# Draft Telecommunications and Other Legislation Amendment Bill 2015
# Submission to the Attorney-General's Department

## Introduction

Internet Australia (IA) welcomes the opportunity to provide comments on the Draft Telecommunications and Other Legislation Amendment Bill 2015.

IA appreciates the critical role that telecommunications networks and facilities play in our national security and the need for appropriately robust telecommunications infrastructure. However, we consider that in its current form the Bill represents an unacceptable and unreasonable transfer of responsibility and oversight from the Parliament to the bureaucracy.

Furthermore, we are concerned that even allowing for conscientious consideration of industry's needs, this Bill places too much arbitrary power in the hands of the Secretary of the Attorney General's Department.

Our ongoing experience with the problematic implementation of the Data Retention Act gives us little confidence in the ability of the department to fully appreciate the technical issues involved. This is not a criticism of any individuals, or of the department *per se,* it is simply the observation that the essential level of technical knowledge in respect of telecommunications systems and equipment is not resident in the department. With this legislation, as was the case with the Data Retention Act, an appropriate and sensible move would be for the Communications Department to be more directly involved and consulted.

A potential, if unintended, consequence of the powers vested in the bureaucracy through this draft Bill is a hampering of innovation and the evolution of telecommunications networks. It also threatens to distort the proper free market in which the telecommunications sector is provided with goods and services.

IA has recently called for a Digital Future Forum[1] aimed at creating a bipartisan blueprint for our digitally enabled economic future. At the centre of this blueprint must be the encouragement of local entrepreneurs and manufacturers. We fear that in its current form the Bill will entrench legacy systems and legacy providers (most likely to be large foreign owned corporations).

[1] https://www.internet.org.au/news/92-30-june-2015-internet-australia-calls-for-a-digital-future-forum

Internet Australia urges the Government to consider, as an alternative, a robust and workable regime by which the objectives of the Bill are addressed without the imposition of legislation. Through significantly greater collaboration with peak bodies, such as ourselves, the creation of appropriate industry-developed standards might well achieve the same outcome - delivering the Government's objective in a manner more acceptable to the telecommunications industry.

IA also has these specific concerns about the draft Bill:

- The apparent lack of coordination between recent telecommunications inquiries and proposed amendments to the *Telecommunications Act 1997*;

- The lack of explicit recognition that it is industry's as well as the Government's interest to have as secure networks as is reasonably possible;

- The need for this legislation to:

    - create a partnership between the Government and industry to achieve secure national telecommunications networks and facilities;

    - support the development of guidelines that assist different sections of the industry in understanding and complying with the requirements for secure networks and facilities; and

    - reinforce existing requirements for continued protection of privacy, including those in the Privacy Act.

## Relationship with Previous Inquiries

In finalising this legislation, recent amendments to the Act and recommendations from recent inquiries should be taken into account.

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* has raised a range of issues for industry including the need to more clearly define what data must be retained by industry and how the costs of retaining that data will be met. Indeed, the industry is still working with the Attorney-General's Department (AGD) to clarify details of the data that should be retained. It is also becoming clear that compliance with the legislation will impose significant costs on industry, particularly on the smaller industry participants. All of those costs will ultimately be borne by Australian Internet users, either by way of taxation or increased Internet service charges by service providers.

The recent report of the House of Representatives Standing Committee on Infrastructure and Communications on section 313 of the Act reviewed that section's requirements on the blocking of access to illegal online services.

It is clear from the evidence given to that inquiry that technical knowledge and expertise are required to ensure that such legislation is implemented in the way in which the Government and Parliament intended. This is reflected in the report's second recommendation.[2]

> The Committee recommends to the Australian Government that all agencies using section 313 of the *Telecommunications Act 1997*, to disrupt the operation of illegal online services have the requisite level of technical expertise within the agency to carry out such activity, or established procedures for drawing on the expertise of other agencies.

Indeed, the Committee's conclusions acknowledged the need for a better understanding of technology, combined with better processes to prevent problems from occurring in the use of the existing section 313 for blocking sites, and acknowledged the potential costs for ISPs in complying with requests under that section.[3]

The lessons from both highlight the technical complexity involved in implementing Government policy for telecommunications, the additional costs to industry with each new change in policy and time necessary for industry to implement the requirements placed on it under this and other legislation.

