Submission No 187

Inquiry into potential reforms of National Security Legislation

Name: Peter Lee
Chief Executive Officer

Organisation: Internet Industry Association (IIA)

INTERNET INDUSTRY ASSOCIATION

PO BOX 3986,
MANUKA ACT 2603
P: 02 6232 6900
F: 02 6232 6513
www.iia.net.au
ABN 71 071 075 575

Internet Industry Association

Submission to Parliamentary Joint Committee on Security and Intelligence

The Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
CANBERRA ACT 2600

By email: pjcis@aph.gov.au

20 August 2012

Inquiry into potential reforms of national security legislation

Introduction

The Australian Government has asked the Parliamentary Joint Committee on Intelligence and Security (**the Committee**) to consider a package of national security ideas comprising proposals relating to the following legislation:

- *Telecommunications (Interception and Access) Act 1979* (**TIA Act**);
- *Telecommunications Act 1997* (**Telco Act**);
- *Australian Security Intelligence Organisation Act 1979* (**ASIO Act**); and
- *Intelligence Services Act 2001* (**IS Act**).

As such, the Committee has commenced an inquiry into potential reforms of national security legislation (**the Inquiry**) and invited interested persons and organisations to provide a submission addressing the terms of reference of the Inquiry[1] (**Terms of Reference**). The Attorney-General's Department (**AGD**) has released a discussion paper [2](**the Discussion Paper**) to accompany consideration by the Committee of the potential reforms, which includes the Terms of Reference.

[1] The Terms of Reference of the Inquiry are set out in Chapter One of the Discussion Paper – available on the Committee website at: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/index.htm

[2] *Equipping Australia Against Emerging and Evolving Threats* - July 2012

Having regard to:

- the desirability of comprehensive, consistent and workable laws and practices to protect the security and safety of Australia, its citizens and businesses;

- the need to ensure that intelligence, security and law enforcement agencies are equipped to effectively perform their functions and cooperate effectively in today's and tomorrow's technologically advanced and globalised environment, and

- the fact that national security brings shared responsibilities to the government and the private sector:

the Committee is to inquire into potential reforms to key legislation, consider the effectiveness and implications of any proposals to ensure law enforcement, intelligence and security agencies can meet the challenges of technology evolution required within a modern agency framework and assess the need for enhancements to the security of the telecommunications sector.

The Internet Industry Association (**IIA**) appreciates the opportunity to provide a submission to the Committee inquiry into potential reforms of national security legislation.

About the IIA

The IIA is Australia's leading industry body for Internet commerce, content and connectivity. Founded in 1995, IIA promotes a faster, safer, secure, fairer and more trusted Internet. Members include telecommunications carriers and carriage service providers (**C/CSPs**), content creators and publishers, web developers, e-commerce traders and solutions providers, hardware vendors, systems integrators, banks, insurance underwriters, technology law firms, educational institutions, research analysts, and those providing professional and technical support services. Increasingly, our members also include businesses hoping to establish an effective on-line presence for the purposes of e-commerce, while we also provide guidance to the general public on Internet related issues.

On behalf of its members, the IIA provides policy input to government and advocacy on a range of business and regulatory issues, to promote laws and initiatives which enhance access, equity, security, reliability and growth of the Internet within Australia.

In preparation for the drafting of this submission, the IIA asked its members to comment on the legislative aspects of the Inquiry and the associated Terms of Reference. We received a diversity of views and comments from IIA members. We have assessed those comments and provide the following summary, implications, considerations and conclusions associated with the potential reforms of national security legislation.

Executive summary

IIA acknowledges and supports, in principle, the requirement for our law enforcement and intelligence agencies to have the necessary powers and capabilities to respond to threats from all forms of terrorism, serious and organised crime and cyber-crime.

However, potential reforms need to be considered with an appropriate level of checks and balances that do not unnecessarily impact on the rights or privacy of an individual, business or the community that society rightly demands. Further consideration also needs to be given to the cost and impact of the reforms on the telecommunications sector, particularly C/CSPs, to ensure that unreasonable and unnecessary regulatory burden and costs are not being imposed on the industry.

The Terms of Reference states[3] that the National Security Legislation, subject of the Inquiry, has three different elements and objectives:

1. modernising lawful access to communications and associated communications data;

2. mitigating the risks posed to Australia's communications networks by certain foreign technology and service suppliers; and

3. enhancing the operational capacity of Australian intelligence community agencies.

