



Office of Hon Amy Adams

Member of Parliament for Selwyn

Minister for the Environment

Minister for Communications and Information Technology

Associate Minister for Canterbury Earthquake Recovery

07 AUG 2013

CITAA12-13/338

Vikram Kumar

by email: fyi-request-903-fdc56435@requests.fyi.org.nz

Dear Vikram

I refer to your Official Information Act 1982 (OIA) request dated 1 June 2013 in relation to the Telecommunications (Interception Capability and Security) Bill (the Bill), for

"all information (including but not limited to, briefing papers, meeting notes, emails and Cabinet papers) directly or indirectly related to the need for inclusion of service providers within the ambit of the Bill as well as options and analysis of the proposed obligations, rights, penalties, notifications, processes and exemptions."

As well as:

"all information (including the Ministry's views and assessments) relating to encryption and decryption of services provided by network operators, service providers and resold overseas services."

I have interpreted your request to relate to all information relating to the Bill's provisions regarding the 'deem-in' of service providers, and all information in relation to encryption and/or decryption.

I have identified ten documents that contain information within the scope of your request.

The relevant sections of the following documents are released in full:

| Paper title | Date |
|--|----------------|
| 1. A3 – Network Security and Interception B – Proposed Legislative Framework | July 2012 |
| 2. A3 – Review of Telecommunications (Interception Capability) Act 2004 – potential obligations by layer | September 2012 |
| 3. Technical Paper: Telecommunications Interception Capability and Network Security | December 2012 |

The relevant sections of the following documents are released with partial withholdings under the following sections of the OIA:

- S6(a) – release of the information would be likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand;

- S6(c) – release of the information would be likely to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial;
- S9(2)(a) – withholding of the information is necessary to protect the privacy of natural persons; and
- S9(2)(g)(i) – withholding of the information is necessary to maintain the effective conduct of public affairs through the free and frank expression of opinions by or between or to Ministers of the Crown or members of an organisation or officers and employees of any department or organisation in the course of their duty.

| Paper title | Date |
|--|----------------|
| 4. Report – Review of Telecommunications (Interception Capability) Act (TICA) | May 2012 |
| 5. Interception and Network Security | August 2012 |
| 6. Briefing – Interception and Network Security: Options | September 2012 |
| 7. Cabinet Paper – Telecommunications Industry – Paper 1: Overview of Interception Capability and Network Security Proposals | March 2013 |
| 8. Cabinet Paper – Telecommunications Industry – Paper 2: Updating Interception Capability Obligations | March 2013 |
| 9. Cabinet Paper – Telecommunications (Interception Capability and Security) Bill: Approval for Introduction | April 2013 |

The relevant sections of the following document are withheld in full under the following sections of the OIA:

- S6(a) – release of the information would be likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand;
- S6(b)(i) – release of the information would be likely to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by the Government of any other country or any agency of such a Government; and
- S6(c) – release of the information would be likely to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial.

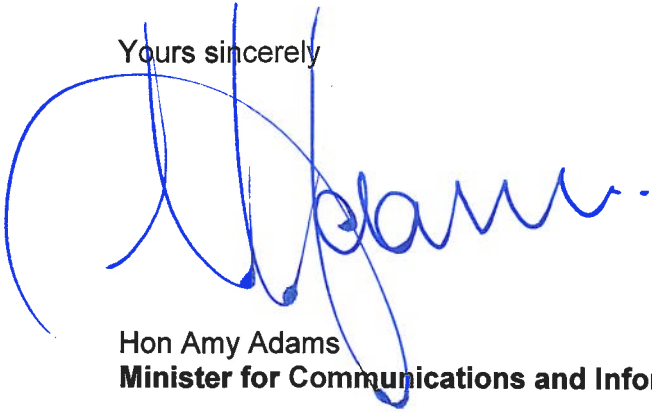
| Paper title | Date |
|--|---------------|
| Brief – NZIC Policy and Legislation Review and Telecommunications: industry Obligations and Security | December 2012 |

The Regulatory Impact Statement (RIS) relating to the Interception Capability proposals in the Bill also contains information relevant to your request. The RIS can be found on the website of the Ministry of Business, Innovation and Employment, using the following link: www.med.govt.nz/sectors-industries/technology-communication/communications/legislation-relating-to-the-telecommunications-sector.

I do not consider that the withholding of the information in these documents is outweighed by other circumstances which render it desirable, in the public interest, to make that information available.

You have the right by way of complaint under section 28(3) of the OIA to an Ombudsman, to seek an investigation and review of the release of the information referred to above.

Yours sincerely

A handwritten signature in blue ink, appearing to read 'A. Adams', with a large, sweeping circular flourish on the left side.

Hon Amy Adams
Minister for Communications and Information Technology

Network Security and Interception B – Proposed Legislative Framework

Part 1: Lawful Interception

1. Obligation to be “intercept capable” for “network operators” and some “application providers”

OUT OF SCOPE

- Deem-in and deem-up process to impose interception obligations on telecommunications providers who do not have obligations under the Act (legislation flexible over time) or to increase obligations if an operator becomes more critical for interception purposes.

