Document 8

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]

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)]