While acknowledging that our national security capabilities need to keep pace with technology and the evolving methodologies employed by terrorists and organised criminals, the Discussion Paper itself does not go to sufficient detail to justify any radical changes to the legislative framework.

Citing that potential reforms of national security legislationare required for the greater good of protecting the national interests without sufficient detailed evidence to support the justifications, on which they are based, requires further consideration to ensure that any potential reforms achieve an appropriate and acceptable balance between:

- the human rights and privacy of individuals;

- the cost and impact of the reforms on the telecommunications sector, businesses and the community; and

- the needs of law enforcement agencies to be efficiently equipped with the skills, technologies and legislative powers required in a rapidly changing telecommunications world.

The IIA acknowledges that the Australian Government (**the Government**) has a responsibility to ensure that Australian law enforcement and security agencies are not only equipped with the right level of skills and technology, but are also not restricted in fulfilling their mandate to protect Australia from threats and criminal activity by an out dated or ineffective legislative framework.

Requesting the Committee to consider a package of national security ideas is recognised as a positive step to progressing potential reforms. However, the Inquiry should be considered as just one step in an ongoing process for consideration of these reforms. Any subsequent

[3]The Discussion Paper, p.7

report/recommendations from the Inquiry should be subject to further consultation, particularly where significant amendments to legislation are envisaged as a result, which should also be subject to further consultation rather than just introduced into Parliament for debate and passage.

Additionally, the Terms of Reference states that the proposals across the three different packages, subject of the Inquiry, are separated into three different groupings:

A. those the Government wishes to progress (**Group A**);

B. those the Government is considering progressing (**Group B**); and

C. those on which the Government is expressly seeking the views of the Committee (**Group C**).

Although the package is referred to the Committee in its totality, on face value, it appears that the Government's grouping of packages implies that Group A may already be a *'fait accompli',* Group B is likely to progress following the Inquiry and the outcome of Group C will be determined based on the express views of the Committee.

As such, the IIA would recommend that further detailed consultation on a number of the reform proposals are required before any definitive conclusions can be made on their merits, including, but not limited to:

- clarifying the streamlining of information sharing between agencies, including the regulatory and enforcement role of the Australian Communications and Media Authority (**ACMA**);

- reducing the number of agencies eligible to access communications information and how that relates to the streamlining of information sharing;

- changes to mandatory record-keeping standards;

- the standardisation of warrant tests and thresholds;

- the removal of legislative duplication and associated impacts;

- aligning industry interception assistance with industry regulatory policy;

- expanding the basis of interception activities;

- the application of proportionality tests for issuing of warrants;

- the implementation of detailed requirements for industry interception obligations;

- the extending of the regulatory regime to ancillary service providers not currently covered by the legislation; and

- the implementation of a three-tiered industry participation model.

The IIA believes that a base set of principles should be applied by the Committee in their assessment of the degree of effectiveness to which the proposed reforms will achieve the desired national security outcomes. This assessment needs to be balanced to also ensure that any implications, including costs, which may be imposed on the telecommunications industry, are fair and reasonable and that the privacy and rights of individuals are protected to the extent that society rightly demands.

Implications

While it's not unexpected that national reforms of the scale and nature being proposed are likely to have an impact on any number of stakeholders, individuals and the community, it should not be considered a *'fait accompli'* that the proposed reforms should just be accepted for the good of the nation's security and intelligence interests without conducting an appropriate analysis and considering the effectiveness, implications and outcomes of such reforms.

The IIA acknowledges that the Government's referral to the Committee to consider a package of national security ideas and proposed legislative reforms and the Committee's subsequent Inquiry are positive steps in that ongoing review process. However, it is worth taking the time to assess what the potential implications of such reforms could mean for all stakeholders by posing a number of questions for consideration in light of some of the proposals.