OUT OF SCOPE

3. Duty to assist extended to include assistance with decryption.

OUT OF SCOPE

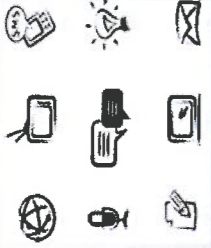
OUT OF SCOPE

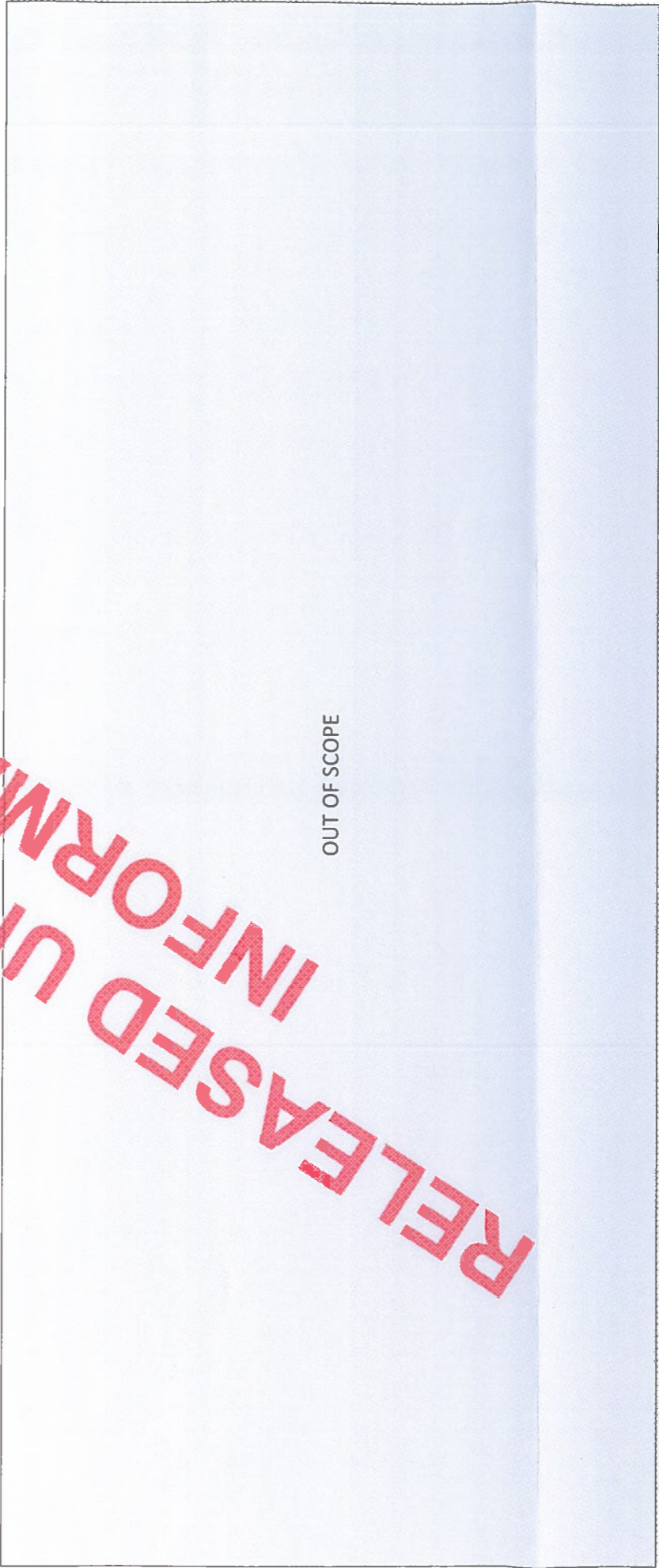
OUT OF SCOPE

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

IN CONFIDENCE

IN CONFIDENCE

| Review of Telecommunications (Interception Capability) Act 2004 – potential obligations by layer | | | |
|--|--|---|--------------|
| Applications eg. webmail, VoIP | OUT OF SCOPE | <div>Extend obligation to be interception capable: include providers who provide public telecommunications services to subscribers in New Zealand</div> <div></div> <div>+</div> | OUT OF SCOPE |
| Layer 3 – eg. RSPs, ISPs – internet and telephone services | <div>OUT OF SCOPE</div> <div>RELEASED UNDER THE OFFICIAL INFORMATION ACT</div> | | |
| Layer 2 – eg ethernet, managed bandwidth (fibre and Copper UBA) | | | |
| Layer 1 – eg. dark fibre and Un-bundled Copper Local Loop | | | |
| | | OUT OF SCOPE | OUT OF SCOPE |
| | | Express obligation to help with decryption | OUT OF SCOPE |



IN CONFIDENCE



**Ministry of Business,
Innovation & Employment**

**TECHNICAL PAPER:
TELECOMMUNICATIONS
INTERCEPTION CAPABILITY
AND
NETWORK SECURITY**

December 2012

[Introduction (pages 2 to 4) out of scope]

TABLE OF CONTENTS

[Out of scope]

| | |
|---|-----------|
| 1.5.2 ENSURING THE SCOPE OF OBLIGATIONS IS CLEAR AND PROPORTIONATE | 28 |
| <i>Clarify the nature and scope of the duty to assist.....</i> | <i>28</i> |
| <i>Ensuring obligations remain proportionate and well-justified</i> | <i>29</i> |

[Out of scope]

IN CONFIDENCE

[Out of scope]

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

**PART 1 - Review of Telecommunications (Interception Capability)
Act 2004**

[Paragraphs 1 – 29 out of scope]

1.3 Issues with the current interception scheme

Developments in the telecommunications industry

30. Industry and government stakeholders have identified a range of issues and concerns with the current interception scheme. Some of these problems arise from the broad wording of the TICA, or the way the interception scheme has been implemented and supported by government to date.

