DOCUMENT 6

In Confidence

Interception and Network Security: Options

To	Hon Amy Adams	**Priority**	Medium
Date	21 September 2012	**Deadline**	26 September

Purpose

[Out of scope]

e. Appendix 5: extracts of the deem-in and decryption proposals from the technical consultation document.

Recommendation

[Out of scope]

Kirstie Hewlett
Director
Energy and Communications Branch

Hon Amy Adams
Minister for Communications and Information Technology

[Out of scope]

[Out of scope]

[Out of scope]

Distorts the market: the drafting of the TICA places "network operators" at a competitive disadvantage by requiring not only their networks but all of their services to be intercept capable, when identical services may be offered by a company which is not a network operator and therefore does not have an obligation to invest.

[Withheld under s6(a) and s6(c)]

[Out of scope]

Issues for Government –

[Out of scope]

Insufficient flexibility for changing telecommunications markets: as the telecommunications industry continues to change, the Act does not have sufficient flexibility to keep pace with new practices/services/players in the industry.

a. Help with decryption is listed as part of the duty to have interception capability, because when the Act was passed, generally only network operators did encryption. Now it happens at several levels by default, but only one level has an express obligation to help decrypt.

b. The Act does not have the ability to extend to emerging telecommunications services if they become significant in future. Without extending the scope of the legislation, when that is required, **[Withheld under s6(a) and s6(c)]** , and there is more risk that a wide range of telecommunications services are not interception capable.

[Out of scope]

In Confidence

[Appendix two paragraphs 1 to 28 out of scope]

Option	Benefits	Costs/Risks
[Out of scope]	[Out of scope]	[Out of scope]

Option	Benefits	Costs/Risks
[Out of scope]	[Out of scope]	[Out of scope]
[Out of scope]	[Out of scope]	[Out of scope]

Option	Benefits	Costs/Risks
[Out of scope]	[Out of scope]	[Out of scope]
[Out of scope]	[Out of scope]	[Out of scope]

Option	Benefits	Costs/Risks
1. Include an explicit capability obligation on application providers	• Bringing application providers into the regime recognises that it will be simpler, and more effective, for surveillance agencies to intercept data at this layer. Its inclusion also resolves competitive distortion in the market immediately, and makes regime more future proof. • However, we do note that: 1. in the absence of this explicit obligation, application providers are already caught by the duty to assist (which applies to all service providers); and 2. an explicit obligation is only one, of a number, of steps that would need to be taken **[Withheld under s6(a) and s6(c)]**	• The proposal is simply to extend the interception capability obligation to application providers, and it does not extend the circumstances in which the surveillance agencies are legally permitted to intercept.[7] However, this distinction is hard to explain, and the proposal may instead be cast as increasing interception and surveillance across a broader range of services.
2. Remove Application providers and replace with a deem-in (or clarifying how the duty to assist applies, and what it entails)	• The benefit of this option is that it still retains the ability for providers, like application providers, to be brought into the regime in the future and makes the legislation more flexible and durable. It also means there will not be unreasonable competitive distortions as the range of providers and services grow over time. • It attempts to provide a deem-in process which is transparent and balances a range of factors/protections to ensure privacy interests and	**[Withheld under s6(a) and s6(c)]**

[7] The surveillance agencies already have lawful authority to intercept at the application level.

Option	Benefits	Costs/Risks
	interests of the sector are preserved. **[Withheld under s6(a), s6(c), and s9(2)(g)(i)]** • In addition, or as an alternative, we could specify that the duty to assist does apply to application providers whether or not they are based within the jurisdiction, and provide some detail as to what that assistance would entail to provide greater clarity about what assistance is expected at the application level. **[Withheld under s6(b)(i) and s9(2)(g)(i)]** It already applies to all service providers, and therefore includes application providers.	1.

