Telecommunications industry – Updating interception capability obligations

Agency Disclosure Statement

1. This Regulatory Impact Statement has been prepared by the Ministry of Business, Innovation and Employment.

2. It provides an analysis of options to update the obligations for interception capability on network operators, and to implement a compliance and enforcement framework.

3. The analysis is based on the assumption that the compliance and enforcement framework will be accepted in its entirety, thereby giving surveillance agencies the tools to appropriately address issues of non-compliance.

4. The analysis in this statement includes an examination of the likely costs, benefits and risks of these actions. It also outlines the alternative options that were examined during the policy process but not recommended to Cabinet.

5. The recommended options are estimated to save network operators significant investment, in some cases, running into tens of millions of dollars. [Information Withheld]

6. This Regulatory Impact Statement is one of two Regulatory Impact Statements prepared to inform changes to the Telecommunications (Interception Capability) Act 2004.

[Information withheld]

12 March 2013

Part one

Lawful interception

Introduction

7. Law enforcement and security agencies have used interception of telecommunications as a tool in their work to combat serious crime and maintain national security, since telephones became widely available to the public.

8. Today, interception of telecommunications in real-time is a vital tool to:

   - Investigate, disrupt and prosecute serious criminal activity, including organised crime,
   - detect and prosecute international and serious local cybercrime,
   - combat threats to national security and critical infrastructure, and

- respond to emergencies like armed offender situations or kidnappings.

9. Interception of private telecommunications without a valid warrant or other legal authority is an offence under s216B of the Crimes Act 1961. Only three government agencies can lawfully conduct interception: the New Zealand Police, the New Zealand Security Intelligence Service, and the Government Communications Security Bureau. These will be referred to as the "surveillance agencies".[1]

Problem definition

10. 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.

11. However, many are also the result of developments in the telecommunications industry. These developments include:

    a. a shift in industry structure, moving from a small number of vertically integrated players to increasing numbers of players operating at different levels (infrastructure, wholesale and retail);

    b. changes in infrastructure and technology, with the build-out of fibre access networks through the Ultra-fast Broadband Initiative, and the future shift to 4G/LTE networks likely through re-allocation of the 700MHz spectrum;

    c. decreasing revenues and margins for telecommunications providers, due to fragmentation of the market, increased competition, and consumer demand for increased service offerings without a commensurate increase in price;

    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

    e. changing use of telecommunications services, as people increasingly use services while roaming across a number of different network types and providers.

12. These changes are likely to accelerate in coming years, but (along with underlying issues with the way the Act is framed and implemented) have already led to the following problems:

    - in situations where more than one network operator is involved in providing a telecommunications service, then the Act requires investment in interception capability to be duplicated at a number of levels, and does not account for the likelihood of an interception taking place on any given service, or the relative cost and technical feasibility of intercepting at different layers, or recent changes in industry structures and practices;
    - there are no consistent or binding standards for compliance, so differing technical, delivery and administrative arrangements from each of the authorised agencies lead to additional compliance cost for industry;

[1] The Search and Surveillance Act 2012 also provides the ability for the New Zealand Customs Service and the Department of Internal Affairs to become intercepting agencies, if they meet the statutory criteria in section 50 of the Act.

- there are few processes to encourage and support compliance;
- enforcement options for non-compliance are impractical; and
- [Information withheld]

13. Industry advice to date is that their three key concerns are the inflexibility of the current blanket obligation on all network operators' services, [Information withheld] and the lack of unified, binding standards for compliance with the Act. These elements can drive much higher than necessary compliance cost (potentially in the tens of millions of dollars, see table at paragraph 65 for detailed cost estimates), and/or distort market dynamics.

14. [Information withheld]

Meanwhile, new technologies are emerging rapidly, but there is no capacity to quickly adapt obligations to suit market evolution. [Information withheld]

Together, these factors mean that the capability that does exist today may not provide the same coverage in the future. This puts in jeopardy the ability to carry out lawful interception as authorised by a court or Parliament.

Status quo

15. The Act imposes two kinds of obligations on the telecommunications industry:

- all network operators must have interception capability (section 7 of the TICA); and
- all network operators and service providers have a duty to assist (section 13 of the TICA).

16. Except for a broad distinction between network operators and service providers, the Act does not differentiate between types of telecommunications providers within these categories. It places an obligation to be fully interception capable on all network operators – whether they are small or large, infrastructure providers or retail service providers, or whether they are providing a telecommunications service over their own network or merely reselling that service.

