Submission No 108

Inquiry into potential reforms of National Security Legislation

Organisation: iinet

Submission to the Parliamentary Joint Committee on Intelligence and Security

Inquiry into potential reforms of national security legislation

INTRODUCTION

The Parliamentary Joint Committee on Intelligence and Security (**the Committee**) has been requested to inquire into a package of reform proposals of the following legislation:

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

The Committee has invited interested persons and organisations to address the terms of reference of the inquiry[1] (**Terms of Reference**). The Attorney General's Department has released a discussion paper to accompany the Terms of Reference[2] (**the Discussion Paper**).

iiNet is a carriage service provider and carrier[3]. iiNet is Australia's second largest DSL Internet Service Provider. iiNet employs more than 2000 staff across four countries and supports over 1.7 million broadband, telephony and Internet Protocol TV services nationwide. Many of the proposals that the Committee is considering are directly relevant to iiNet. However, iiNet believes that the proposed reforms have the potential to have a significant impact not only on carriers and carriage service providers (**C/CSPs**) but also on the privacy of individuals. Accordingly, iiNet believes that it is appropriate that the proposed reforms be subject to broad scrutiny and feedback rather than subject only to targeted confidential consultation with C/CSPs. Accordingly, iiNet welcomes the Committee's inquiry and the opportunity to provide a public submission to the Committee.

SCOPE OF THIS SUBMISSION

According to the Terms of Reference, the proposed reforms are stated to have the following three elements and objectives:

1. modernising lawful access to communications and associated communications data (for ease of expression the reform proposals that

---

[1] The terms of reference of the Committee's Inquiry are set out in a document entitled: *Terms of Reference - Inquiry into potential reforms of National Security Legislation* - available at: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/tor.htm

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

[3] The relevant carrier licence is held by Chime Communications Pty Ltd which is a subsidiary of iiNet Limited.

relate to this objective will be referred to as **the Interception and Access Reform Proposals**)[4];

2. mitigating the risks posed to Australia's communications networks by certain foreign technology and service suppliers (for ease of expression the reform proposals that relate to this objective will be referred to as **the Network Security Reform Proposals**)[5], and

3. enhancing the operational capacity of Australian intelligence community agencies (for ease of expression the reform proposals that relate to this objective will be referred to as **the Intelligence Agencies Reform Proposals**)[6].

iiNet is a telecommunications service provider and network owner. Therefore, the Interception and Access Reform Proposals and the Network Security Reform Proposals are both directly relevant to iiNet. However, the Intelligence Agencies Reform Proposals are not directly relevant to iiNet. In light of this, iiNet believes that it is appropriate for iiNet to limit its submission to addressing only the Interception and Access Reform Proposals and the Network Security Reform Proposals. For ease of expression the Intelligence Agencies Reform Proposals and the Network Security Reform Proposals will be referred to collectively as the **Reform Proposals**.

iiNet's consideration of the issues arising involves the adoption of a five step reasoning process as follows:

- Step 1 - identify the specific Reform Proposals.

- Step 2 - identify the justifications for the Reform Proposals (i.e. what are the reasons given as to why the Reform Proposals are necessary).

- Step 3 - identify whether there is any evidence which supports the justifications for the Reform Proposals. iiNet submits that this step is important because if there is no evidence to support a justification for a particular Reform Proposal, then it may be appropriate not to consider that Reform Proposal further until such evidence has been provided.

- Step 4 - identify the relevant criteria to be considered when assessing whether the Reform Proposals should be accepted (i.e. identify the interests to be weighed and the principles to be applied).

- Step 5 - form a view on each Reform Proposal on the basis of Steps 1 to 4 above.

---

[4] These proposed reforms are discussed in chapter 2 of the Discussion Paper.

[5] These proposed reforms are discussed in chapter 3 of the Discussion Paper.

[6] These proposed reforms are discussed in chapter 4 of the Discussion Paper.