**Recommendations**

1. **That Clause 2 of the Bill be amended to give industry at least 12 months after Royal Assent to comply with requirements of the Act.**

2. **That in the further drafting of this Bill and subsequently making decisions pursuant to the legislation the Attorney General's Department be required to consult with the Communications Department.**

## Industry and Network Security

Some evidence given to the PJCIS inquiry on national security legislation questioned the need for Government intervention of this issue. Macquarie Telecom, for example, stated in its submission:

> We are not saying that means that the entire Australian network and national security is in perfect hands, but we want to bring it to the attention of the committee that there are market responses going on that ought to be taken into account when thinking about what the broader regulatory arrangements should be that affect all players.[4]

---

[2] House of Representatives Standing Committee on Infrastructure and Communications, *Balancing Freedom and Protection: Inquiry into the use of Subsection 313(3) of the Telecommunications Act 1997 by government agencies to disrupt the operation of Illegal Online Services*, 1 June 2015, Recommendation 2 p. 63

[3] Ibid p. 51

[4] PJCIS, n 1, p. 73.

While others supported the introduction for a regulatory framework for network security, the emphasis was on the Government's role in setting security objectives, but leaving the more complex, technical issues to industry to address. For example, Optus submitted that:

> We support the idea that a scheme should be targeted to achieve and verify outcomes, rather than be prescriptive about particular business practices, network designs or purchasing decisions.[5]

## Proposed Objectives

The objectives of the Act do not include network stability and security. IA believes that such objectives should be incorporated into the Act.

The objectives should recognise that achieving network stability and security must be a cooperative endeavour between the Government and industry participants.

The objectives proposed by AGD in 2012 clearly state the desired objectives of a security framework for telecommunications, which recognised that partnership:

- government and industry have a productive partnership for managing national security risks to Australia's telecommunications infrastructure,
- security risks relating to Australia's telecommunications infrastructure are identified early, allowing normal business operations to proceed where there are no security concerns and facilitating expedient resolution of security concerns,
- security outcomes are achieved that give government, business and the public confidence in their use of telecommunications infrastructure for both routine and sensitive activities,
- the protection of information, including customer information and information about customers, contained on or transmitted across telecommunications networks is better assured, and
- compliance costs for industry are minimised.[6]

An express statement of these objectives in the Act should recognise that industry has both the incentive and the expertise to ensure the safety and stability of telecommunications networks and facilities.

[5] Ibid p. 75

[6] Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, quoted in PJCIS report, p. 34.

**Recommendation**

3. **That the Act be amended to include an objective for industry protection of their networks and facilities from unauthorised interference or unauthorised access.**

## Implementation of the Bill

The Explanatory Memorandum makes it clear that this draft legislation has been introduced pursuant to Recommendation 19 of the PJCIS inquiry into national security.[7]

However, that recommendation included the issues raised by the Inquiry that should be addressed in the implementation of the recommendation as follows:

> The Committee further recommends that the Government, through a Regulation Impact Statement, address:
>
> - the interaction of the proposed regime with existing legal obligations imposed upon corporations;
> - the compatibility of the proposed regime with existing corporate governance where a provider's activities might be driven by decisions made outside of Australia;
> - consideration of an indemnity to civil action for service providers who have acted in good faith under the requirements of the proposed framework; and
> - impacts on competition in the market-place, including:
>   - the potential for proposed requirements to create a barrier to entry for lower cost providers;
>   - the possible elimination of existing lower cost providers from the market, resulting in decreased market competition on pricing; and
>   - any other relevant effects.[8]

**Recommendation**

4. **The legislation and its Explanatory Memorandum, as finally passed, should address all of the issues raised by the PJCIS Inquiry into National Security.**

## Test for Compliance

The Bill would require carriers and carriage service providers (including intermediaries) to 'do their best' to protect their networks and facilities from 'unauthorised interference or

[7] Explanatory Memorandum (EM) Telecommunications and Other Legislation Amendment Bill 2015, p. 3.
[8] PJCIS, n 1. p. 84.

unauthorised access', and ensure both the 'availability and integrity' of their networks and the 'confidentiality of communications' carried on and information contained in those networks.[9]

The way that the term 'do your best' in section 313 has been interpreted by the Government was explained by the Department of Communications:

> The section is drafted in a way that they can provide the assistance that they are capable of providing – their best endeavours. If they have that flexibility then that also allows them to say back to the requestor, 'instead of doing it like that, we could do it like this'.[10]

The flexibility for industry compliance allowed by amendments to section 313 is in contrast to the Directions Power that would be given to the Attorney General's Secretary in the new Division 4.