17. These obligations reflect the time in which they were created, and assume both a small number of vertically integrated telecommunications companies, and that telecommunications services were provided almost exclusively by network operators. However, the telecommunications industry has changed significantly since that time, with shifts in industry structure, the entrance of new kinds of players, and the introduction of new infrastructure, technologies and services.

18. Preliminary feedback from members of the telecommunications industry and the authorised agencies, is that the drafting of the Act, together with these changes, have led to the following problems with the obligation to have interception capability:

- the structure of the TICA obligations leads to duplication of interception capability in some circumstances. This duplication is inefficient, is not always required to meet the operational needs of the authorised agencies, and can significantly increase cost for industry;
- the Act can be read as requiring full interception capability applies to providers who have no technical way to meet it (eg. infrastructure providers cannot identify communications made by a particular customer of the retail service provider using that network);
- the interception obligation is not proportionate to size and type of providers [Information withheld]
- the blanket nature of the obligation (together with a limited exemption power) does not allow network operators to prioritise their investment, and invest in areas of the greatest operational use and significance for the authorised agencies; and
- if a company falls within the definition of network operator, all its public networks must be interception capable, but also all its services, whether or not they are provided to the public. This leads to unnecessary complexity and needless exemption applications.

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

20. [Information withheld]

21. Continuing with the status quo is not an option if government is [Information withheld] and wanting to reduce compliance costs on the industry.

The telecommunication industry

22. Currently there are 13 known network operators that have 10,000 or more end users, and over 30 known operators that are below that threshold. The exact numbers are not known and no estimate is available.

23. There are no statistics available of how many warrants are served on network operators, as the GCSB and the NZSIS do not publish these. The World Internet Survey showed that 92 percent of all internet traffic was carried across five providers, all that have more than 10,000 end users. [Information withheld]

Objectives

24. To be successful, a national interception scheme must enable agencies to intercept effectively, without imposing disproportionate cost on telecommunications users, providers and government. That is, a successful scheme is one which gives effective coverage of interception capability, while ensuring:

    a. the privacy of communications outside the scope of a warrant or lawful authority to intercept;

    b. minimum interference with or disruption to telecommunications services;

    c. minimum duplication of equipment and operational capability (by clear and efficient allocation of obligations within industry, and between industry and agencies);

    d. transparency of requirements to provide maximum certainty for industry in making investment decisions;

    e. reasonable and equitable expenditure by industry to achieve interception capability (by aligning requirements with international standards and future operational priorities and capability); and

    f. low impact on the market (legislation and its implementation or enforcement do not unduly distort competition or create undue barriers to entry and innovation).

25. In order to achieve these outcomes, an interception capability scheme should have the following characteristics:

    a. be suitable for the size and structure of the New Zealand telecommunications market;

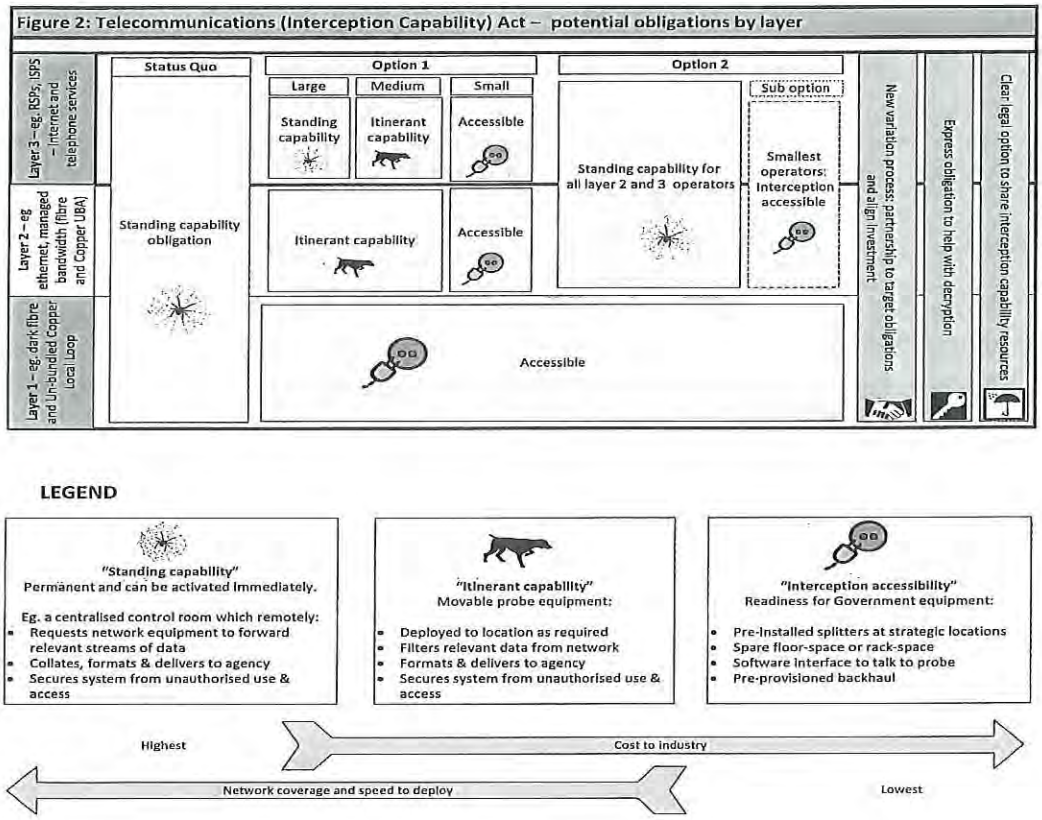
    b. allow industry and government to work in partnership; and