This reasoning process gives rise to the following five questions:

1. What are the Reform Proposals?

2. What are the justifications for the Reform Proposals?

3. What is the evidence that supports the justifications for the Reform Proposals?

4. What criteria should be applied in order to decide whether the Reform Proposals should be accepted?

5. What conclusions should be made about the Reform Proposals?

This submission sets out iiNet's answers to each of these questions in respect of:

- those Interception and Access Reform Proposals that are directly relevant to iiNet; and

- the Network Security Reform Proposals.

For ease of expression a reference in this submission to a 'law enforcement agency' includes a reference to 'Agencies' and 'the Organisation' as defined in the TIA Act, as well as any other organisation or body that is entitled to require a C/CSP to provide it with assistance in relation to law enforcement or national security.

SUMMARY OF CONCLUSIONS

iiNet acknowledges the obvious public interest in law enforcement agencies having effective interception and access capabilities and in telecommunications networks being kept secure from threats posed by criminals and terrorists. However, there is also an obvious need to balance the following against the needs of law enforcement agencies:

- the human rights and privacy of individuals; and

- the cost and impact of the reforms on the telecommunications sector.

In iiNet's view, the Discussion Paper does not make a sufficient case to justify either of the following:

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

- the imposition of significant additional costs on C/CSPs.

Specifically, iiNet submits that:

1. The Reform Proposals should be rejected insofar as they require the following:

    a. C/CSPs being required to collect or retain information that they would not otherwise collect or retain.

    b. C/CSPs' interception and access obligations being subject to specified response timeframes.

    c. C/CSPs being potentially liable for an offence of failure to assist in the decryption of communications.

    d. The Government having an unfettered power to require C/CSPs to provide information to Government about their networks. Any such power 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 limited to information that is necessary to ascertain whether such a threat does in fact exist.

    e. The Government having an unfettered power to issue a binding direction to a C/CSP to take specified action to protect their network. Any such power of direction should be strictly limited to where there is a real, immediate and significant threat to security if the specified action in the direction is not taken. Furthermore, in order to ensure proportionality, there should be an obligation for the decision maker to consider the least cost alternative to the C/CSP in mitigating a particular threat. In circumstances where there is no immediate threat to security, any binding power of direction should be subject to a right for the C/CSP to seek independent review of the decision - i.e. there should be some form of appeal to a Court or administrative tribunal.

2. iiNet's grounds for rejecting the Reform Proposals referred to in point 1 above are that:

    a. there is insufficient evidence to support the justifications on which they are based; and/or

    b. they fail to achieve an appropriate balance between:

        i. the human rights and privacy of individuals;

        ii. the cost and impact of the reforms on the telecommunications sector; and

iii. the needs of law enforcement agencies.

3. Further detail on the following Reform Proposals is required before any conclusion can be made on their merits:

   a. The removal of legislative duplication.

   b. Aligning industry interception assistance with industry regulatory policy.

   c. Clarifying the AMCA's regulatory and enforcement role.

   d. Expanding the basis of interception activities.

   e. Implementing detailed requirements for industry interception obligations.

4. Consideration needs to be given to the issue of whether imposing interception obligations on ancillary service providers could disadvantage Australian based providers of such services (who will be subject to the cost of compliance) as compared to their overseas competitors (who will likely be beyond the reach of any enforcement powers that would result from a failure to comply with the interception obligations).

5. The obligation to provide interception capability should apply uniformly to all C/CSPs. However, there should be flexibility as regards the manner in which a particular C/CSP complies with the obligation to provide interception capability, and the size and resources of the C/CSP should be a relevant consideration in the assessment of that C/CSP's interception capability plan.

6. It is important that it be recognised that C/CSPs are not agents of the State, and a clear demarcation should be maintained between CSPs providing interception and access to law enforcement agencies and C/CSPs doing more than this.

7. 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 to '*give such help as is reasonably necessary*' is vague and uncertain.

