services used by the person, and telecommunications service providers..." (p.21). Indeed, unique relationships rarely existed when all an individual needed to do was to use someone else's telephone – with or without authorisation.

ISOC-AU, therefore, submits that any legislative change should adopt a technology neutral, principles based approach that would better withstand technological change coupled with a strict preservation of fundamental citizen rights.

Over the last two decades and more, access to the Internet has brought about tremendous commercial, educational and broad social benefits. ISOC-AU is concerned that should a substantial increase in surveillance be introduced within Australia there will be a corresponding risk to the

citizenry coupled with an increase in fear of the impact of surveillance. Citizens may therefore choose to use the Internet less, to create, deliver and use fewer services, thus stymying innovation and reducing the benefit it brings. This is not good for the Internet within Australia. The propensity for an increase in fears of this type have been documented elsewhere, such as in Omand et al 2012[i].

Many of the items referred to in the AGD discussion paper, if implemented, would result in an increase in capital and operational cost with attendant labour force requirements inside all network and content service providers involved. Even with some cost recovery from the Commonwealth, and in turn, the taxpayer, much of this cost will be passed on to Internet users. ISOC-AU wishes to express its concern for the overall cost of compliance and considers that there may be more effective means to obtain positive law enforcement outcomes.

In order to ensure the effectiveness of evidence so collected, there must be associated systems and procedures to protect and maintain the veracity of data collected. The cost of procuring, installing, maintaining and operating these, for example, would introduce further barriers to market entry and reduce competition, as well as potentially deter local service creation and location. This would effectively be a national impediment to innovation.

Existing classical voice systems produce logs that are often embedded with time stamps, and management systems, when implemented, possess audit controls listing which user made what changes where; newer systems, however, rarely have sophisticated management systems and produce text based logs that are readily tampered with and lacking the overall discipline and consistency required for evidence. Warrant management systems designed to interface with classical voice switches may not be adapted to the diversity of newer technology.

Over recent times, a number of groups have observed a lessening of Australian involvement in international technology standards development. ACMA noted[ii]:

> *The decline in Australian involvement in international telecommunications activity has meant that Australian is now overwhelmingly a "standards taker", adopting/adapting international standards for national conditions. This "standards taker" role is likely to continue into the future. This role has broader implications for technical regulation in Australia, including in relation to the role of national standards in the Australian regulatory framework and the recognition of overseas compliance marks in Australia.*

The declining lack of participation in global standards processes by Australians means that Australian technology interests are not taken into account in standards development. In addition it means that Australians are less readily able to translate into impact technology developments at their emergence. Thus the implementation of security measures to ensure the security of emerging systems may be overlooked.

ISOC-AU notes there are no Internet standards for interception data and the nearest thing would be metadata corresponding to IP routing and IP flows, and this corresponds to the traffic alone without higher order user data. Data of this type is extremely detailed and given the sheer dimensions of Australian communications networks today would result in massive quantities of data requiring secure storage. This would be a data deluge on a similar scale to that of our most robust scientific enquiry into astronomical phenomena!

The discussion paper is weak on oversight provisions and in particular, there appears to be a lack of apparent room for third party oversight, such as a public interest monitor, that would include consumer and independent technology advice. Reporting requirements should be designed to provide public transparency and regulatory control over abuses of the various schemes, and take

primacy over the convenience of law enforcement agencies.

Due to time limitations, not all subsections of the terms of reference are discussed. A lack of comment should not be construed as supporting the concept proposed. ISOC-AU would welcome the opportunity to comment further or to participate in ongoing consultation.

In summary, the Internet Society of Australia whilst having some sympathy for updating the various Acts referred to, holds serious and continuing concerns for the privacy of individuals, community groups and businesses, as well as the well-being of the Australian Internet, should the proposals be implemented as described.

Comments on the procedure used

The Internet Society of Australia (ISOC-AU) notes that it has not been approached to date to provide input into this review and fears a lack of broad consultation, particularly from the user base, and that this has been exacerbated by the relatively short time frames for submissions. ISOC-AU remains concerned that the short time frames have not yielded a sufficient period within which to address all of the matters contained in both the terms of reference and the AGD discussion paper.

The AGD discussion paper, which can be commended for the breadth of issues touched upon, is unclear and contains no certain path to clear proposals for legislation, or the timetable that one might expect. Very few proposals contained have sufficient depth for costing or for determining the full impact thereof.

ISOC-AU also considers that these legislative processes need to abide by the highest standards of diligence and consultation, given the gravity of the proposals, the wide ranging nature of the proposals, and the potential for severe penalties – to both society and individuals should mistakes be made.

Commentary on specific terms

Due to time limitations, not all subsections of the terms of reference are discussed. A lack of comment should not be construed as supporting the concept proposed. ISOC-AU would welcome the opportunity to comment further or to participate in ongoing consultation.