    c. be flexible enough to support interception capability in a changing industry and technological environment.

Options

Option one – a multi-tiered framework by layer (not recommended)

26. Option one is to have a framework that has tiered obligations depending on the network layer at which the service is provided and the size and revenue of the operator (option 1 being small, medium and large; option two using an exclusion for smaller operators). There would be three categories of capability – standing, itinerant, and accessible, where standing and itinerant categories were defined by the type of capability solutions used. The framework is illustrated below in Figure 2.



27. While the benefits and costs for both government and industry are largely the same as for option two (see paragraph 64 below), the feedback from industry on this proposal was that there should be no standing capability requirement, it was better not to prescribe technical solutions as they did not always correlate with speed of activation. If speed was the outcome sought, this should be specified instead. It was also reflected that some services already have standing capability, and this was unlikely to change in the near future. However, to allow flexibility, network operators should not have to have permanent, fixed infrastructure on all parts of their network.

28. This option does not meet the objectives stated in paragraph 24, especially minimum duplication of equipment and operational capability (by clear and efficient allocation of obligations within industry, and between industry and agencies) and reasonable and equitable expenditure by industry to achieve interception capability (by aligning requirements with international standards and future operational priorities and capability).

Option two – a risk-based framework by type of service offered and the number of end users *(recommended)*

29. Option two is to have a framework that creates reduced obligations for some services and network operators, depending on the type of service, or the number of end users. The statutory requirement to assist in the fulfilment of warrants (the duty to assist) would remain equally on all network operators and service providers. The framework is illustrated in the diagram below.

[Information withheld

]

30. The following amendments are recommended to give effect to this framework.

Removing capability obligations on infrastructure-level services

31. [Information withheld

32.] it is proposed to amend the TICA to remove interception capability obligations from infrastructure-level services, but to indicate that if and when interception is required at this level for a specific operation, a Minister may require that the necessary part of the network be made accessible to interception equipment at a specified point (see 'deem-up' process in paragraph 51 below).

Removing capability obligations from resold services

33. Some network operators sell services to end users, which are in fact provided completely by another network operator. An example is 'mobile virtual network operators', such as TelstraClear, which merely re-bills services offered over Vodafone's network. The TICA did not contemplate the emergence of 'pure resellers' and currently requires both the actual network operator and the reseller to have capability on the relevant service. This is both unnecessary and impossible, as the reseller has no access to the relevant network to install capability or effect interceptions.

34. It is proposed to amend the TICA to remove interception capability obligations from resold telecommunications services, in cases where the person who owns, operates or controls the service has standard (ie. unreduced) capability obligations under the TICA.

Reducing obligations on wholesaled services: 'interception accessibility'

35. The TICA's current requirement for full, independent interception capability on wholesaled telecommunication services is neither appropriate nor necessary, because:

    a. all services sold on a wholesale basis are subsequently provided to end-users by a retail service provider,

    b. wholesale prices for some providers can be heavily regulated by the Commerce Commission, and the Local Fibre Companies have contracted for set prices with the Government as part of the Ultra-fast Broadband Initiative. This means there is very limited ability for some wholesalers to recover the capital expenditure involved in purchasing capability, and

---

[Information withheld]

c. agencies are of the view that, [Information withheld] as this is generally simpler, more efficient, and provides better capture of communications within the scope of the warrant.[4]

36. However, there will be cases [Information withheld]

37. Accordingly, it is proposed that the TICA be amended to impose reduced obligations on wholesaled services. The capability on the wholesaled service would be provided by the retail provider whose customer is the subject of the warrant. The wholesaler would only be required to provide access to their own network for the retailer's capability.

