



iiNet Limited
ACN 068 628 937

head office
level 1, 502 hay street
subiaco wa 6008
phone: 1300 722 545

support: 13 22 58
sales: 13 19 17
fax: 1300 785 632

email: iinet@iinet.net.au
web: www.iinet.net.au

Senate Standing Committee on Legal and Constitutional Affairs - Comprehensive revision of Telecommunications (Interception and Access) Act 1979

Introduction

Thank you for the opportunity to provide comments to the Committee for its Review of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act).

iiNet is Australia's second largest DSL Internet Service Provider (ISP) and the leading challenger in the telecommunications market. We maintain our own super-fast broadband network and support over 1.8 million broadband, telephony and Internet Protocol TV services nationwide.

iiNet has previously contributed to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) *Inquiry into Potential Reforms of Australia's National Security Legislation* which reported in May 2013. We direct you to our written [submission](#) to that Committee and in particular our submissions in relation to mandatory data retention.

Necessary and proportionate

iiNet agrees with the position clearly articulated by the Law Council of Australia in its [submission](#) that where a State seeks to restrict human rights, such as the right to privacy, for legitimate and defined purposes, in this case in the context of telecommunications access and interception, the principles of necessity and proportionality must be applied.¹

For example, iiNet agrees with the PJCIS's recommendation that the Attorney-General's Department review the threshold for access to telecommunications data and that such a review should reduce the number of agencies able to access telecommunications data by using gravity of conduct which may be investigated as the threshold on which access is allowed. [Analysis](#) of the publicly available figures has revealed that:

No less than 40 government agencies made [293,501 warrantless requests](#) for metadata from internet service providers in the 2011-12 financial year. Just 56,898 of those requests were made by the Federal Police, which has the primary criminal law-enforcement role. The RSPCA, Wyndham City Council, the Tax Practitioners Board and even the Victorian Taxi Directorate also have been allowed to access individual telecommunications data for a 'law-enforcement purpose'.

As noted by the Attorney-General's Department in its [submission](#)² to this Committee, a revised regime could, in particular, restrict access to telecommunications data to a narrower range of law enforcement, anti-corruption and national security agencies that have a demonstrated investigative need for access to that range of information, and which are subject to independent oversight.

Mandatory data retention

iiNet is concerned that a number of law enforcement agencies, such as the NT, Victorian and WA Police, have in the course of this Review again submitted that the government should introduce a mandatory data retention regime.

¹ For a further elaboration of these principles, we draw the Committee's attention to the [International Principles on the Application of Human Rights to Communications Surveillance](#)

² Page 20.

These proposals extend to data not currently collected by all service providers. For example, iiNet does not retain browsing history. Even if we did retain this data, the Australian Privacy Principles highlight that best practice is to not retain personal information for any longer than we need the data³.

iiNet agrees with the observations made in Communications Alliance/AMTA joint industry [submission](#) that:

- a data retention scheme will involve an increased risk to the privacy of Australians and provide an incentive to hackers and criminals;
- data retention is at odds with the prevailing policy to maximise and protect privacy and minimise the data held by organisations. Industry believes it is generally preferable for consumers that telecommunications service providers retain the least amount of data necessary to provision, maintain and bill for services.

The Office of the Australian Information Commissioner has spent considerable time and resources since November 2012 educating businesses and the community about the new [Australian Privacy Principles](#) (APPs) which commenced in March this year. iiNet only needs to retain the data required for us to deliver the services for our customers, in line with the APPs and additional data is only retained when authorised. Relevantly, APP 3.2 provides:

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

So on one hand, we have one government agency highlighting the need for businesses like iiNet to respect and protect our customer's personal information and on the other, government agencies again calling for mandatory data retention with too little evidence about the necessity, or efficacy, of such a regime.

On a practical level, we know the quantity of fixed line broadband services is at about 6 million in Australia but the number of mobile services is over [30 million](#). Who knows how many tablets, gaming consoles, or even - in the age of the Internet of Things - mythical internet fridges there are, that will need to have their data stored? By 2020 global IP addresses are predicted to pass 50 billion in use. It is an impractical idea to store such data and it is even more impractical to suggest that a law enforcement agency, can simply call up a service provider and say "Give me all Joe Blow's URLs for 15 June 2012".