THE INTERCEPTION AND ACCESS REFORM PROPOSALS

What are the Interception and Access Reform Proposals?

The Interception and Access Reform Proposals are[7]:

Matters the Government wishes to progress

1. *Examining the legislation's privacy protection objective, the proportionality test for issuing warrants, mandatory record keeping standards, and oversight arrangements by the Commonwealth and State Ombudsmen.*

2. *Reducing the number of agencies eligible to access communications information.*

3. *Standardising warrant tests and thresholds.*

4. *Simplifying the information sharing provisions that allow agencies to cooperate.*

5. *Removing legislative duplication.*

6. *Aligning industry interception assistance with industry regulatory policy.*

7. *Clarifying the AMCA's regulatory and enforcement role.*

Matters the Government is considering

8. *Creating a single warrant with multiple TI powers.*

9. *Implementing detailed requirements for industry interception obligations.*

10. *Extending the regulatory regime to ancillary service providers not currently covered by the legislation.*

11. *Implementing a three tiered industry participation model.*

Matters on which the Government expressly seeks the views of the Committee

12. *Expanding the basis of interception activities.*

13. *Establishing an offence for failure to assist in the decryption of communications.*

14. *Instituting industry response timelines.*

---

[7] As set out in the Discussion Paper at p. 13.

15. *Applying 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.*

What are the justifications for the Interception and Access Reform Proposals?

iiNet notes that the following comments in the Discussion Paper are relevant to ascertain the justifications for the Interception and Access Reform Proposals[8]:

> *Substantial and rapid changes in communications technology and the business environment are rapidly eroding agencies' ability to intercept.*[9]
>
> […]
>
> *As carriers' business models move to customer billing based on data volumes rather than communications events (for example number of phone calls made), the need to retain transactional data is diminishing. Some carriers have already ceased retaining such data for their business purposes and it is no longer available to agencies for their investigations*[10].
>
> […]
>
> *The use of encryption and propriety data formats and typically large data volumes, makes reconstructing communications into an intelligible form difficult for agencies.*[11]
>
> […]
>
> *The pace of change in the last decade has meant the Act has required frequent amendment resulting in duplication and complexity that makes the Act difficult to navigate and which creates the risk that the law will not be applied as Parliament intended.*

From these comments it appears reasonable to conclude that the justification for the Interception and Access Reform Proposals is that they are required to address the following problems:

- law enforcement agencies are having difficulty intercepting and accessing the content of communications due to technological change;
- the retention of telecommunications data and subscriber information retained by C/CSPs is decreasing, and this is causing problems for law enforcement agencies; and
- the TIA Act is complex and difficult to navigate,

(referred to collectively as the **Interception and Access Problems**).

[8] Discussion Paper at p.17.

[9] Discussion paper at p.23.

[10] Discussion Paper at p.21.

[11] Discussion Paper at p.22.

What is the evidence that supports the justifications for the Interception and Access Reform Proposals?

iiNet notes that there is no 'hard evidence' referred to in the Discussion Paper to support the assertion that changes in technology and the practices of C/CSPs are causing serious problems for law enforcement agencies. For example, no statistics have been provided on the number of attempts made by law enforcement agencies to obtain data from C/CSPs that were unsuccessful due to the C/CSP not having retained or collected the data that the law enforcement agency required. On the contrary, the Discussion Paper refers to evidence which suggests that interception powers continue to be used effectively[12].

What criteria should be applied in order to decide whether the Interception and Access Reform Proposals should be accepted?

iiNet submits that, having regard to the relevant information in the Terms of Reference and the Discussion Paper, the Interception and Access Reform Proposals should not be accepted unless they achieve an appropriate balance between the following:

- the human rights and privacy of individuals[13];
- the cost and impact of the reforms on the telecommunications sector[14]; and
- the needs of law enforcement agencies[15].

What conclusions should be made relating to the Interception and Access Reform Proposals?

Each of the Interception and Access Reform Proposals that are directly relevant to iiNet will be considered in turn[16].