Reducing obligations on very small retail operators: 'intercept readiness'

38. The TICA does not account for the emergence of very small network operators, who have very limited likelihood of receiving a warrant (given the size of their customer base), and who also have very limited funds to invest in capability resources. In order to make compliance cost on these smallest players more proportionate with government's operational needs, it is proposed to reduce their obligation from investment in interception capability, to investment in 'interception readiness'.

39. The proposed reduced capability obligation would apply to network operators with 10,000 or fewer end users on all their services, and all their public networks.

40. The obligation would involve the same obligations of pre-establishing access points for interception, and cooperating to enable use of third-party capability (as in the accessibility obligation for wholesaled services).

41. Because operators in this category would have minimal up-front investment obligations, it is proposed that they not be eligible to seek reimbursement from government for their costs involved in effecting an operation.[5]

42. Companies' obligations would grow as they increase in size. This should mitigate any concerns about significant competitive advantage arising from allowing lesser investment.

43. [Information withheld]

A new exemption process to reduce obligations, using a risk-based assessment

---

3. [Information withheld]
4

[5] Section 18 of the TICA currently provides for payment of the actual and reasonable costs incurred in assisting the agencies.

44. The TICA currently allows a network operator to seek an exemption from the requirement to have interception capability on all their services and all their public networks. However, the current exemption process is inflexible and slow. The process can take months even when the application is straightforward and uncontroversial. The TICA only permits exemptions to be granted in limited 'special circumstances' such as a pilot trial of a new network or service. This inflexibility does not allow industry investment in capability to be prioritised to align with the operational interests (and investment) of the surveillance agencies.

45. It is proposed that the TICA be amended to include a new and more flexible exemption process, through which capability obligations on particular operators or classes of operators or service can be reduced.

46. The Minister responsible for the TICA would have the power to vary or revoke exemptions, and include transitional arrangements if required.

47. *Decision-making: process and timing:* it is proposed that the TICA be amended to include provisions setting out the exemption process. The Act would create a statutory position to which applications for exemption are to be addressed. The TICA would specify that a substantive response must be made as soon as practicable, or no later than 20 working days after the request is received. The surveillance agencies would have the ability to request a reasonable extension.

48. In assessing exemption applications, the decision-maker would be required to take into account all relevant factors, including:

    a) the government's operational and strategic interests in national security or law enforcement;

    b) the network operator's customer numbers or revenue by service (not by operator);

    c) the cost of compliance with the obligation sought to be varied; and

    d) whether compliance could be achieved appropriately by another means.

49. The primary consideration would be (a), with the other factors as subsidiary considerations.

50. *Preventing numerous applications relating to the same issue*: There are a range of services offered by telecommunications companies where it is either not necessary or possible to provide interception capability, but which nevertheless fall within the scope of the TICA. These can include, for example, technical trials or demonstrations where there are no users.

51. Currently, time-limited exemptions must individually be sought, granted and renewed for such network services, to avoid legal risk. It not appropriate to exempt these services from having capability obligations in the TICA itself, as this would in many cases disclose gaps in capability which could be exploited by those who wish to avoid interception. It is proposed that the surveillance agencies issue class exemptions for categories of services on which they jointly agree that standard interception capability should not or cannot sensibly be required, using the proposed new ability to issue class exemptions.

<u>The ability to increase obligations where Act imposes lower capability requirements: deem-up power</u>

52. In all the cases above where a network operator has less than standard obligations under the TICA, it is proposed that the Minister responsible for the TICA would have ability to impose a higher capability obligation on a network or service, or part of a network or service. For example, this could increase obligations from an intercept 'accessible' or 'ready' obligation to the standard intercept capable obligation, or from having no obligation to having to install an access point at Layer 1. The requirement for greater obligations could be time-limited, or for an unspecified period, depending on operational requirements and the nature of the increased obligation.

53. There would be a statutory threshold for the deeming power. 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.

54. In reaching that conclusion, the Minister would be required to take into account all relevant factors, including:

    a. whether the current level of interception capability on that network or service adversely affects national security or law enforcement;

    b. whether the cost of compliance would seriously adversely affect the business of the company providing that network or service;

    c. whether the revised obligations would unreasonably impair the provision of telecommunications services in New Zealand or competition in telecommunications markets, or create barriers to the introduction of new or innovative telecommunications technologies.