[Out of scope]

- d. increasingly common encryption of telecommunications services at multiple layers (eg. no longer just by the network operator, but also at the level of individual emails or conversations); and

[Out of scope]

Issues with the TICA

[Out of scope]

[Out of scope]

The key concern for Government

[Out of scope]

new technologies are emerging rapidly, but there is no capacity to quickly adapt obligations to suit market evolution.

[Out of scope]

[Out of scope]

Status quo

[Paragraphs 37 – 40 out of scope]

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

[Paragraphs 37 – 40 out of scope]

2. In addition, the Act is unclear as to the scope of the duty to assist, in relation to help with decryption.

Proposal

[Out of scope]

42. This chapter therefore sets out proposals to:

[Out of scope]

- ensure the scope of obligations is clear and well justified (by clarifying the scope of obligations in relation to decryption, and setting out due process and considerations to be taken into account, if obligations were proposed for new categories of provider in future (see section 1.5.2));

[Out of scope]

[Out of scope]

[Paragraphs 44-87 out of scope]

[Out of scope]

Clarify the nature and scope of the duty to assist

88. Only network operators are obliged to pro-actively invest in interception capability on their networks. However, section 13 of the TICA requires all service providers to assist with an interception operation, when presented with a warrant or other lawful authority to intercept. This assistance is specified as including (a) making technical staff available, as well as (b) all other reasonable steps necessary to give effect to the interception.
89. This current obligation is very broadly worded. It is proposed that this section be amended to specify in more detail what is reasonably necessary to give effect to an interception. These specifications would be based on the current requirements for interception capability in section 8 of the TICA. That is, the legislation would specify that all network operators and service providers (whether based in New Zealand or based overseas) are required, to the extent possible and whether or not they have made prior investment in capability, to provide assistance in fulfilling the warrant or lawful authority, including assistance to:
- a. identify and intercept only those communications which are authorised to be intercepted,
 - b. obtain call associated data and call content in a useable format,
 - c. carry out the interception unobtrusively, without unduly interfering with any communications, and in a matter which protects the privacy of other communications,
 - d. undertake these actions as close as practicable to the time of transmission, and
 - e. decrypt encryption which the operator or provider has performed.
- The advantage of the proposal is that it would provide greater transparency, business and legal certainty (including for newer or smaller companies who have not had experience of warrants being activated on their service).

Decryption

90. It is proposed to specify expressly that help with decryption only involves using means in the network operator or service provider's control, to help undo any encryption which they have applied.
91. 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.
92. 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.
93. Encryption can make interception more costly, less timely, or even impossible, and it is becoming a more ubiquitous default feature of telecommunications services.

94. While the current scope of the duty to assist encompasses assistance with decryption, the nature of what could be involved with this assistance is not clearly spelt out. This raises concerns that companies might be required to remove encryption which they did not apply themselves.
95. It is proposed to specify that providers would not be required to undo encryption applied by another party, and would have a choice of how to assist.
96. 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.
97. It should be noted that this 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.³⁰
98. The advantages of this proposal are that:
- there is a clear, up to date statement of the scope of the duty to assist, and
 - interception can continue to happen effectively and efficiently, where there is lawful authority to do so.
99. As it is simply a clarification, there is no apparent disadvantage to the proposal.

Ensuring obligations remain proportionate and well-justified

100. 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.

[Out of scope]

101. It is proposed to establish a structured “deem-in” process, which would guide decisions about imposing a capability obligation on telecommunications providers who do not currently have any under the TICA framework. This deem-in process would expressly be limited to services or [Out of scope] the agencies have the ability to obtain lawful authority to intercept ([Out of scope] 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).
102. In considering whether to deem a network or service in to an interception capability obligation, the Minister could be required to have regard to the same considerations as for the deem-up process [Out of scope]
103. In considering these factors, the Minister would be required to take into account the views of the relevant providers, and the surveillance agencies, and consult with the Ministers responsible for Police, the NZSIS, and the GCSB.
104. The deem-in process could be used either for a category of provider, or for specified individual providers. Where it related to a category of provider, the deem-in could be done by regulation. This would ensure that the costs and benefits of imposing the capability were thoroughly explored and consulted on. Where the deem-in process related to specified providers, it would probably need to be done by Ministerial directive (so as not to publicly announce a lack of capability in a particular service). Whether the deeming were done by directive or by regulations, a phase-in period for roll-out of capability would be provided for.

[Remainder of document (paragraphs 105 – 295, glossary and collated questions for feedback) out of scope]

In Confidence

18 May 2012

Review of Telecommunications (Interception Capability) Act (TICA)

Purpose

[Out of scope]

Action Sought

| | Action Sought | Deadline |
|--|---|-------------|
| Minister for Communications and Information Technology | Note the contents of the report. | 23 May 2012 |

Ministry Contacts

| Name | Position and Unit | Telephone | | 1 ST Contact |
|---------------------------|--|---------------------------|-------------|-------------------------|
| | | Work | After Hours | |
| Kirstie Hewlett | Director, Energy and Communications Branch | [Withheld under s9(2)(a)] | | ✓ |
| [Withheld under s9(2)(a)] | | | | |
| [Withheld under s9(2)(a)] | | | | |

In Confidence

5 August 2013

Minister for Communications and Information
Technology

Review of Telecommunications Interception Capability Act (TICA)

[Paragraphs 1-34 out of scope]

In Confidence

[Paragraphs 1-34 out of scope]

Issues raised during the review

Background

35. The current TICA, and the telecommunications interception scheme more broadly, reflected the time in which it was created and assumed the following:

[Out of scope]

- d. encryption by network operators only;
- e. telecommunications services provided almost exclusively by network operators; and

In Confidence

[Out of scope]

36. All of these assumptions have been displaced or impacted by recent changes in the telecommunications industry. These changes include:

[Out of scope]

- c. entrance of new kinds of telecommunications services (for example Voice over Internet Protocol (VoIP) and chat services) which run "over-the-top" of network operators' infrastructure and are offered by separate companies;
- d. increasingly common encryption of telecommunications services at a number of layers at once (e.g. both at the level of the individual email, and at the network level);

[Paragraphs 36(e)-44 out of scope]

In Confidence

[Paragraphs 36(e)-44 out of scope]

Application providers displacing network operators

45. Increasingly, a number of internet based services (known as “application services”, for example, VoIP services), which allow people to communicate with each other, are being offered by companies other than traditional telecommunications providers, and ‘over-the-top’ of those telecommunications providers’ networks. Some of these services – for example, VoIP, and IP video conferencing, web-based email – are displacing the telecommunications services which are provided by network operators.
46. These services were once a core component of the services of fully integrated telecommunication companies, however technology has evolved to allow companies to provide these services to end users without themselves owning or controlling a public telecommunications network.
47. These “application services” will become an increasingly integral part of the way people communicate, and are likely to carry a larger proportion of communications in future, as services migrate to the ‘cloud’.
48. Currently, specialist application providers do not have interception obligations, because they operate over-the-top of another providers’ network and do not fall into the definition of a network operator. They are only subject to the duty to assist interception agencies.

[Withheld under s6(c)]

Encryption at more than one level

49. The TICA requires that a “network operator” decrypt telecommunications they are intercepting, to the extent that they provided the encryption themselves. However, it is increasingly common for a telecommunication to be encrypted at more than one level (for example, at the network, retail, and application 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.

In Confidence

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

[Paragraphs 54-86 out of scope]

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

In Confidence

Overview of draft proposals for change

[Out of scope]

- 1) Tailoring obligations to services and layers

[Out of scope]

- 4) Ensuring interception capability not eroded by new technologies
 - Requiring interception capability from certain application providers
 - Expressly requiring assistance with decryption

[Out of scope]

In Confidence

[Out of scope]

Kirstie Hewlett
Director
Energy and Communications Branch
[Withheld under s9(2)(a)]

Hon Amy Adams
**Minister for Communications and
Information Technology**

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

In Confidence

Interception and Network Security

| | | | |
|-------------|----------------|-----------------|-------------------|
| To | Hon Amy Adams | Priority | Medium |
| Date | 31 August 2012 | Deadline | 11 September 2012 |

Purpose

[Paragraphs 1 to 12 out of scope]

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

MBIE-MAKO-2367281

Prepared by
Briefing No: To be supplied
File No: P/002/TP020/001

[Paragraphs 1 to 12 out of scope]

Lawful Interception (Review of the Telecommunications (Interception Capability) Act 2004)

Problem definition

[Out of scope]

The interception capability obligation:

[Out of scope]

- d. places “network operators” at a competitive disadvantage by requiring 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.

[Out of scope]

In Confidence

[Out of scope]

- 17 More generally, 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. For example, it does not sufficiently address the increasing encryption of communications, and does not have the ability to extend to emerging telecommunications services if they become significant in future.

[Out of scope]

In Confidence

24 Australia,

[Out of scope]

are consulting on the possibility to provide for tiered interception obligations on industry, setting out more detailed requirements as to how to provide interception capability on different services, extending interception to ancillary providers (for example, social networking sites and cloud computing providers), and providing an offence for failing to assist with decryption.

[Paragraphs 25 – 40 out of scope]

In Confidence

[Paragraphs 25 – 40 out of scope]

[Withheld under s9(2)(g)(i)]

MBIE-MAKO-2367281

Prepared by:
Briefing No: To be supplied
File No: P/002/TP020/001

In Confidence

- 42 Application providers: The need for application providers to have adequate interception capability, whether they are New Zealand based or not, is an increasingly important issue (especially with moves to cloud computing), **[Withheld under s6(a) and s6(c)]**

Industry is also concerned to see change in this area because the current distribution of obligations is inequitable and leads to market distortions. In any targeted consultation New Zealand network operators are likely to raise the need to shift capability obligations onto application providers (so that local network operators are not required to provide application-level capability).

- 43 We also recognise that there is a need to ensure a mechanism in the TICA to address new providers and services in future (like application providers), as there is a risk that any amendments to the TICA will be inflexible and very quickly out of date.

44

[Withheld under s9(2)(g)(i)]

- 45 Given the operational need for the surveillance agencies to intercept effectively at the application level and the industry concerns,

[Withheld under s9(2)(g)(i)]

- 46 We also note that there is an independent proposal to provide a structured process (effectively a deem-in process) in the legislation to extend capability requirements in the future which may be applied in future to application providers and any other new kinds of providers. This proposed process would only apply to services which are already authorised to be intercepted in the warranting legislation of agencies, and only if insufficient investment in capability was adversely affecting national security or law enforcement.

- 47 Under this proposed process, the impact of capability obligations on the business of the provider, and the impact on competition and innovation would also need to be taken into account. This would ensure the legislation is flexible for the future and issues like application providers, as they arise, can be considered through a fair process which does not require legislative amendment, but that these issues do not need to be debated in detail now. This also provides another mechanism to cover application providers if an explicit targeted extension to application providers was not favoured.

