Submission by the New Zealand Telecommunications Forum on the Telecommunications (Interception Capability and Security) Bill.

Introduction

1. This submission is made by the New Zealand Telecommunications Forum Inc. (**TCF**). TCF members provide more than 90% of the internet and voice connections in New Zealand.

2. The TCF appreciates the opportunity to comment on the Bill and would like to appear before the Select Committee in support of its submission.

3. TCF members today have significant obligations under the Telecommunications (Interception Capability) Act 2004, enabling surveillance agencies to carry out the lawful interception of telecommunications under an interception warrant or other lawful interception authority.

4. The TCF supports the review of the existing obligations, particularly to ensure that the regime remains effective in crime detection and prevention. The regime must keep pace with rapidly developing technologies and changes in communication methods, and impose obligations fairly and effectively across all communications providers – whether the operators of networks, providers of retail services or "over-the-top" providers. For the regime to be effective, the same level of interception must apply.

5. The TCF recognises that secure and resilient infrastructure will be central to the protection of New Zealand's social and economic interests, and those of the nation as a whole. It is also important to New Zealand's national, economic and security interests.

6. This submission sets out its members' collective views on the key areas of this proposed legislation, Interception and Network Security, that the TCF considers should be given further consideration and amended to best achieve the desired policy outcomes. Individual members may choose to provide their own submissions on aspects that are of particular importance to them.

1. INTERCEPTION

7. TCF members have current interception obligations under the Telecommunications (Interception Capability) Act 2004. The TCF welcomes the recognition of the impact of interception obligations on the industry, and the attempts to simplify and streamline the obligations on existing providers.

8. The key question to consider is whether the existing interception obligations are likely to meet the purpose of interception.

Telecommunications Users are increasingly using Over-The-Top services

9. Electronic communications are changing rapidly. How people communicate has changed significantly since the passage of the 2004 Act. At that time, voice services were exclusively provided by fixed and mobile telecommunications networks, owned and controlled by the providers who had the duty to intercept voice calls.

10. Today, this has changed, and we expect this to accelerate. Increasingly, voice services are provided over broadband data circuits. Examples include Skype and Viber services. For example, global trends show the impact:

- Teleography has estimated that Skype now carries over a third of all international voice minutes.[1]
- Informa Media and Telecoms estimates that Over-the-Top (OTT) messaging traffic will be at least double traditional SMS traffic this year.[2]

11. OTT commonly describes delivery of content where a network operator is not involved in the control or distribution of that content. The network operator may be aware of the passage of IP packets, but the content is delivered to an end user direct from the OTT provider, using the network operator solely for the transportation of the data packets without any necessary knowledge of the content or the service provided.

12. This presents two key challenges in the effective use of interception:

- Limiting the obligations to traditional network providers only leaves a considerable hole in the regime's effectiveness – a problem that will only get more acute.
- OTT applications are not always controlled locally, but rather globally.

13. The Bill appears to partially recognise these issues by:

- Extending the Act to allow for OTT providers to be captured under the Act under the definition of "service provider";
- The Minister, by directive, can impose greater obligations on OTT providers in the future; and
- Extending the right for the Minister to extend the Ministerial Direction relating to resold overseas telecommunications services.

14. However, TCF members do not consider that the Bill goes far enough to ensure that all traffic is readily interceptable, for security agencies to achieve their outcomes.

RECOMMENDATION ONE: Obligations should automatically extend to cover all OTT providers

15. To be effective, the legislation must include OTT providers automatically. It is not satisfactory that OTT providers will be covered under the Act if security agencies request that the Minister issue a Directive to increase the interception obligations to those of network operators.

16. Section 9 of the Bill requires that Network Operators have a duty to have full interception capability.

17. Given the prevalence, both now and increasingly in the future, of OTT services, the same obligations as faced by network operators should apply today. TCF members do not consider that taking a 'wait and see' approach is appropriate. We consider this to be a preferable approach that puts the onus on OTT providers to demonstrate why an exemption

[1] http://www.telegeography.com/research-services/telegeography-report-database/index.html

[2] http://blogs.informatandm.com/12861/news-release-ott-messaging-traffic-will-be-twice-the-volume-of-p2p-sms-traffic-by-end-2013/

for their services are appropriate, and do not undermine the effectiveness of the interception regime.