55. In applying this test, the Minister would be required to give primacy to consideration (a). Paragraphs (b) and (c) would be subsidiary considerations.

56. Ability would be provided for the affected telecommunications company to submit directly to the Minister in relation to the statutory considerations and the nature of the increased capability to be imposed. However, no appeal or review rights are proposed as it would be clearly anticipated on the face of the legislation that those companies with reduced obligations may have them increased where necessary for operational reasons. Judicial review would remain available.

<u>Ensure obligations in the Act can remain up to date: Deem-in process</u>

57. 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. Therefore, it is proposed that the TICA provide a "deem-in" process, which would allow for "service providers" (who currently only have a duty to assist) to be partly or fully deemed-in to a form of interception capability obligation by the Minister responsible for the TICA. This process could be used for a category of provider, or for specified individual providers, or for specified types of services only that companies provide. It could be used to extend capability obligations in New Zealand law, to application service providers.

58. This deem-in process would expressly be limited to services or networks 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). The deemed-in service provider would then be subject to all the compliance obligations (eg. registration, security cleared staff etc) which apply to network operators.

59. The agencies would apply to the Minister and notify the company individually (or consult with the group, if by regulation).

60. In considering whether to deem a network or 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.

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

61. 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 TICA, would ensure sufficient safeguards (including the requirement for the Minister to take into account relevant providers' views). Furthermore, because it is a class of company, there would be competitive neutrality.

Deem-in via Ministerial directive (for individual named providers)

62. Where the deem-in process related to specified providers, it would be done by Ministerial directive, so as not to publicly disclose operational or strategic information. Provision would be made for affected providers to make a submission directly to the Minister.

63. A review process would be provided for, because there may be competitive disadvantage when a single provider is singled out for additional compliance cost. Judicial review would also remain available.

Other minor amendments to give effect to option two

64. It is proposed that there be other minor amendments to give effect to option two, and to ease compliance efforts for industry. These include:

a. allowing network operators to share interception resources through commercial contractual arrangements;

b. adding a timeliness factor to section 8 of the TICA;

c. refining the "duty to assist" to specify in more detail what is reasonably necessary to give effect to a request for assistance; and

d. specifying which series of international standards are to be complied with when formatting intercepted material for delivery to agencies.

Benefits and costs for option two

65. The anticipated benefits and costs to both government and industry from the changed interception capability obligations are detailed in the table below.

	Government	Industry
Benefits	• [Information withheld] more proportionate obligations and ability to work together • More ability to negotiate tighter	• Flexibility for industry regarding technology and solutions – industry can negotiate equipment sharing contracts and share expertise to meet their obligations

	timeframes for network operators to have interception capability up and running on key services after receiving a warrant • Faster exemption process will lead to less administration time for officials and Ministers • More flexible obligations will allow more agile responses to technological developments • Specified standards will make it easier to prove non-compliance, and without reference to the capability of the agency to receive the data (as is currently the case)	• More proportionate obligations to the likelihood of receiving a warrant to intercept • Removes the blanket requirement on all services and focussing the requirement on services of operational interest • Increased compliance creates a more level playing field amongst operators of a similar size • Specified standards will make it easier for industry to comply, and gives certainty. It will also reduce costs as they will no longer have to reformat material for delivery to agencies • Faster exemption process will cut administrative costs and allow trials of new services and networks to proceed at a faster pace • Gives more certainty and clarity about what is required under the "duty to assist"
Costs	• The cost for government should not increase, as these obligations already exist and these proposals do not increase the power to obtain a warrant • C Information withheld •	• Cost of complying with obligations – these costs are not new, as the obligations exist already • C Information withheld J

	]	

66. The amendments proposed are designed to reduce unnecessary investment obligations imposed on the industry. These savings have been estimated as follows.

Proposed amendments re:	**Estimated total savings for network operators across New Zealand**
Obligations on infrastructure services	Several tens of millions of dollars
Obligations on wholesaled services	Several millions of dollars
[Information withheld	Information withheld]
Retail providers with under 10,000 end users	Savings of 45%-65%, [Information withheld]
Reducing need for exemption requests, and faster exemption process	Several millions of dollars (savings largely limited to larger providers)
Specifying that compliance with specified international standard constitutes a 'useable format'	Several millions of dollars

67. There is not expected to be any impact for industry from the introduction of the express reference to 'timeliness' as a component of capability, as agencies advise that there is sufficient timeliness today on the services which are usually called upon in emergency interception situations.