- 48 Decryption: there is simply a proposal to amend the Act to make clear that the duty to assist includes help with decryption, but that telecommunications providers need only provide that assistance in a manner of their choosing, and are only required to use means within their control. Clarifying the scope of assistance with decryption in this way will not change current privacy settings. The requirement would only apply to communications already authorised to be intercepted, and after a provider is presented with a warrant or lawful authority.

[Paragraphs 49 – 62 out of scope]

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

In Confidence

[Paragraphs 49 – 62 out of scope]

Kirstie Hewlett
Director
Energy and Communications Branch

Hon Amy Adams
**Minister for Communications and
Information Technology**

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

MBIE-MAKO-2367281

Prepared by:
Briefing No: To be supplied
File No: P/002/TP020/001

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]

In Confidence

[Out of scope]

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

In Confidence

[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]

In Confidence

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]

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

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

In Confidence

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

MBIE-MAKO-2697154
Briefing No: 12-13/0469
File No: P/002/TP020/001

In Confidence

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

In Confidence

| Option | Benefits | Costs/Risks |
|---|--|--|
| <p>1. Include an explicit capability obligation on application providers</p> | <ul style="list-style-type: none"> 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: <ol style="list-style-type: none"> in the absence of this explicit obligation, application providers are already caught by the duty to assist (which applies to all service providers); and an explicit obligation is only one, of a number, of steps that would need to be taken <p style="text-align: center;">[Withheld under s6(a) and s6(c)]</p> | <ul style="list-style-type: none"> 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. |
| <p>2. Remove Application providers and replace with a deem-in (or clarifying how the duty to assist applies, and what it entails)</p> | <ul style="list-style-type: none"> 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 | <p style="text-align: center;">[Withheld under s6(a) and s6(c)]</p> |

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

In Confidence

| Option | Benefits | Costs/Risks |
|--------|--|-------------|
| | <p>interests of the sector are preserved.</p> <p>[Withheld under s6(a), s6(c), and s9(2)(g)(i)]</p> <ul style="list-style-type: none"> 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. <p>[Withheld under s6(b)(i) and s9(2)(g)(i)]</p> <p>It already applies to all service providers, and therefore includes application providers.</p> | <p>1.</p> |

In Confidence

| Option | Benefits | Costs/Risks |
|--|--|---|
| <p>3. Remove any interception obligation, deem-in provision, or clarification of the duty to assist, that might apply to application providers</p> | <p>[Withheld under s9(2)(g)(i)]</p> | <ul style="list-style-type: none"> 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)] |
| <p>4. Remove the proposal to extend the duty to assist to apply to decryption</p> | <ul style="list-style-type: none"> 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. <p>[Withheld under s9(2)(g)(i)]</p> | <p>[Withheld under s6(a) and s6(c)]</p> |

In Confidence

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

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

In Confidence

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

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

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.

In Confidence

- 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).

RESTRICTED

OFFICE OF THE MINISTER
FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY

The Chair
Cabinet Committee on Domestic and External Security

**TELECOMMUNICATIONS INDUSTRY – PAPER 1: OVERVIEW OF INTERCEPTION
CAPABILITY AND NETWORK SECURITY PROPOSALS**

[Paragraphs 1 – 15 out of scope]

[Out of scope]

[Paragraphs 1 – 15 out of scope]

Proposed amendments to the TICA

- 16 Paper 2 of this series seeks approval to amend the TICA to (1) make obligations on industry clear and effective, and avoid unnecessary compliance cost [Out of scope]
- 17 Intended benefits from the proposed changes are:

[Out of scope]

- c. More flexible obligations enabling more agile responses to technological developments, including the ability to extend capability obligations beyond network operators, to telecommunications service providers, if certain criteria are met.

[Out of scope]

[Out of scope]

[Out of scope]

Make obligations on industry clear and effective, and avoid unnecessary compliance cost

18 Paper 2 proposes that Cabinet approve amendments to the TICA to:

[Out of scope]

- b. Ensure obligations in the Act can remain up to date, by creating a structured process for the future extension of interception capability obligations to those telecommunications service providers who do not have obligations today⁴ (via a deem-in process).
- c. Make today's compliance requirements more certain by: a) amending the 'duty to assist' to expressly list key elements of assistance which may be required to help fulfil a warrant (including help with decryption), and b)

[Out of scope]

[Paragraphs 19 – 70 out of scope]

[Paragraphs 19 – 70 out of scope]

Recommendations

It is recommended that the Committee:

[Out of scope]

Interception capability obligations on the telecommunications industry

[Out of scope]

- 3 **Note** that Paper 2 proposes that a Telecommunications (Interception Capability and Security) Bill (the Bill) be prepared to amend the Telecommunications (Interception Capability) Act 2004, so as to:
- 3.1 update existing obligations on the telecommunications industry (to help effect duly authorised interception operations), to make the obligations more proportionate flexible and certain; and

[Recommendations 3.2 – 12 out of scope]

[Recommendations 3.2 – 12 out of scope]

Hon Amy Adams
Minister for Communications and Information Technology

____/____/____

[Appendix 1: Out of scope and remainder withheld under s6(a) and 6(c)]

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

[Appendix 2 (pages 21 to 22): Out of scope]

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

RESTRICTED

OFFICE OF THE MINISTER
FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY

The Chair
Cabinet Committee on Domestic and External Security Coordination

TELECOMMUNICATIONS INDUSTRY – PAPER 2: UPDATING INTERCEPTION
CAPABILITY OBLIGATIONS

Proposal

[Out of scope]

- a. updating existing obligations on the telecommunications industry (to help effect duly authorised interception operations), to make the obligations more proportionate and flexible, and

[Paragraphs 1(b) – 9 out of scope]

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Addressing over-investment: making the obligations to invest more targeted

10 This paper proposes that Cabinet approve amendments to the TICA to:

[Out of scope]

- c) Ensure obligations in the Act can remain up to date, by creating a structured process for the future extension of interception capability obligations to telecommunication providers and network elements which do not have them today (via a 'deem-in' process).