Proposal/s regarding Term 11. c "Enable the disruption of a target computer for the purposes of an access warrant" lacks clarity and detail.
ISOC-AU is concerned that this provision would apply equally to both a piece of critical infrastructure as it would to a domestic computer. The basis might on which this might be justified is also troubling. ISOC-AU believes that such an action must be commensurate with risk and take into account the type and quantity of services potentially being delivered on the target computer, such as domain name services, routing database information, and whether the computer is a critical part of a person or persons' legal livelihood or well-being.

Term 14 a. "Expanding the basis of interception activities"
Unclear and concern that it would reach into areas not previously covered such as content service providers without the depth of skill previously found in telecommunications carriers. Concern that small players, such as community groups, would be retaining data with limited ability to protect such data.

Term 15 c. 'tailored data retention periods for up to two years for parts of a data set, with specific time frames taking into account agencies priorities, and privacy and cost impacts'.

In Australia to date, it is sad to say that the telecommunications industry has suffered a number of

serious breaches of privacy of individuals, and there exist cases which appear to have flagrant disregard for privacy in making use of data sets for commercial gain[iii]. Indeed most recently the vulnerability for further exposure was highlighted by the so-called hacktivist group 'Anonymous' who exposed data belonging to a prominent service provider[iv]. Telecommunications carriers are accustomed to high levels of regulation and the attendant compliance burden, thus one would expect better adherence to procedure and better regard for customer privacy and the TIA 1979 as it stands. ISOC-AU remains deeply concerned that if sophisticated players cannot ensure customer privacy, what would smaller operators, newer entrants, content providers and third party players suffer?

In its media release of 30 April 2012, the Office of the Australian Information Commissioner stated: "The Office of the Australian Information Commissioner (OAIC) was notified of 56 data breaches in the last financial year, equivalent to a data breach a week. This is up from 44 in the previous year, an increase of 27 per cent," Mr Pilgrim said. However, the Privacy Commissioner also noted that he opened a further 59 investigations into other breaches where he wasn't notified of the incident.

As referred to also in the Policy Position section above, the capacity of modern network equipment to produce terabytes of data with attendant storage, management and analysis costs for both the communications service providers as well as law enforcement agencies should not be underestimated. The potential for law enforcement agencies to be swamped by data is very real.

Term 16 a. 'by instituting obligations on the Australian telecommunications industry to protect their networks from unauthorised interference'

ISOC-AU welcomes the concept of performance standards and promotion of, and potential adherence to, higher levels of security in Australian Internet networks and their underlying suppliers. To date we have seen a paucity of Australian providers adopt important standards such as DNSSEC and efforts such as IPSEC and databases to improve routing security. ISOC-AU would be keen to assist in such efforts to further promote appropriate levels of Internet security within Australia.

Security is, however, a double-edged sword. The imposition of security requirements must be done carefully and with appropriate support and be kept current. The appearance of security must not be allowed to undermine the performance of these networks. For example the installation of firewalls across Internet networks would impose a significant capital and operational cost, and not necessarily meet appropriate security standards particularly where ill-maintained, low throughput devices are used. Well-designed, properly maintained, network equipment can meet corresponding security performance without the need for external firewalls.

Term 16 b. 'by instituting obligations to provide Government with information on significant business and procurement decisions and network designs'

Proposals associated with this term are vague and it is unclear what might constitute 'significant'. In order to support the evidence for such a requirement some questions are posed: does the Government intend to provide a service listing devices containing security or other fundamental flaws rendering them unsuitable for deployment? Such a service would need to be kept current, and complemented by a test service such that communications service providers could validate whether existing equipment was suffering vulnerabilities.

Term 16 c. 'Creating targeted powers for Government to mitigate and remediate security risks with the costs to be borne by providers' Government would need to maintain sufficient skill in-house to support such an activity even if a regime of audits and external auditors was used. The telecommunications industry itself has reported difficulty in recruiting and maintaining staff.

Term 16.d. 'Creating appropriate enforcement powers and pecuniary penalties': ISOC-AU recommends that penalties be commensurate with the risks involved.

Term 17.a. 'Using third party computers and communications in transit to access a target computer under a computer access warrant.'

ISOC-AU is extremely concerned that extensions to this power could be unduly wide ranging and implicate law abiding citizens inappropriately. Furthermore inappropriate access by unskilled personnel to pieces of critical Internet infrastructure can have serious and widespread consequences. The Australian Government should consider very carefully the ramifications of such a power.

Narelle Clark
President
Internet Society of Australia

---

[i] Sir David Omand, Jamie Bartlett, Carl Miller, 2012, #intelligence, Demos, ISBN 978-1-909037-08-3
[ii] ACMA Technical Advisory Group Minutes 30 August 2008
[iii] http://www.itwire.com/business-it-news/security/55578-privacy-thodey-thumps-telstra-team-over-trust-breach
[iv] http://www.itnews.com.au/News/309902,aapt-confirms-data-breach.aspx