Risks

Public perception that agencies will have increased interception powers

68. There is a risk that the public will perceive that any changes to the interception regime could or will increase the powers of the surveillance agencies to carry out more interception. No proposals in this paper extend the scope of warranting powers for any agency.

69. This concern can be mitigated through communications messages, clearly stating that the interception powers will not be altered.

[

70. Information withheld

71.

72.

73.

]

Net impact

74. Overall, this option reduces duplication and wasted capability, is more proportionate for smaller network operators where the cost of complying can be prohibitive and unjustified by operational need. It also aligns investment with operational priorities of agencies.

75. It is not anticipated that this option will have any significant increase in cost for government.

[Information withheld

]

76. This option meets all of the objectives stated in paragraph 24, particularly minimum duplication of equipment and operational capability, reasonable and equitable expenditure by industry to achieve interception capability, and transparency of requirements to provide maximum certainty for industry in making investment decisions.

Part two

Compliance and enforcement framework

Introduction

77. In order to give effect to the interception capability proposals above, it is recommended that there be an improved compliance and enforcement framework implemented. Much of this framework is replicated for network security. For discussion on the network security considerations, please see the companion Regulatory Impact Analysis.

Problem definition

78. [Information withheld

]

79. The only enforcement option in the TICA is for one of the surveillance agencies to take High Court action in instances of alleged non-compliance with interception obligations. Where the High Court finds that a telecommunications provider is non-compliant, it may issue a compliance order requiring the company to do, or cease doing, any specified thing.

80. The enforcement option is problematic for a number of reasons:

a. this is a serious and resource-intensive response to problems, and is only appropriate in the most severe cases of non-compliance. There are no formal intermediate steps available.

b. surveillance agencies need to work with telecommunications companies regularly, and court proceedings are inimical to maintaining on-going working relationships, especially where they are a disproportionate response to the issue at hand.

c. Court proceedings are poorly suited to the sensitive nature of the subject-matter (as information about capability gaps, and sensitive commercial information could become public)

d. it is also a slow process, and therefore is not well equipped to deal promptly with instances of non-compliance.

81. [Information withheld

]

Status quo

82. Telecommunications service providers are not required to be licensed, register, or have a presence in order to operate in New Zealand. The Act itself is a "passive" compliance regime – which means that obligations are assigned but there is no formal requirement on government or industry to advise whether networks and services are compliant.

83. As a result of this, the agencies have good knowledge of some network operators, [Information withheld]For security purposes it also makes it difficult to know to whom, and when, the Government should be providing information.

84. [Information withheld

]

85. In cases where operators have not complied with their obligations, the remedy for government is to take a case to the High Court to seek a compliance order. If the compliance order is breached, the maximum penalty is a fine not exceeding $500,000, and $50,000 per day for continued non-compliance.

86. In addition, the Act does not explicitly require that network operators either have someone within their company, or have access to someone externally, who holds an appropriate security clearance. If network operators do not have access to someone with an appropriate security clearance, the agencies have difficulty both serving a warrant to activate a particular interception operation, and/or do not have a clear point of contact within each operator to discuss interception capability on their network. It is also difficult for Government to share detailed information about the security of networks and explain why risk mitigations are needed, if there is not someone with the appropriate clearance available.

87. [Information withheld

88.

]

89. Finally, there are no powers available for agencies to seek information from companies regarding interception or security matters, nor to test, inspect or otherwise confirm compliance of networks with the relevant legal obligations.

90. Continuing with the status quo is not recommended. [Information withheld] Industry also needs a way to enter into constructive dialogue with government, including the ability to share relevant information.

Objectives

91. The objective of an updated compliance and enforcement framework prescribed in legislation is to:

    a. provide the surveillance agencies with an increased, and more practical, ability to enforce compliance with the TICA; and

    b. include a formal escalating enforcement process for responding to minor breaches of administrative requirements (to be dealt with by way of a breach notice), through to instances of serious non-compliance, with the existing High Court process available as an option of last resort.

92. If these objectives are met, it is more likely that government will be able to effectively respond to non-compliance. It is also more likely that network operators will comply, as these obligations should increase awareness of the obligations and requirements to comply with the TICA at the Board and Chief Executive level within many companies.

Proposal – compliance and enforcement

Administrative requirements

93. It is proposed that there be administrative requirements imposed on network operators to enable surveillance agencies to gather important information and data pertaining to the network operators' size and obligations, and to ensure compliance.