<u>What are some of the proposals and what could they potentially mean?</u>

1. Review privacy framework within the TIA Act

   Does this equate to: *more secret interception and access?*

2. More specific technical requirements to cater for a diverse and sophisticated telecommunications environment

   Does this equate to: *mandated and/or unnecessary technical requirements?*

3. Extending the interception regime to such social networking and cloud providers

   Does this equate to: *regulation of social media and online services currently outside the interception framework?*

4. A tiered model with a sliding scale of interception and delivery capability depending on the size of the provider

   Does this equate to: *more regulation and obligations for companies with more market share?*

5. Retention of current information and assistance to agencies to decrypt information

Does this equate to: *more regulatory impost on business to capture, secure and store data not otherwise necessary for conduct of business? Will there be compensation? What's the risk of unauthorised access?*

6. Clarify the role of the ACMA and industry standards, expanding the range of regulatory options available to the ACMA

   Does this equate to: *more standards to deal with data retention, facilitating interception, wider powers to deal with non-Telco service providers and more enforcement powers?*

7. Establish a risk based regulatory framework

   Does this equate to: *secure services that are hard for the government to access being subject to the greatest degree of regulation?*

8. All C/CSPs to protect their infrastructure and the information held on it or passing across it from unauthorised interference

   Does this equate to: *more carrier obligations and regulatory requirements?*

9. C/CSPs to provide Government with information to assist in the assessment of national security risks to telecommunications infrastructure on request

   Does this equate to: *issues of cost recovery, compensation and the cost of maintaining the capacity to assist?*

10. Compliance framework based on C/CSPs demonstrating competent supervision and effective controls over their networks. C/CSPs to demonstrate compliance to Government on request (compliance assessments and audits)

    Does this equate to: *additional audit and reporting requirements?*

11. C/CSPs to help establish whether national security concerns can be co-operatively addressed

    Does this equate to: *increased importance and recognition by the Government of industry self-regulation (such as the iCode) and similar approaches?*

12. Graduated suite of enforcement measures so C/CSPs who are ineffective, or blatantly disregard security information are directed to targeted mitigation or remediation of security risks (modifications to infrastructure, audit, and ongoing monitoring). Administrative penalties or directions to C/CSPs imposed where a risk has been assessed as significant and prior engagement has proved ineffective.

    Does this equate to: *more powers and potential penalties?*

13. Computer access warrant issued in relation to a computer, computers on particular premises, computers connected to a particular person or a computer network. Single warrant covering all ASIO Act warrant powers where the relevant legislative thresholds are satisfied. Streamlining of warrants so that fewer applications are required for broader warrants

Does this equate to: *a broadening of search and seizure powers?*

14. Introduction of an authorised intelligence operations scheme

    Does this equate to: *providing ASIO officers and human sources with protection from criminal and civil liability for certain conduct in the course of authorised intelligence operations?*

15. *"The requirements are aimed at ensuring that agencies keep appropriate records necessary to demonstrate that agencies are using their powers lawfully. However, many of the requirements reflect historical concerns about corruption and the misuse of covert powers and do not reflect the current governance and accountability frameworks within which agencies operate."* [4]

    Does this equate to: *a view from the Government that "current governance and accountability frameworks" render record keeping requirements unnecessary today?*

    This would not be the view of the IIA. It is imperative that any expansion of existing powers be accompanied with a clear demonstration of an effective and transparent governance and accountability framework, as a basic prerequisite.

This is not intended to be an exhaustive list of potential implications but rather an interpretation of some of the reform proposals and what those proposals could mean, for further consideration by the Committee.

Data retention

Classified under Group C of the Terms of Reference the Discussion Paper proposes:

> *"tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities and privacy and cost impacts."*[5]

The data retention (**DR**) proposal has been the focus of significant reporting in the media since the release of the Discussion Paper. In fact, during the period of the Inquiry the international hacktivist group Anonymous has been reported to have laid claims to be responsible for a number of attacks on networks and websites to obtain secure data in protest of the DR proposal.

If nothing else this [act of hacking to obtain what may be considered secure data] highlights the need to ensure that any proposed reforms imposed on C/CSPs are cognisant of the level of security mechanisms required to protect such data.

Where ever there is an incentive for criminals to gain access to certain types of data then protecting and securing access to that data becomes more of a time, cost and technology burden. It is therefore important to ensure that data is not collected unnecessarily and that any proposals for retention of that data for extended periods can be justified by clearly demonstrating the necessity of that data to law enforcement activities.