Make today's compliance requirements more certain by: a) amending the 'duty to assist' to expressly list key elements of assistance which may be required to help fulfil a warrant (including help with decryption), and

[Out of scope]

[Paragraphs 10(e) – 99 out of scope]

[Paragraphs 10(e) – 99 out of scope]**Ensuring obligations in the Act can remain up to date: Deem-in process**

The telecommunications industry will continue to evolve rapidly, and it will be important for the Act to keep pace, so that surveillance agencies can continue to intercept when authorised to do so. To ensure sufficient flexibility and responsiveness of obligations to invest in interception resources, I propose that the Act be amended to allow interception capability obligations to be extended if needed,

[Out of scope]

- b. organisations which are telecommunication service providers (rather than 'network operators').
- 101 That is, I propose that the Act be amended to include a new "deem-in" process, which would allow for **[Out of scope]** "telecommunications service providers" (on which there is currently only a duty to assist) to be partly or fully deemed-in to a form of interception capability obligation by the Minister responsible for the Act. This process could be used for a category of provider, or for specified individual providers, or for specified types of services. It could be used to extend capability obligations in New Zealand law, to application service providers. It could be done either by regulation (for a category of service provider eg. 'webmail service providers') or by ministerial direction (for named individual service providers, **[Out of scope]**)
- 102 This deem-in process would expressly be limited to services **[Out of scope]** for which the agencies have the ability 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). Deemed-in service providers would be subject to all lawful interception obligations (including registration, security cleared staff etc.) which apply to network operators. Deeming-in would not permit the extension of network security obligations beyond the scope proposed in Paper 3.
- 103 The agencies would apply to the Minister responsible for the Act and notify the company individually (or consult with the group, if by regulation).
- 104 In considering whether to deem a **[Out of scope]** service in to an interception capability obligation, the Minister would be required to conclude on reasonable grounds that the proposed new interception capability obligation is justified for reasons of national security and/or law enforcement.
- 105 In reaching that conclusion, the Minister would be required to take into account the same factors, and relative weightings, as for 'deem-up'.

- 106 In considering these factors, the Minister would be required to take into account the views of the relevant network operators or service providers, and those of the surveillance agencies, and consult with the Ministers responsible for Police, the NZSIS, the GCSB, and the Minister for Communications and Information Technology.
- 107 In deeming-in, the Minister would be required to provide an appropriate lead-in time during which the provider(s) could develop and implement the new capability requirement.

Deem-in via regulation (to be used for categories of provider):

- 108 Where the deem-in relates to a category of provider, the deem-in would be done by regulation. No appeal process would apply as the regulation making process, and requirements imposed by the Act, would ensure sufficient safeguards (including the requirement for the Minister to take into account relevant providers' views). And because it is a class of company, there would be competitive neutrality.

Deem-in via ministerial direction (for individual named providers)

- 109 Where the deem-in process related to specified providers, **[Out of scope]**, it would be done by ministerial direction, so as not to publicly disclose operational or strategic information.
- 110 Provision would be made for affected providers or network operators to make a submission directly to the Minister.
- 111 A review process would be provided for, because there may be competitive disadvantage when a single provider or operator is singled out for additional compliance cost. I note that judicial review would also remain available.
- 112 *Proposed process:* All material submitted to the Minister in relation to the application, would be referred to a panel of three appointed by the Minister. The Panel would consider the materials and all other relevant information, and would make a recommendation to Minister. The Minister would be required to consider the recommendation and would have the discretion to maintain, amend or revoke the direction. The affected network operator would be provided with a summary of the Panel's recommendation and reasons, however there would be no requirement to disclose any classified information supporting the reasons.

Making today's compliance requirements more certain

Spelling out the 'duty to assist'

- 113 Only network operators are obliged to pro-actively invest in interception capability on their networks. However, section 13 of the TICA requires all service providers, as well as all network operators, to assist with an interception operation, when presented with a warrant or other lawful authority to intercept. This assistance is specified as including (a) making technical staff available, as well as (b) all other reasonable steps necessary to give effect to the interception.

- 114 This current obligation is very broadly worded. I propose that this section be amended to specify in more detail what is reasonably necessary to give effect to a request for assistance. These specifications would be based on the current requirements for interception capability in section 8 of the TICA.
- 115 This would put beyond doubt the intention that all providers of telecommunications services in New Zealand are expected to assist in the fulfilment of warrants, wherever possible. It would also provide greater transparency, business and legal certainty, especially for newer or smaller companies who have not had any experience of warrants being activated on their service.
- 116 I propose that the TICA be amended to specify that all network operators and service providers (whether based in New Zealand or based overseas) are required, whether or not they have made prior investment in capability, to provide assistance in fulfilling the warrant or lawful authority, including assistance to:
- a. identify and intercept only those communications which are authorised to be intercepted,
 - b. obtain telecommunications content, and associated data in a useable format,
 - c. carry out the interception unobtrusively, without unduly interfering with any communications, and in a matter which protects the privacy of other communications,
 - d. undertake these actions as close as practicable to the time of transmission, and
 - e. decrypt encryption which the operator or provider has provided.
- 117 *Decryption:* Encryption can make interception more costly, less timely, **[Withheld under s6(a) and s6(c)]**, and it is becoming a more ubiquitous default feature of telecommunications services.
- 118 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 surveillance agency. It is not proposed to change this requirement. 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, some or all of the communication may still be encrypted or otherwise modified, in a way which makes it unintelligible without further processing.
- 119 The current scope of the duty to assist encompasses assistance with decryption. The duty applies to any network operator or service provider on which the warrant is served, even if they did not perform the interception.