94. The specific administrative requirements proposed are listed below.

Proposal	Purpose
Registration: All network operators (and service providers deemed in to interception capability obligations) register with government, and provide specified information relating to interception capability and network security.	Ensure government has key information relating to those telecommunications companies, so it can be sure of the level of obligation for individual operators.
Self-certification: network operators that authorised agencies consider may be avoiding (or only partially) complying with their obligations be required to have the network operator director confirm: 1. adequate resources are allocated to comply with TICA obligations, they maintain and operates interception capabilities, and that to the extent within the company's control, they comply with the TICA, and 2. where they are not compliant, and whether the company is in the process of seeking an exemption.	Incentivises compliance by network operators and brings the obligations under the TICA to the attention of directors (which may not otherwise happen).
Have someone with security clearance: all network operators (and service providers deemed in to interception capability obligations) employ, within their company, someone who has, or is in the process of, obtaining secret level government sponsored security clearance. Exception for companies with under 10,000 end users, [Information withheld]	Allow authorised agencies to serve a warrant trusting that all information pertaining to that warrant and the subsequent interception will be kept confidential.
Compliance testing: allow authorised agencies to initiate end-to-end compliance testing for interception obligations. **Right to request entry and inspection**: power for a designated officer from a surveillance agency to request entry and inspection for interception compliance purposes: • enter a place owned by, or under the control of, a telecommunications company, in which there is a reasonable expectation of documents, information and/or equipment related to obligations under the TICA; and • examine, copy, any document, information, equipment and/or system, where the documents information, equipment and/or systems are relevant to interception capability obligations under the TICA. • Employees of the telecommunications company required to give all reasonable assistance to allow exercise the above powers.	Measure levels of compliance with both interception and security requirements. Assures compliance in advance of a specific operation in cases where they have an operational/strategic interest.

Minor breaches of administrative requirements

95. It is proposed that the TICA specify what counts as a minor breach, which would include:

    a. failure to respond, within the statutory timeframe, to the requirement of registration (including failure to provide one of the component parts of the registration, such as specified information)

    b. failure to comply with a request for self-certification;

    c. failure to comply with a request for information under the TICA;

    d. failure to respond, within the statutory timeframe, to a request by government to participate in compliance testing, or unreasonable refusal to participate in testing;

    e. failure to respond, within the statutory timeframe, to a request by government to enter and inspect or to facilitate entry; and

    f. other breaches of the standards which agencies find appropriate to deal with by way of breach notice in the first instance.

96. Breaches falling into this category would need to involve straightforward issues of fact, and be considered at the minor end of the scale (in terms of gravity and impact).

97. The enforcing agency would send a notice of breach to a network operator, setting a defined period of time within which the operator must comply (for example, 10 working days), and advising that if the company does not respond within that period, the breach will become *deemed non-compliance* and be dealt with through the process for serious non-compliance.

Serious non-compliance, including deemed non-compliance

98. It is proposed that the TICA also specify what counts as serious non-compliance, which would include:

    a. non-compliance with interception capability or intercept accessibility obligations;

    b. non-compliance with mandatory interception standards and failure to assist; and

    c. *deemed* non-compliance (that is breaches of administrative requirements that continue to not be complied with after the notice of breach, and period allowed for rectifying the breach).

99. For actual or deemed non-compliance, the enforcing agency would send a notice of serious non-compliance to the network operator, advising that they will initiate High Court proceedings under the TICA, in which they will seek a compliance order and penalties if that order is breached.

100. The compliance order and, if breached, pecuniary penalties (maximum of $500,000, and $50,000 per day for so long as the breach continues), would remain available for serious non-compliance as is the case today for both arbitration (see the proposal in paragraph x below) and in the High Court.

101. At any point in the enforcement process the agencies could either work with the network operator to achieve compliance, exercise their rights for compliance testing, entry and inspection, or pursue the formal enforcement process of High Court proceedings.

No reimbursement in cases of actual non-compliance with interception obligations for operational costs of assistance

102. In addition to the compliance and enforcement process above, it is proposed that in cases where non-compliance has impacted on the agencies' ability to carry out an authorised interception (for example, an agency has had to use its own equipment and expertise), then the non-compliant provider would:

    a. not be entitled to seek reimbursement for the costs of any assistance they provided (as they are currently able under section 18); and

    b. be required to reimburse the agencies, on a cost recovery basis, for additional costs to the agencies for the interception, directly arising from its non-compliance.

103. For the avoidance of doubt, this provision would not apply to any non-compliance with security requirements (given there is no payment for operational costs in the first instance).