Customer information, retained in line with mandatory data retention requirements, would also need to be carefully encrypted and securely stored. Unfortunately, security breaches can and will occur. As iiNet highlighted in our oral [statement](#) to the PJICIS, our estimate is that complying with such a scheme would require a large data centre storing possibly 20 thousand terabytes of data at a cost of around \$60 million. There is no indication that the government would pay these costs, so our customers would have to pick up the costs in the form of a new tax collected by our industry.

Contrary to the Attorney-General Department's submission to this Committee, access to telecommunications data is not necessarily less privately intrusive than access to the content of a communication. We draw the Committee's attention to recent [research](#) from Stanford University which should put to bed the fallacy that the community should only be concerned about access to telecommunications content and not "metadata" or telecommunications data. Telecommunications data when accessed and analysed may create a profile of a person's life including medical conditions, political and religious views and associations:

The researchers initially shared the same hypothesis as their computer science colleagues, Mayer said. They did not anticipate finding much evidence one way or the other.

³ See Australian Privacy Principle 11.2

"We were wrong. Phone metadata is unambiguously sensitive, even over a small sample and short time window. We were able to infer medical conditions, firearm ownership and more, using solely phone metadata," he said.

It's not at all clear that this increased surveillance and fundamental privacy risk, together with the significant cost, is either necessary or proportionate. We've not seen solid evidence that justifies surveilling minors and citizens on the chance that two years later some evidence might help an investigation.

iiNet is uncomfortable with the notion that commercial businesses may be forced into a role as unwilling agents of the state to collect, store and safeguard very large databases for which the companies themselves have no use – a role very different from that which those companies were originally established.

Website blocking

One of the difficulties for law enforcement agencies, service providers and the community is that relevant provisions concerning privacy are distributed between parts of the TIA Act and the Telco Act, making it difficult to clearly understand how the privacy of telecommunications is protected.

iiNet reiterates its concern with law enforcement agencies use of [section 313](#) of the Telco Act to force ISPs to block websites. This provision obliges carriers and carriage service providers "*...to do their best...*" to ensure that their networks and facilities are not used to commit offences.

The controversial use by ASIC of section 313 is one example of how the exercise of this power can contravene the principles of necessity and proportionality discussed above. iiNet is also very concerned about the lack of appropriate due process, accountability and oversight. The scope of this law enforcement obligation is vague and uncertain and unfairly puts the onus on testing the validity of the request on the service provider. It is critical that any exercise of section 313 powers to block websites must be accompanied by sufficient information to confirm that it is appropriately authorised by a senior representative of the relevant agency.

In this context, iiNet last year developed an internal Site Blocking Policy which we believe could provide an appropriate framework for other service providers in considering such requests and for the government in narrowing the scope of section 313. iiNet works to achieve an appropriate balance between complying with its legal obligations to action requests from agencies to block websites and ensuring that such requests are legally justified.

We've outlined the fundamental components of this policy below:

- iiNet will block sites only where external requests for compliance with legal obligations are supported by legitimate authorisation, appropriate legislation and due process.
- Any requests which do not meet the minimum criteria outlined in the policy will be declined.
- Any request that meets the requirements of this Policy must be approved by an iiNet executive before a site block can be implemented.
- While the obligations in section 313 are broad, iiNet must be diligent in testing all such requests to ensure that they meet reasonable standards.
- iiNet insists that requests for the blocking of infringing sites also provide (at a minimum):
 - a) personal contacts of the requestor in the relevant Authority;
 - b) a redirection page with details of the reasons for the block and appropriate remediation or appeal processes for the affected parties;

- c) evidence that the site contains prohibited content and/or is the subject of a relevant court order or judgment.

iiNet welcomes any questions from the Committee relating to this submission or the terms of Reference for this Review more generally.