18. Instead, OTT players should face the same obligations as network providers if interception is to be effective. OTT providers should then have the option to seek an exemption, evaluated on its merits (per subpart 4). As we discuss later in our submission, consideration of exemptions could be considered through a New Zealand Technical Advisory Board.

19. Alternatively, the Bill should set out that network operators do not have any obligations in lieu of the OTT service provider in relation to an OTT service. The duty on the network operator ought to be only to assist the OTT service provider to comply with their obligations. Either the OTT service is covered therefore by obligations on the OTT service provider, or the OTT service is not covered at all.

20. At the very least, if a network operator resells OTT services, the obligations on the network operator should be reduced to reflect the fact that the network operator has little control over the OTT service, eg the interception obligation should only extend to access based interception, or to the extent granted to the network operator by the OTT service provider.

21. The TCF notes that one of its members, namely Vector Communications, does not support Recommendation One. Vector may address such concerns in an individual submission.

Ministerial directions and regulations

22. The Bill introduces the Directive process, covering both Interception and Network Security, where, on the advice of a security agency, the Minister can issue a direction that could compel a TCF member to:

- Impose increased interception capability requirements above that ordinarily required under the Bill (Subpart 5); or
- Impose specific requirements regarding network architecture or vendor selection.

23. As discussed above, the TCF considers that interception capability requirements should apply equally to all providers (unless an exemption is granted) with lower obligations imposed on very small operators.

24. While TCF members appreciate the underlying purpose of Directives, the Bill as currently drafted can impose significant risk and potential financial impacts on providers if a Directive was issued, under a somewhat arbitrary process. It is essential that any request for a Directive is appropriately considered, tested and consulted upon.

25. Subpart 5 sets out the process where a surveillance agency seeks a Directive from the Minister. While the scope of a directive is limited to a service that can *adversely affect national security or law enforcement* (section 35(2)(a)), consultation and transparency is currently extremely limited, in our members' view.

26. A surveillance agency must notify an affected service provider of its application to the Minister (section 35(3)) to allow the opportunity to make a submission to the surveillance agency. However, as currently drafted, there is no obligation to provide the grounds or basis for the requested Directive – making meaningful consultation impossible.

27. Section 35(7) sets out that the Minister must take into account four factors:

(a) whether the current level of interception capability *adversely affects national security or law enforcement*;
(b) the impact of compliance costs on the provider;
(c) whether it would unreasonably impact the provision of services, or hinder the introduction of new services; and
(d) any other matters.

28. The Minister is required under section 35(8) to give primacy to 35(7)(a).

29. The TCF is concerned that such information would be withheld from the affected service provider on the basis of security concerns. As a result, an affected service provider has limited opportunity to submit on a proposal put forward by a security agency that has the benefit of all the information.

30. This then places the Minister in the invidious position of having to consider a recommendation that has not had the benefit of full consultation and views from the impacted party. It relies on the Minister taking, on trust, the views of the security agency.

31. The TCF accepts that the Government must balance the need for secrecy of security information relating to national security threats, and the rights of impacted service providers. However, we consider that the opportunity to have constructive input into the decision making and consultation process is unnecessarily and inappropriately limited.

32. As currently drafted in the current Bill, potentially impacted service providers face the following challenges:

- Security agencies are only required to advise a potentially impacted service provider of a Directive application. There is no obligation to provide the application or the grounds for the request.

- The Minister is required to give primacy to the question of whether the current level of risk affects national security or law enforcement – issues which are likely to be withheld on the basis of secrecy. Potentially impacted service providers will not be in a position to weigh up the competing priorities.

- The Government has little incentive to consider the financial impact on the impacted service provider. TCF members recommend that the Government should compensate providers for any additional costs as a result of a Directive.

- Appeal rights are limited to judicial review. And yet, impacted providers have limited ability to be consulted or participate in the decision making process.