Arbitration in cases of serious non-compliance (not recommended)

104. To provide for a faster enforcement process, where the decision-maker would have greater specialist expertise, the option of providing the agencies with the ability to go to arbitration under the *Arbitration Act 1996* in cases of serious non-compliance was considered.

105. The arbitrator would have had the same ability as the High Court to impose a compliance order, and pecuniary penalties where a network operator breaches the compliance order.

106. The intention of allowing an arbitration process was to allow government and network operators to work through differences without the publicity of the High Court, and to have another step in the escalation process before going to Court. However, arbitration is used to deal with disputes rather than issues of non-compliance, so the proposal is not suitable.

Benefits and costs of compliance and enforcement frameworks

107. The anticipated benefits and costs to both government and industry from the compliance and enforcement frameworks are detailed in the table below.

	Government	Industry
Benefits	• Escalating enforcement regime gives government practical means to enforce compliance [Information withheld]	• [Information withheld •]
Costs	• Cost for government of taking a network operator to the High Court [Information withheld]	• There may be a cost to network operators if enforcement action is taken against them for non-compliance. This is likely to be minimal but is appropriate if in breach of statutory obligations

108. It is not possible to quantify costs for non-compliance with lawful interception obligations, as non-compliance puts into jeopardy the ability of surveillance agencies to enforce the law and guard against national security threats. These are a public good, fundamental to a well-functioning society, and a cost cannot be put on them. However, the costs for inability to exercise interception range from (at the lower end) additional operational costs for Police in an investigation to get evidence by other means, to (more serious) the inability to combat cyber threats to the economy or critical infrastructure.

109. As there are no business reasons for network operators to invest in interception capability, they are doing it solely to comply with their TICA obligations. Therefore, the government should make commensurate investment when needed, to help industry meet their obligations equitably and continue to comply with the TICA.

Risks

Exposure of weak points in the network (lack of interception capability)

110. [Information withheld

111.

112.

113.

114.

]

Net impact

115. Overall, having a compliance and enforcement framework will allow surveillance agencies to ensure that network operators are complying with their obligations, and gives them a means to check compliance, and , when necessary, to take appropriate enforcement action.

116. For network operators, this framework will give clarity about what is expected of them, and should increase compliance. Having a graduated enforcement regime will make it more likely that compliance will be enforced, thereby creating a more level playing field between operators of similar sizes, and increasing competition.

117. This option meets all of the objectives stated in paragraph 24.

Part three

Conclusions and recommendations

118. The Ministry of Business, Innovation and Employment recommends that:

    a. The proposal to have a multi-tiered framework by layer does not proceed

    b. The proposal to have a risk-based framework by type of service offered and the number of end users proceeds

    c. The compliance and enforcement framework, as described in part two, proceeds in its entirety.

Implementation

119. All "network operators" have interception obligations today, and with the exception of infrastructure-level providers will have some form of obligation (whether it is to be intercept capable, intercept ready or intercept accessible) under the new scheme. It is proposed that the amendments to interception obligations would only come into force 6 months after assent, to allow companies to familiarise themselves with, and prepare for, their revised obligations.

120. A period of 6 months is proposed, as in most cases where a company obligations change, this will be a reduction in the cost and complexity of meeting the obligation (or else removal of the obligation to have interception capability). In this 6 month period, today's interception capability obligations would continue to apply.

121. However, two exceptions are proposed, namely:

    a. the registration requirement would come into force immediately; and

    b. the updated exemption process, and the ability to apply for exemptions would also come into force immediately, to ensure that there is not a back-log of applications to process immediately after the new Act comes into force.

Monitoring, evaluation and review

122. At this stage there is no plan do undertake any formal review or evaluation after implementing the legislation. Officials will monitor the operation of the provisions and report to relevant Ministers if any issues arise.

Part four

Industry consultation

123. The proposals in this paper were finalised following feedback from [i.a.] telecommunications companies of varying types and sizes, on a detailed technical consultation paper. The initial interception proposals in the consultation paper were developed following a series of industry workshops which identified problems with the current interception scheme, and initial costings and feedback on options for change.

124. [Information withheld

]

125. [Information withheld]

Departmental consultation

126. This Regulatory Impact Analysis paper was developed with New Zealand Police, the New Zealand Security Intelligence Service, the Government Communications Security Bureau, and the National Cyber Policy Office (DPMC). The Treasury was consulted. The Ministry of Justice, Ministry of Foreign Affairs and Trade and the Privacy Commissioner were consulted on the proposals in this paper. New Zealand Customs and the Department of Internal Affairs were informed of the proposals in this paper.