Under the proposed clause 315B, the Secretary has very broad powers to direct carriers or carriage service providers to do, or not do, anything in relation to the supply of networks or facilities, as long as the Secretary is satisfied that it involves a 'risk of unauthorised interference with, or unauthorised access to, the networks or facilities, and, as a result, presents a 'risk to security'.[11]

## Procedural Fairness and Transparency

The Explanatory Memorandum suggests that:

> The C/CSP will also be afforded procedural fairness by way of an opportunity to make representations to the Secretary about the proposed exercise of the directions power.[12]

However, there is nothing in the Bill that requires such procedural fairness. The only requirements for consultation prior to making a direction are for the Secretary to consult the Director-General of Security and the Communications Secretary.[13] The Bill specifically 'does not limit the persons' with whom the Secretary may consult – but does not require any such consultation?[14]

Directions given under proposed sections 315(A) or (B) must be given to the ACMA. However, it is not clear whether the ACMA would make such directions public. Further, the Attorney-General may give directions to the Attorney-General's Secretary about the exercise of the

[9] Telecommunications and Other Legislation Amendment Bill 2015 (the Bill) Clauses 1A and 2A
[10] House of Representatives Standing Committee on Infrastructure and Communications, *Balancing Freedom and Protection: Inquiry into the Use of Subsection 313(3) of the Telecommunications Act 1997 by Government Agencies to disrupt the operation of Illegal Online Services*, (S 313 Report) Evidence given by Trudi Bean, Deputy General Counsel, Department of Communications, p. 15.
[11] Bill, Clause 315B(1)
[12] EM p 14
[13] Bill Clause 315B(3)
[14] Bill Clause 315b(4)

Secretary's power of direction under proposed section 3125(B) but such a direction is not a legislative instrument and therefore, not subject to Parliamentary scrutiny.[15]

**Recommendation**

5. **All directions made under proposed sections 315(A) and (B) be made legislative instruments and therefore subject to Parliamentary scrutiny.**

## Clarity on Coverage

The Bill only refers to carriers and carriage service providers, suggesting that all providers will be covered by the Bill's requirements. However, the Explanatory Memorandum suggests that some (all?) requirements may fall only on 'nominated' providers.[16]

The actual 'nomination' process will be done under the *Telecommunications (Interception and Access) Act 1979,* s. 197(4). Under that Act, there is no process for industry involvement in the 'nomination' process and such nomination is not a legislative instrument and therefore not subject to Parliamentary scrutiny.[17]

Therefore, there is no clarity in this draft Bill as to whether the legislation will cover all carriers or carriage providers or only those nominated. Furthermore it does not state which providers will or will be 'nominated' as mentioned under the Explanatory Memorandum (but which is not referred to in the Bill).

## Impacts on Industry

Because of the width of the directions power, and the absence of any requirement for consultation with industry, the likelihood is that industry will be forced to gravitate towards a few compliant vendors. Innovation in relation to the development of new products and services, therefore, is likely also to be impacted.

Smaller service providers are unlikely to offer new products that potentially risk the intervention of the Attorney-General. As Vodafone submitted to the PJCIS;

> A regulatory regime that mandates external controls over procurement and network design practices and requires extensive notification practices would certainly amount to an overly prescriptive level of intervention. The Associations believe that such a regulatory framework would restrict the ability of network and infrastructure providers to cost-effectively implement platforms that are innovative, progressive and provide supplier differentiation. Controls over procurement would also unnecessarily increase timeframes for network rollouts, which would contradict the Government's advocacy for increased broadband deployment.[18]

---

[15] Bill Clause 315B(7) and (9)
[16] EM p. 8
[17] TIAA s. 197(5)
[18] PJCIS report p. 76, quoting Vodafone's submission

**Recommendation**

6. **That section 313 be amended to allow industry to develop guidelines, in consultation with the AGD, on what will amount to compliance with the amended section 313 by various sectors of the industry.**

## Protection of Personal information

Both the Data Retention Act and this draft legislation present significant challenges to privacy protections in Australia.

The proposed clauses 313(1A) and (2A) in this Bill reiterate the obligation on carriers and carriage service providers (and their intermediaries) to do their best to protect the confidentiality of both the communications carried on networks and information on those networks.

However, nothing else in the Bill recognises the necessary balance that must be struck between law enforcement/security and privacy.

**Recommendation**

7. **That the Government consult closely with the Office of the Australian Information Commissioner in the final drafting of the legislation and ensure that the OAIC is adequately resourced to assist in this task.**

**About Internet Australia**

Internet Australia is the not-for-profit peak organisation representing everyone who uses the Internet. We are a broad member-based organisation not an industry lobby group. Our mission – "Helping Shape Our Internet Future" – is to promote Internet developments for the benefit of the whole community, including business, educational, government and private Internet users. Our directors and members hold significant roles in Internet-related organisations and enable us to provide high level policy and technical information to Internet user groups, governments and regulatory authorities. Through our participation as the Australian chapter of the global Internet Society we contribute to the development of international Internet regulations and policies.