---

[12] At page 14 of the Discussion Paper reference is made to the TIA Act Report for the year ending 30 June 2011 which states that in 2010/11 there were 3168 prosecutions based on lawfully intercepted material. At page 17 of the Discussion Paper reference is made to a major money laundering investigation where information obtained through interception activities helped the Australian Federal Police arrest 35 offenders and to seize 421 kilograms of drugs and over $8,000,000 in cash.

[13] As per paragraph 3(a) of the Terms of Reference.

[14] As per paragraph 3(b) of the Terms of Reference.

[15] As per paragraph 3(c) of the Terms of Reference.

[16] This submission does not address the following Interception and Access Reform proposals which are not directly relevant to iiNet: *reducing the number of agencies eligible to access communications information; standardising warrant tests and thresholds; and simplifying the information sharing provisions that allow agencies to cooperate*.

Examining the legislation's privacy protection objective, the proportionality test for issuing warrants, mandatory record keeping standards, and oversight arrangements by the Commonwealth and State Ombudsmen.

In iiNet's view, the Discussion Paper does not make a sufficient case to justify either of the following:

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

- the imposition of significant additional costs on C/CSPs.

Therefore, iiNet believes that any re-examination of the TIA Act should not lead to either of these outcomes.

Removing legislative duplication

In principle, legislative duplication does not serve any useful purpose and so should be avoided. However, it is difficult for iiNet to comment any further without seeing the detail of the proposed reform.

Aligning industry interception assistance with industry regulatory policy

This proposed reform appears to iiNet to be capable of being very broad. It is not expressly discussed in any detail in the Discussion Paper. Without detail of what this reform would involve, it is difficult for iiNet to provide any meaningful comment.

Clarifying the AMCA's regulatory and enforcement role

It is unclear what precise reforms are contemplated. Therefore, it is difficult for iiNet to provide any meaningful comment on this proposed reform.

Creating a single warrant with multiple TI powers

The Discussion Paper does not specify what the particular 'TI powers' will be (i.e. whether a consolidation of existing powers is intended or the addition of new powers). iiNet believes that it is important that it be recognised that C/CSPs are not State agents, and a clear demarcation should be maintained between CSPs providing access and C/CSPs doing more than providing access. Furthermore, C/CSPs should not be required to make any judgement calls as regards what particular information is required for a C/CSP to comply with a warrant. Therefore, warrants should contain clear and specific terms.

Implementing detailed requirements for industry interception obligations

This proposed reform appears to iiNet to be capable of being very broad. It is not expressly discussed in any detail in the Discussion Paper. Without detail of

what this reform would involve, it is difficult for iiNet to provide any meaningful comment, except to say that there should be thorough consultation with industry on these detailed requirements. iiNet believes that consideration of any such reform should include giving consideration to clarifying the scope of section 313 of the Telco Act. The scope of the obligation to '*give such help as is reasonably necessary*' is vague and uncertain.

Extending the regulatory regime to ancillary service providers not currently covered by the legislation

While in principle such an extension may seem appropriate, iiNet believes that consideration needs to be given to the issue of whether imposing interception obligations on ancillary service providers could disadvantage Australian based providers of such services (who will be subject to the cost of compliance) as compared to their overseas competitors (who will likely be beyond the reach of any enforcement powers that would result from a failure to comply with the interception obligations).

Implementing a three tiered industry participation model

iiNet agrees with the comments in the Discussion Paper that a tired model would more accurately reflect industry practice[17]. However, iiNet believes that it is appropriate to distinguish between:

- the legal obligation to provide interception capability; and
- the manner in which that obligation is complied with by a particular C/CSP.

iiNet believes that the obligation to provide interception capability should apply uniformly to all C/CSPs. However, iiNet believes that there should be flexibility as regards the manner in which a particular C/CSP complies with the obligation to provide interception capability, and the size and resources of the C/CSP should be a relevant consideration in the assessment of that C/CSP's interception capability plan.