---

[4] The Discussion Paper, p.26

[5] The Discussion Paper, p.10

DR is a scheme that should not require the industry to "create" data. So in simplest terms, a voice over internet protocol (**VoIP**) operator that does not produce individual call records should not have to start doing that. The term "not create" data also means that information present within network equipment for transient duration should not have to be extracted out into IT systems and then held. It's also not productive to have a scheme where the IP source/destination must be recorded for every packet, or where mobile location has to be captured for mobile customers on a regular basis.

IIA believes that it is important that this aspect of the proposed reforms be clarified before proper consideration can be given to it. This should include:

- clearly defining the type of data sets that would be required to be collected and retained for periods of up to 2 years;
- undertaking an extensive analysis of the costs, benefits and risks of such a scheme;
- justifying the collection and retention of personal data by demonstrating the necessity of that data to law enforcement activities;
- quantifying and justifying the expense to C/CSPs of data collection and storage by demonstrating the utility of the data retained to law enforcement;
- specifying the manner in which data is to be stored and recovered [encryption and decryption], including the methods and location of storage;
- assuring Australians that data retained under any such scheme will be subject to appropriate accountability and monitoring mechanisms, and will be stored securely with recommended, tested and approved methodologies; and
- consulting further with a range of affected stakeholders.

Another key issue is that service supply in the internet environment is disaggregated – there are many over the top (**OTT**) services ranging from things like Hotmail, Gmail, instant messaging, etc. to social networking such as Facebook, to Cloud storage and application hosting. If those services are hosted outside of Australia, then data retention obligations have little to no effect. As such, onerous obligations on Australian based suppliers could make it difficult for them to compete on a level playing field with these OTT or international competitors, while also taking into consideration the proposals to extend the regulatory regime to ancillary service providers.

Additionally, it is worth noting that no supporting statistics have been provided that indicate a systemic failure by law enforcement agencies to obtain relevant data from C/CSPs due to the C/CSP not having retained or collected the types of data that a law enforcement agency may require.

With regards to additional cost burdens being imposed on C/CSPs to comply, it is difficult to quantify with any degree of accuracy what those costs may be until more precise detail has been provided about the type, location and methodology that data would be required to be collected and retained under the reform proposals.

Network security and resilience

Under the Terms of Reference, the Government has proposed a regulatory approach to address national security risks relating to telecommunications infrastructure, achieved by making amendments to legislation, such as the Telco Act, such that C/CSPs protect their networks from unauthorised interference with the following elements:[6]

1. *an industry wide obligation on all C/CSPs to protect their infrastructure and the information held on it or passing across it from unauthorised interference to support the confidentiality, integrity and availability of Australia's national telecommunications infrastructure;*

2. *a requirement for C/CSPs to provide Government, when requested, with information to assist in the assessment of national security risks to telecommunications infrastructure; and*

3. *powers of direction and a penalty regime to encourage compliance.*

The Government justifies the need for such reforms as follows:[7]

> "*Australia's national security, economic prosperity and social wellbeing is increasingly reliant on the Internet and other information and communications technologies (ICT). Underpinning our use of these technologies is our telecommunications infrastructure. However, there are very real challenges to ensuring its security in the face of criminal and strategic threats."*
>
> […]
>
> *"Failure to effectively manage national security risks therefore has implications beyond individual C/CSPs; it is a negative externality affecting government, business and individual Australians."*

and in the following context:[8]

> *"While advances in technology and communications have resulted in unquestionable benefits to society and the economy, they have also introduced significant vulnerabilities, including the ability to disrupt, destroy, degrade or alter the functioning of our critical telecommunications infrastructure and the information held on it. A clear understanding of the current telecommunications environment is essential to identifying network vulnerabilities and managing them effectively. This includes the composition and operation of the telecommunications industry, national security risks, and the current regulatory environment."*

[6]The Discussion Paper, p.33-34

[7]The Discussion Paper, p.29

[8]The discussion Paper, p.30

However, IIA is not aware of any examples or statistics relating to the number or type of any breaches to the security of Australian telecommunications networks where they have been compromised by criminals or terrorists, in context of the above.

As such, IIA believes that an appropriate test of whether the network security and resilience proposals are reasonable and proportionate should apply while recognising:

- that it is in a C/CSP's self-interest to ensure the security of its network - i.e. if a telecommunications service provider's network security is frequently breached, it is likely to lose the confidence of its customers;

- the extent, if any, to which the security of a C/CSPs network infrastructure has been previously compromised and the degree and implications of any such security breach should be an acceptable measure of effective controls; and

- that C/CSPs are already under legal obligations to take reasonable steps to protect the privacy of customer information that is carried on their networks.