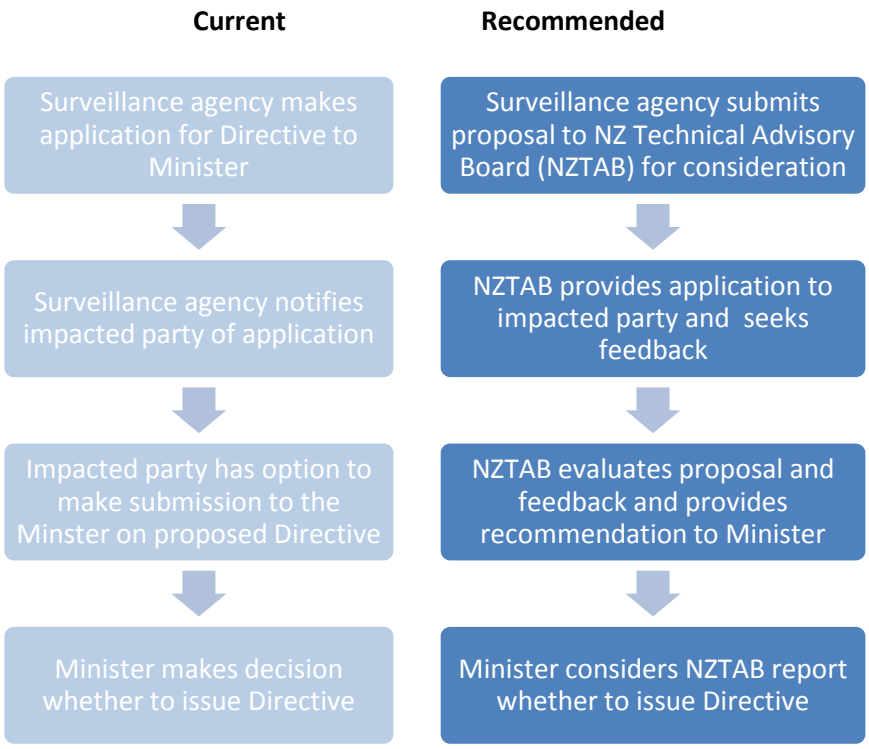
RECOMMENDATION TWO: A joint industry/security technical advisory Board should be established to evaluate any application for a Ministerial Directive

33. The TCF recommends that additional protections are put in place, relating to the issuing of Directives. We consider that an additional step in the process between the security agency

and the Minister should be inserted into the consideration process, to appropriately address these concerns. We consider that the UK approach achieves this well.

34. An independent expert panel should consider any Directive proposal from a security agency, and submissions from impacted parties, before providing its recommendation to the Minister. The independent panel would be balanced by an equal number of security-cleared security specialists from telecommunications providers and representatives from security agencies. The panel should also have an independent chair. All participants would have secret-level government-sponsored security clearance.

35. We consider such an approach would better ensure that security concerns are addressed, both from the perspective of the security agencies, but also the perspective of the network providers. It would also ensure that the Minister receives a balanced view of the risks and impacts. This is best illustrated in the table below:



36. Notwithstanding the creation of the above, the TCF supports the basic concept that any party potentially affected by a Ministerial direction should have the right to engage directly with the Minister and/or the security service involved.

The UK Technical Advisory Board

37. The UK has taken such an approach. We consider that the New Zealand Technical Advisory Board could be modelled on the Technical Advisory Board in the UK.

38. The UK Technical Advisory Board (TAB) has 6 members from the communications industry, 6 from government intercept agencies and a neutral chair. Members are appointed by the Home Secretary. [3]

39. The TAB advises the Home Secretary on whether the obligations imposed on communications service providers (CSPs) under the terms of Regulation of Investigatory Powers Act (RIPA) are reasonable. The TAB is an advisory non-departmental public body of the Home Office.

40. The TAB advises on obligations placed on CSPs including:
- the obligation to maintain interception capability; and
- the obligations and exemptions listed in their legislation.

41. The TAB also manages appeals from CSPs on notices they consider unreasonable, and advise the Home Secretary on each case.

Subpart 4 – Exemptions

42. The TCF supports the simplified Exemption process set out in SubPart 4. When considering an exemption, the designated officer must consider:

(a) national security or law enforcement interests;
(b) the number of customers or end-users of the relevant service
(c) the cost of compliance
(d) whether compliance could be achieved appropriately by another means; and
(e) any other matter the designated officer considers relevant.

43. While the reasons for the decision must be set out in the decision, except for those parts of the reasons that would reveal classified information (section 32(4)), the consultation requirements remain unclear. Similar to the issues discussed above on security agencies' application for a Ministerial Directive, similar risks around meaningful consultation apply.

RECOMMENDATION THREE: A technical advisory Board should evaluate requests for Exemptions.