Expanding the basis of interception activities

It is unclear to iiNet what this proposed reform contemplates. Therefore, iiNet is unable to comment.

Establishing an offence for failure to assist in the decryption of communications

The introduction of criminal sanctions for a failure by a carriage service provider to assist a law enforcement agency would appear to be a major shift

[17] Discussion Paper at p.28.

away from the current regime which relies on service provider rules[18]. iiNet believes that the Interception and Access Problems do not require such a shift. Therefore, iiNet does not support this proposed reform.

Instituting industry response timelines

iiNet submits that imposing specific industry timeframes is unnecessary. iiNet notes that there is no suggestion in the Discussion Paper that industry tardiness is in any way a cause of any of problems for law enforcement agencies.

Applying 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

iiNet submits that consideration of this proposed reform should start with the National Privacy Principles (**NPPs**) under the *Privacy Act 1988*. NPP 1.1 provides that an organisation must not collect personal information unless the information is necessary for one or more of its functions or activities. Therefore, if collection of telecommunications data[19] or subscriber information[20] is necessary for one or more of the functions or activities of a C/CSP (for example providing a telecommunications service), there will be no issue with NPP 1.1.

However, if a C/CSP decided off its own bat (i.e. without any legal obligation to do so) to collect and retain data that is personal information solely because that data had the potential to be of use to law enforcement agencies, that C/CSP would likely be in breach of NPP 1.1. Therefore, the effect of the proposed reform is to effectively provide a statutory exemption to NPP 1.1 and allow personal information to be collected and retained where the sole reason for the collection and retention of that personal information is the fact that it *may* be of use to law enforcement agencies. This clearly has major implications for privacy. These implications for privacy are magnified if the reform would include the routine collection and retention of the content of communications rather than just telecommunications data and subscriber information. iiNet believes that it is crucial that this aspect of the proposed reform be clarified before proper consideration can be given to it. iiNet notes that in its report, the Senate Standing Committee on Environment,

---

[18] Under section 101 of the Telco Act, service providers are required to comply with the service provider rules set out in Schedule 2 of the Telco Act. Clause 1 of Schedule 2 of the Telco Act requires compliance with Chapter 5 of the TIA Act. If a service provider does not comply with the service provider rules, it will be liable for pecuniary penalties under Part 31 of the Telco Act.

[19] The term 'telecommunications data' refers to information about a communication that is not the content of the communication, for example an IP address or telephone number.

[20] The term 'subscriber information' refers to information about a subscriber to a telecommunications service, for example their name, address or date of birth

Communications and the Arts recommended that before pursuing any mandatory data retention proposal, the Government should[21]:

- undertake an extensive analysis of the costs, benefits and risks of such a scheme;
- justify the collection and retention of personal data by demonstrating the necessity of that data to law enforcement activities;
- quantify and justify the expense to Internet Service Providers of data collection and storage by demonstrating the utility of the data retained to law enforcement;
- assure Australians that data retained under any such scheme will be subject to appropriate accountability and monitoring mechanisms, and will be stored securely; and
- consult with a range of stakeholders.

iiNet notes that no reference has been made to this recommendation in the Discussion Paper. With regard to the second point in the recommendation, as noted above, no statistics have been provided on the number of attempts made by law enforcement agencies to obtain data from C/CSPs that were unsuccessful due to the C/CSP not having retained or collected the data that the law enforcement agency required.

As regards the cost of complying with such a scheme, iiNet believes that the costs would be significant. However, until more precise detail has been provided about what particular data will be required to be retained, it is not possible to provide any estimate of what those costs might be.

THE NETWORK SECURITY REFORM PROPOSALS

What are the Network Security Reform Proposals?

The Reform Proposals are as follows[22]:

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*

[21] Environment and Communications References Committee, The adequacy of protections for the privacy of Australians online, April 2011 - recommendation 9.

[22] Discussion Paper at pp 34/35.