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

in

cases where this is not the most efficient way to achieve decryption.

120 Accordingly, I also propose that the Act also be amended to specify that the network operator or provider assisting with decryption must consult with the relevant surveillance agency regarding the most efficient way to do so, in that operation. In some cases the most efficient way will be for the network operator or service provider to decrypt themselves, while in others it will be more efficient for the surveillance agency to be provided with the means to decrypt.

121 It should be noted that this proposal does not change existing policy settings in relation to privacy, 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 should be provided in consultation with the relevant surveillance agency, 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 generally, including in relation to the amended requirement.²⁵

[Paragraphs 122 – 218 and recommendations 1 – 54 out of scope]

²⁵ 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 reporting, compliance checking and audit powers (see s216B of the Crimes Act 1961, and the legislation cited in footnote 1).

²⁶ Section 8(1)(c) of the TICA.

[Paragraphs 122 – 218 and recommendations 1 – 54 out of scope]

Deem-in

Agree to create a statutory process for extending interception capability obligations, ie. 'deeming-in',

[Out of scope]

55.2 organisations which are telecommunication service providers (and the services they provide).

56 **Agree** that deeming-in to full or partial capability obligations could be done by ministerial direction (in the case of named organisations, [Out of scope], or by regulation (in the case of categories of organisation

57 **Agree** that this process could not be used unless the network or service in question is one for which a New Zealand surveillance agency could, at the time the extension is proposed, obtain lawful authority to intercept.

58 **Agree** that if a [Out of scope] service or organisation is deemed-in, [Out of scope] service provider is subject to all the lawful interception-related obligations (but not network security obligations) of a network operator under the Act, unless otherwise specified.

- 59 **Agree** that a deeming-in process would be initiated by application from a surveillance agency to the Minister responsible for the Act. The surveillance agency would have the obligation to notify the affected network operator(s) or service provider(s).
- 60 **Agree** that prior to determining to deem-in [Out of scope] organisation, it would be necessary for the Minister to conclude on reasonable grounds that the proposed new interception capability obligation is justified for reasons of national security and/or law enforcement. The Minister would be required to take into account the same statutory considerations and relative weightings as for the deem-up process.
- 61 **Agree** that prior to deeming-in any [Out of scope] organisation the Minister responsible for the Act must:
- 61.1 take into account the views of the relevant [Out of scope] or service provider;
 - 61.2 take into account the views of the surveillance agencies; and
 - 61.3 consult with the Minister of Police, the Minister in charge of the New Zealand Security Intelligence Service, the Minister Responsible for the Government Communications Security Bureau, and the Minister for Communications and Information Technology.
- 62 **Agree** that in cases where the Minister responsible for the Act issues a direction deeming-in a named organisation [Out of scope], the [Out of scope] service provider may submit directly to the Minister in relation to the statutory considerations and the nature of the obligations to be imposed.
- 63 **Agree** that when deeming-in any [Out of scope] organisations, the Minister must provide for a reasonable lead-in time during which the relevant network operator or service provider is able to take all steps to become compliant.
- 64 **Agree** that in cases where the Minister responsible for the Act issues a direction deeming-in a named organisation or a specific network element, the affected [Out of scope] service provider may request that the Minister's decision be reviewed.
- 65 **Agree** that the process for review of a deem-in direction will be as follows:
- 65.1 the Minister responsible for the Act must appoint a three-person panel to review all relevant submissions made to the Minister, take into account all other relevant information, and make recommendations to the Minister in relation to the deeming-in of the service provider,
 - 65.2 the Minister must consider the recommendations of the review panel,
 - 65.3 having considered the recommendations of the review panel the Minister may maintain, vary or revoke the direction.
 - 65.4 a summary of the review panel's recommendation and reasons must be provided to the affected service provider, and any classified information may be withheld from that summary.

Duty to Assist

- 66 **Agree** that the existing 'duty to assist' in the TICA be amended to expressly provide that all network operators and service providers, whether based in New Zealand or overseas, are required, to the extent possible, and whether or not they have made prior investment in capability, to provide assistance in fulfilling a warrant or lawful authority to intercept, including assistance to:
- 66.1 identify any intercept only those communications which are authorised to be intercepted;
 - 66.2 obtain telecommunications content, and associated data in a usable format;
 - 66.3 carry out the interception unobtrusively, without unduly interfering with any communications, and in a manner which protects the privacy of other communications;
 - 66.4 undertake such actions as close as possible to the time of transmission; and
 - 66.5 decrypt encryption which the operator or provider has provided.
- 67 **Note** that the requirements listed in paragraphs 66.1-66.5 mirror the elements listed in the current standard capability obligation.
- 68 **Agree** that the network operator or provider assisting with decryption must consult with the relevant agency regarding the most efficient way to do so, in that operation.
- 69 **Note** that the proposals to clarify the duty to assist do not require additional investment or change existing policy settings in relation to privacy.