44. A technical advisory Board, comprising of both industry security representatives and agencies would be able to effectively act as the designated officer proposed under the Bill. This would not only balance information asymmetries between security agencies and network providers, but also network providers could provide technical leadership to consider whether compliance could be achieved appropriately by another means (a requirement of the designated officer under section 32(1)(d)).

45. Similarly a technical advisory Board could consider and make recommendations to the Minister in respect of class exemptions under section 34 of the Bill.

[3] See www.gov.uk/government/organisations/technical-advisory-board

Subpart 5 – Ministerial Directions

46. Subpart 5 sets out that the Minister may require service providers to have the same obligations as network operators in respect of interception capability, where the Minister receives a recommendation from a surveillance agency.

RECOMMENDATION FOUR: Network Operators and Service Providers should have the same obligations, with the option for Service Providers to seek Exemptions through the Technical Advisory Board.

47. As discussed above, the TCF considers that limiting the obligations to traditional network providers will undermine the regime's effectiveness, and the current 'gap' that will only become more acute over time. For that reason, the Bill should provide similar obligations for all network and service providers.

48. Service providers should then have the option to seek an exemption to the obligations, through application under Subpart 4, through consultation with the technical advisory Board.

49. The benefits of this approach are:

- Providers of telecommunications services are required to demonstrate to an expert panel that the exemption of their service does not undermine security
- Surveillance agencies get the technical understanding through the technical advisory Board
- Risks of gaps are minimised, which are only discovered if surveillance agencies identify.

RECOMMENDATION FIVE: Any Directive should be considered thoroughly by the Technical Advisory Board.

50. However, if the directive power under Subpart 5 that the Minister may require service providers to have the same obligations as network providers, the TCF recommends that a joint industry/security technical advisory Board should be established to evaluate any application for a Ministerial Directive, as discussed in paragraphs 33 to 35 above.

Subpart 6 – Formatting

51. The time, effort and cost of TCF members to meet the existing obligations under the existing Telecommunications (Interception Capability) Act 2004 are significant.

52. The TCF supports the potential for efficiency through the standardisation of the information format provided, and clarity around the supply of information. We support the continuing engagement between the agencies and TCF members to ensure the cost and impact on network operators is kept to a minimum. The TCF would be happy to help draft the initial standards for interception under the Bill, based on existing agreements between industry and the agencies. This will likely improve efficiency for all parties concerned.

2. NETWORK SECURITY

53. The Network Security obligations proposed under Part 3 of the Bill are fundamentally new.

54. The TCF members have key concerns relating to these new obligations:

- Insufficient protection, transparency and appeal rights in the Directive process, or imposition of additional obligations; and
- Lack of compensation for additional costs imposed by any Directive.

Disclosure

55. As previously discussed, the TCF recommends the introduction of a Technical Advisory Board to provide advice and recommendations to the Minister. We consider this should include:

- any consideration by the Minister to extend the areas of specified security interest under section 46(3); and
- any consideration of exemption under section 48.

Process for preventing or mitigating network security risks

56. Under section 50, the Director of the Government Communications Security Bureau must assess whether a proposal, if implemented, will prevent or mitigate a network security risk. The Director has the option to:

- accept the proposal; or
- refer the matter to the Minister to make a direction under section 54, and advise the network provider of the decision and consultation timeframe.

57. The issuing of a Directive by the Minister under this section is likely to have significant practical and financial implications on the telecommunications provider. As with interception directives, there are inherent limitations in the consultation and appeal process and asymmetries of information between the GSCB and the impacted provider.

RECOMMENDATION SIX: Any Directive should be considered by the Technical Advisory Board.

58. The current Bill provides extremely limited consultation and appeal rights to a network provider. For that reason, the GCSB should be required to submit its recommendation to a Technical Advisory Board, who is able to appropriately consider and balance the risks, before the recommendation is sent to the Minister.

Conclusion

59. In summary, the TCF recommends that:

a. Obligations under the Bill should automatically extend to cover all OTT providers.
b. A joint industry/security technical advisory Board should be established to evaluate any application for a Ministerial Directive provided under the Bill.
c. A technical advisory Board should evaluate requests for Exemptions.

d. Network Operators and Service Providers should have the same obligations, with the option for Service Providers to seek Exemptions through a technical advisory board.

For information on any aspect of this submission, please contact:

David Stone
CEO, New Zealand Telecommunications Forum
PO Box 302469
North Harbour
Auckland
+64 21 937 879