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

According to the Discussion Paper the compliance framework that would result from these reforms would work as follows[23]:

- Government would provide guidance to assist industry to understand and meet its obligation, this would include the dissemination of information on specific security threats to affected C/CSPs on an as needs basis.

- Where requested to do so by Government, C/CSPs would be required to demonstrate compliance to Government.

- Government's preferred approach to dealing with potential issues of concern would be to engage with the relevant C/CSPs to establish whether national security concerns can be co-operatively addressed. However, there would be a graduated suite of enforcement measures (including the power of direction).

- The grounds for issuing a direction would ultimately be determined by security agencies, based on an assessment of risk following their engagement with a C/CSP. A safeguard could include requiring 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.

- The costs of complying with a direction would be borne by the relevant C/CSP.

What are the justifications for the Network Security Reform Proposals?

iiNet notes that the justifications given in the Discussion Paper for these reforms are[24]:

> *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.*

[23] See sections 3.2 and 3.3 of the Discussion Paper.

[24] Discussion Paper at p.29.

What is the evidence that supports the justifications for the Network Security Reform Proposals?

iiNet notes that the Discussion Paper does not provide any examples or statistics relating to the number of times that the security of Australian telecommunications networks have been compromised by criminals or terrorists.

What criteria should be applied in order to decide whether the Network Security Reform Proposals should be accepted?

iiNet submits that the key principles in determining whether the reforms are appropriate are the principles of reasonableness and proportionality. This is expressed in the Terms of Reference as follows (emphasis added):

> *3) The Committee should have regard to whether the proposed responses:*
> *(a) contain appropriate safeguards for protecting the human rights and privacy of individuals and* ***are proportionate to any threat to national security and the security of the Australian private sector***
>
> *(b)* ***apply reasonable obligations upon the telecommunications industry whilst at the same time minimising cost and impact on business operations in the telecommunications sector and the potential for follow on effects to consumers, the economy and international competition***

What conclusions should be made relating to the Network Security Reform Proposals?

iiNet submits that the starting point for consideration of whether the Network Security Reform Proposals are reasonable and proportionate is an acknowledgement 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 customers; and

- C/CSP's are already under legal obligations to take reasonable steps to protect the information that is carried on their networks[25],

  (for ease of expression, these facts will be referred to as the **C/CSP Motivations**).

On the basis of the information in the Discussion Paper, it appears that it is proposed that the Government be given two new powers as follows:

---

[25] By virtue of NPP 4.1 which requires an organisation to take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

- 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.

iiNet will consider each of these proposed powers in turn.

The power to require C/CSPs to provide information to Government

Although at first sight this power may appear to be fairly innocuous, in practice it has the potential to impose a disproportionate cost burden on C/CSPs. Therefore, iiNet believes that the power to request information should not be unfettered but 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 must be limited to information that is necessary to ascertain whether such a threat does in fact exist.

The power to issue a binding direction

iiNet submits that the Government should not have an unfettered power to issue a binding direction to require a C/CSP to take specified action regardless of the cost of that action. iiNet believes that such a power has the potential to result in disproportionate outcomes unless the scope of the power is limited to achieve proportionate outcomes and there are appropriate checks and balances in place that govern its use.

It appears that the only check and balance being considered is the procedural requirement that the Secretary of the Attorney General's Department 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. iiNet believes that given the existence of the C/CSP Motivations, the existence of such a wide ranging power is not justified. Rather, any such power of direction should be strictly limited to where there is a real, immediate and significant threat to security if the specified action in the direction is not taken. Furthermore, in order to ensure proportionality, there should be an obligation for the decision maker to consider the least cost alternative to the C/CSP in mitigating a particular threat.

In circumstances where there is no immediate threat to security, iiNet believes that any binding power of direction should be subject to a right for the C/CSP to seek independent review of the decision - i.e. there should be some form of appeal to a Court or administrative tribunal.

iiNet
20 August 2012