Option	Benefits	Costs/Risks
3. Remove any interception obligation, deem-in provision, or clarification of the duty to assist, that might apply to application providers	**[Withheld under s9(2)(g)(i)]**	• The loss of the deem-in would mean that there is no clear process to impose interception obligations on application providers or other emerging capability gaps in future. It would also mean that the TICA is inflexible (one of the problems with the legislation today), and that a further legislative process is likely to be necessary in the near future (especially given the increasing importance of application providers). • It does not address current issues around distortion of competition in the market between different providers and services. • **[Withheld under s6(a) and s6(c)]**
4. Remove the proposal to extend the duty to assist to apply to decryption	• The current decryption proposal is simply to make clear that the duty to assist includes help with decryption (and service providers will be free to choose the manner of that assistance), and it will only apply to communications already authorised to be intercepted. **[Withheld under s9(2)(g)(i)]**	**[Withheld under s6(a) and s6(c)]**

[Appendix three (pages 17 to 20) out of scope]

[Appendix four (pages 21 to 22) out of scope]

Appendix Five: Deem-in and decryption (technical consultation paper extracts)

Deem-in

1 The telecommunications industry will continue to evolve, and it will be important for the Act to keep pace. However, any future extensions to the scope of companies required to invest in interception capability should be well-justified, and considered in a uniform, balanced way.

2 It is proposed to establish a structured "deem-in" process, which would guide decisions about imposing a capability obligation on new telecommunications providers who do not currently have any under the TICA framework. This deem-in process would expressly be limited to services or networks for which it is possible to obtain lawful authority to intercept (that is, investment in capability would not be required unless it is already possible for a New Zealand government agency to lawfully intercept on that network or service).

3 The deem-in process would take into account the same factors as for "deem-up", namely:

- the extent to which the current level of interception capability on that network or service adversely affects national security or law enforcement;
- the extent to which the cost of complying with the obligation would adversely affect the business of the company providing that network or service;
- whether compliance with obligations would unreasonably impair the provision of telecommunications services in New Zealand or the competitiveness or innovation of the New Zealand telecommunications industry; and
- In considering these factors, the Minister would be required to take into account the views of the relevant providers.

4 However, because this would bring in companies who had previously only had assistance obligations under the Act, the deem-in would be done by regulation (rather than by ministerial directive). This would ensure that the costs and benefits of imposing the capability was thoroughly explored and consulted on. Regulations would provide a phase-in period for roll-out of capability.

Clarify the scope of the duty to assist, in relation to decryption

5 Currently, the duty to have interception capability includes duty to decrypt – if the intercepting network operator applied the encryption, it must provide the intercepted data unencrypted ('in the clear') to the authorised agency.

6 However, encryption is now commonly provided on more than one layer – for example, a single communication can be encrypted at the application level, and at the retail and network levels. Therefore, even when the intercepting party decrypts in compliance with current TICA, the communication may still be encrypted or otherwise modified at other levels, in a way which makes it unintelligible without further processing.

7 Encryption can make interception more costly or less timely, and it is becoming a more ubiquitous default feature of telecommunications services.

8 All telecommunications companies have a duty to assist in section 13 of the TICA, this is broadly worded and could encompass assistance with decryption. However the scope of what could be involved with this assistance is not clearly spelt out, which has led to concerns, including that companies might be required to remove encryption which they did not apply themselves.

9 Accordingly, it is proposed to amend the duty to assist to specify expressly that it includes help with decryption, but only using means in the network operator or service provider's control, to help undo any encryption which they have applied. Providers would not be required to undo encryption applied by another party, and would have a choice of how to assist.

10 In practice this means that if presented with a valid authority relating to the encrypted communications, the telecommunications company could choose to decrypt the material themselves before handing it over, or else choose to provide the authorised agency with the means to do the decryption work itself. It is not proposed to specify which of these options must be followed, given that there will be different cost and complexity involved with either option, depending on the circumstances.

11 It should be noted that the proposal does not change existing privacy settings, because:

- the requirement to assist with decryption would only apply to communications which are already authorised to be intercepted and only if the network operator or service provider is presented with a valid authority relating to those communications.
- companies currently provide a range of assistance, including with decryption, to help fulfil valid warrants. The intention of the proposal is to put beyond doubt that this assistance can be provided in the manner of the company's choice, and only extends to encryption they themselves have applied.
- sections 6(a), 6(b) and 14 of the TICA currently impose specific requirements to maintain the privacy of, and not interfere with, telecommunications which are not authorised to be intercepted. These obligations will continue to apply to the amended requirement.[11]

12 The advantages of this proposal are that:

- there is a clear, up to date statement of the scope of the duty to assist in relation to encryption, and
- interception can continue to happen effectively and efficiently, where there is lawful authority to do so.

[11] Other legislation provides further safeguards against unlawful interception, including criminal offences, restrictions in the authorising legislation for intercepting agencies, and safeguards in the internal procedures of the agencies (including compliance checking and audit powers).