DOCUMENT 3

Ministry of Business, Innovation & Employment

TECHNICAL PAPER:

TELECOMMUNICATIONS

INTERCEPTION CAPABILITY

AND

NETWORK SECURITY

December 2012

RELEASED UNDER THE OFFICIAL INFORMATION ACT

[Introduction pages 2 to 4 out of scope]

RELEASED UNDER THE OFFICIAL INFORMATION ACT

TABLE OF CONTENTS

[Out of scope]

[Out of scope]

RELEASED UNDER THE OFFICIAL INFORMATION ACT

[Out of scope]

RELEASED UNDER THE OFFICIAL INFORMATION ACT

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

[Paragraphs 1 – 29 out of scope]

RELEASED UNDER THE OFFICIAL INFORMATION ACT

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]

RELEASED UNDER THE OFFICIAL INFORMATION ACT

[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]

RELEASED UNDER THE OFFICIAL INFORMATION ACT

[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]

RELEASED UNDER THE OFFICIAL INFORMATION ACT

[Out of scope]

RELEASED UNDER THE OFFICIAL INFORMATION ACT

[Paragraphs 44-87 out of scope]

RELEASED UNDER THE OFFICIAL INFORMATION ACT

[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.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

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]

RELEASED UNDER THE OFFICIAL INFORMATION ACT

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]

RELEASED UNDER THE OFFICIAL INFORMATION ACT