The Discussion Paper contemplates a compliance framework based on C/CSPs being able to demonstrate competent supervision and effective controls over their networks. While this was the preferred approach of industry during previous consultations, it was on the basis that it doesn't have the effect of introducing unnecessary and cumbersome compliance obligations on C/CSPs.

Additionally, the Discussion Paper appears to propose that the Government be given two new powers as follows:

- the power to require C/CSPs to provide information to Government on request; and

- the power to issue a binding direction to a C/CSP to take specified action to protect their network.

Similar to the issues associated with data retention, complying with such requests could, depending on the nature of the request, lead to C/CSPs incurring a significant cost burden. Therefore, IIA recommends that the power to request information or issue a binding direction should not be unfettered and should be subject to appropriate limitations, including that:

- the Government be required to have reasonable grounds to believe that the network of the C/CSP in question poses a risk to national security; and

- the information that the Government requests be strictly limited to information that is necessary to ascertain whether such a threat does in fact exist.

It appears that the only check and balance being considered as part of this proposal is the procedural requirement that the Secretary of the AGD be required to seek the concurrence of the Director General of Security and the Secretary of the Department of Broadband, Communications and the Digital Economy.

The discussion Paper states the following:[9]

> *"Under such an approach, in cases where engagement with C/CSPs proves to be ineffective, or a blatant disregard of security information jeopardises the Government's confidence in the security and integrity of Australia's telecommunications infrastructure, powers of direction could provide a proportionate means to achieve compliance. To safeguard such a power, it could require the Secretary of the Attorney General's Department, to seek the concurrence of the Director General of Security and the Secretary of the Department of Broadband, Communications and the Digital Economy, before directing a C/CSP to alter its business practices or undertake other actions considered necessary to protect national security interests. This would generally follow a period of more direct and intensive engagement with the C/CSP concerned."*

The Discussion Paper continues to state that:

> *"Directions could involve targeted mitigation or remediation of security risks, including modifications to infrastructure, audit, and ongoing monitoring, with costs to be borne by the relevant C/CSP. Grounds for directing mitigation or alternative actions would ultimately be determined by security agencies, based on an assessment of risk following their engagement with a C/CSP. The powers of direction would serve as a means to support the existing powers in the Telecommunications Act relating to national interest matters."*

IIA does not believe that the existence of such a wide ranging power is justified without just cause and should be strictly limited to where there is a real, immediate or significant threat to national security. Given that under such a direction the costs are to be borne by the relevant C/CSP, in order to ensure proportionality, there should be an obligation for the authorising officer, before providing any directions, to consider the least cost alternative to the C/CSP in mitigating any identified or potential threat.

In circumstances where no immediate threat to network infrastructure security exists, within a predefined period, IIA believes that any binding power of direction should be subject to a right where a C/CSP can seek an independent review of the decision - i.e. there should be some form of appeal process to a Court or administrative tribunal.

Further consideration should also be given to the role of self-regulation by the industry rather than amending legislation where it may not be necessary to do so. It should be recognised by the Government and considered by the Committee as part of the Inquiry that a significant amount of expertise exists within the industry and this should be utilised wherever possible.

There are numerous examples of industry self-regulation where codes have been developed to address infrastructure, internet and on-line security issues, such as the iCode[10] developed

---

[9]The Discussion Paper, p.37

[10]A voluntary code of practiceimplemented for Australian (ISPs) to improve cyber security for consumers connected across their networks. More information on the iCode can be found at: http://iia.net.au/codes-of-practice/icode-iias-esecurity-code.htm

in consultation with Australian Internet Service Providers (**ISPs**). Other industry associations such as the Communications Alliance, Australian Mobile Telecommunications Association and the Internet Society of Australia, have all contributed to a very successful and robust self-regulated industry with significant support and ongoing contribution from the sector.

As such, the potential success of self-regulation by the industry that could also achieve the desired outcomes of the Government's network security and resilience proposals should be seriously considered by the Committee as part of the Inquiry.