[Recommendations 70 - 111 out of scope]

[Recommendations 70 - 111 out of scope]

Hon Amy Adams
Minister for Communications and Information Technology

____/____/____

[Appendix 1: Out of scope and remainder withheld under s6(a) and s6(c)]

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

IN CONFIDENCE

OFFICE OF THE MINISTER
FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY

Cabinet

TELECOMMUNICATIONS (INTERCEPTION CAPABILITY AND SECURITY) BILL:
APPROVAL FOR INTRODUCTION

[Paragraphs 1 to 4 out of scope]

Updated Interception Capability Requirements

5. Part 2 of the Bill updates current interception requirements on network operators and telecommunications service providers. The changes are to:

- a. make obligations on industry clear and effective in light of changing industry structures;

[Out of scope]

- c. ensure the scheme is flexible enough to match today's operational needs, and future technology developments.

[Out of scope]

- b. ensure obligations in the Act can remain up to date, by creating a structured process for the future extension of interception capability obligations to telecommunication service providers;

[Out of scope]

[Paragraphs 9 to 16 out of scope]

- a. update existing obligations on the telecommunications industry (to help effect duly authorised interception operations), to make the obligations more proportionate, flexible and certain; and

[Paragraphs 18 to 28 out of scope]

[Paragraphs 18 to 28 out of scope]

Duty to assist

29. The existing TICA currently requires all service providers, as well as all network operators⁶, to assist with an interception operation, when presented with a warrant or other lawful authority to intercept.
30. Subpart 3 amends the duty to put beyond doubt that the duty is relevant to companies whether based in New Zealand or based overseas, and whether or not they have made prior investment in capability. Amendments are also made to expressly list the various elements of assistance which may be required to help

[Out of scope]

⁶ "Service provider" is currently defined as follows, and the definition will not change: "any person who provides a telecommunication service to an end user (whether or not as part of a business undertaking, and regardless of the nature of that business undertaking)". The definition of network operator will not change either: "Network operator" means "a person who owns, controls or operates a public telecommunications network, or a person who supplies (whether by wholesale or retail) another person with the capability to provide a telecommunications service".

fulfil a warrant. These include assistance to remove encryption (if the operator or provider provided that encryption).

31. All these elements mirror requirements in the capability obligation. The difference is the company is required to provide all reasonable assistance, whether or not they have capability or capability obligations.

[Out of scope]

Ability to require service providers to have same obligations as network operators ('Deem-in')

35. Subpart 5 includes new provisions which allow interception capability obligations to be extended, if needed, to 'telecommunication service providers' who, in contrast to 'network operators', do not have any capability obligations today. The category of 'service providers' includes companies who provide software-level telecommunications services (i.e. over the top providers such as webmail, or internet-based VoIP **[Withheld under s6(c)]**, as well as internet cafes.
36. Deemed-in service providers would be subject to all interception-based requirements (including registration, security cleared staff etc.) which apply to network operators.⁸

[Out of scope]

⁸ The deeming-in would not extend network security requirements. These will only apply to network operators.

37. At the application of a surveillance agency, service providers could be deemed-in by confidential ministerial direction (for individually named providers), or by regulation (for categories of provider).
38. The extension of obligations could only be made if the Minister responsible for the Act was satisfied that the direction is necessary for reasons of national security or law enforcement. The Minister would need to have regard to a number of factors, including the cost of compliance, and the effect on competition and innovation. The Minister would be required to take into account the views of affected operators, and those of relevant Ministerial colleagues (the Ministers for the surveillance agencies, and the Minister for Communications and Information Technology⁹).
39. Except where the deem-in occurs by regulation, the affected service provider could also request a review of the Ministerial decision to deem them in. The review panel would be appointed by the Government and would make recommendations to the Minister, which could be adopted at the Minister's discretion.

[Paragraphs 40 – 61 out of scope]

[Withheld under s9(2)(g)(i)]

Interception capability

[Withheld under s9(2)(g)(i)]

[Withheld under s6(a), s6(c) and 9(2)(g)(i)]

[Out of scope]

65. Equally, it is not appropriate to extend capability obligations to application service providers generally, because:
- a. Overseas-based providers generally have capability obligations to meet requirements in their home jurisdiction. **[Withheld under s6(a) and s6(c)]**
 - b. Meanwhile, all service providers (whether at the application level or otherwise) already have a duty to assist, which local providers must comply with, and which international providers can recognise and act upon if it is not inconsistent with their local laws.
66. Instead, the Act is being updated to permit the extension of capability obligations to service providers (including application providers), using a structured process, and where this is shown to be necessary for reasons of national security or law enforcement (the 'deem-in' power).

[Out of scope]

[Out of scope]

69. The amendment to make clear that the duty to assist expressly includes assistance to remove encryption (if the network operator or service provider provided that encryption) may also draw some attention. However, this amendment simply clarifies the current scope of the duty to assist. The amendment mirrors the requirement to decrypt which is part of the current obligation to be intercept capable. Further, the amendment does not change any current privacy settings because it only applies to communications which are already authorised to be intercepted. The current statutory requirements to maintain the privacy of, and not interfere with, telecommunications which are not authorised to be intercepted will remain unchanged.

[Paragraphs 70 – 94 out of scope]

[Paragraphs 70 – 94 out of scope]

Hon Amy Adams
Minister for Communications and Information Technology
____ / ____ / ____

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

[Appendix One (pages 19 to 22) out of scope]

RELEASED UNDER THE
OFFICIAL INFORMATION ACT