Considerations

IIA believes that in reviewing the potential reforms of national security legislation the Government should ensure that there is sufficient justification for any changes proposed accompanied by an acceptable level of checks and balances for any associated obligations imposed on the industry.

The following is a list of some principles that the IIA believes should be considered as part of the Government's proposals and the Committee's Inquiry into any potential reforms of national security legislation.

Statement of Principles

1. There is equity between the requirements of the Government, law enforcement agencies, C/CSPs and the privacy of individuals.

2. There is not an unreasonable expectation placed on the telecommunications industry to implement an unnecessary or costly security, reporting and compliance regime.

3. The privacy and rights of individuals are protected to the extent that society rightly demands.

4. The Government should not have an unfettered power to require C/CSPs to provide information about their networks without appropriate checks and balances.

5. The Government should not have an unfettered power to issue a binding direction to a C/CSP to take specified action to protect their network without appropriate checks and balances.

6. It be recognised that C/CSPs are not State agentsand a clear demarcation should be maintained between C/CSPs providing interception and access to law enforcement agencies and C/CSPs doing more than this.

7. Any newly introduced obligations, such as interception and data retention on C/CSPs or extending the obligations to ancillary service providers not currently covered by legislation, should not disadvantage Australian based providers of such services as compared to any overseas competitors operating in Australian markets.

8. Should the obligation to provide interception capability apply uniformly to all C/CSPs, rather than be based on service type, there should be flexibility as regards the

manner in which a particular C/CSP complies with the obligation based on the size, resources and capabilities of the C/CSP.

9. Consideration of any access and interception reforms should also include giving consideration to clarifying the scope of section 313 of the Telco Act. The scope of the obligation under section 313 of the Telco Act to '*give such help as is reasonably necessary*' is vague and creates uncertainty in its interpretation and effect.

10. Clear security and governance mechanisms should accompany any simplification mechanisms for the sharing of information between agencies.

11. Only where appropriate and clearly justified, legislative duplication that does not serve any useful purpose should be repealed.

12. Self-compliance should be encouraged where ever possible rather that introducing potential criminal sanctions for a failure by a C/CSP to assist a law enforcement agency.

13. Introducing or imposing specific industry timeframes for response should only be contemplated where there is evidence of industry tardiness being a cause of delay or problem for law enforcement agencies.

14. Further clarity should be provided on specific data retention requirements to fully understand the implications of such requirements, allocation of costs to comply and alignment with the National Privacy Principles under the *Privacy Act 1988.*

15. Further consultation with key stakeholders be undertaken by the Government based on any recommendations from the Inquiry to ensure that:

    a. appropriate safeguards for protecting the human rights and privacy of individuals are proportionate to any threat to national security and the security of the Australian private sector; and

    b. any additional obligations imposed upon the telecommunications industry are deemed necessary and reasonable whilst minimising cost and impact on business operations in the telecommunications sector and the potential flow on effects to consumers, the economy and international competitiveness.

Conclusion

While the IIA supports the overarching requirement to protect Australia and respond to threats from all forms of terrorism, serious and organised crime and cyber-crime, it does not believe that the Discussion Paper provides sufficient detail to justify:

- a realignment of the current balance between the requirements of law enforcement agencies and the privacy of individuals;

- the imposition of significant additional regulation and costs on C/CSPs;

- the implementation of tailored data retention periods for up to 2 years for parts of a data set; and

- unfettered powers to issue a binding direction to a C/CSP to take specified action to protect their network or require a C/CSP to provide information to Government on request with any costs to be borne by the C/CSP.

A common theme that has become evident from IIA members is an insufficient degree of transparency and specific details being available on the Government's package of national security ideas and the legislative reform proposals, both through previous consultations and in the Discussion Paper, to enable an informed response to the effectiveness and implications of the proposals.

IIA would encourage the Government to continuing working closely and transparently with affected stakeholders once the Committee has completed the Inquiry to ensure that any recommendations from the Inquiry can be further assessed, before looking to implement any proposed legislative change.

The interests of Australia's ongoing security against emerging and evolving threats is best served by working as closely, collaboratively and transparently as possible with the telecommunications sector, law enforcement agencies and the Australian community.

The IIA would be happy to provide the Committee with further information in relation to the matters canvassed in this submission and once again appreciate the opportunity to provide our views.

Peter Lee

Chief Executive Officer

Internet Industry Association