



Telecommunications (Interception Capability and Security) Bill

Submission | Law and Order Committee

13 June 2013

Executive Summary

Telecom requests the opportunity to be heard in person before the Law and Order Select Committee.

The Telecommunications (Interception Capability and Security) Bill (**Bill**) proposes to amend the Telecommunications (Interception Capability) Act 2004 (**TICA**) to:

- ensure that interception obligations are clear and reflect the changing telecommunications industry structure, do not impose unnecessary compliance costs, and are sufficiently flexible to match today's operational needs and future technology developments; and
- introduce obligations for network operators to engage and co-operate with Government on network security matters where they may raise a risk to New Zealand's national security or economic well being.

INTERCEPTION OBLIGATIONS

Telecom welcomes the review of interception obligations which we agree need updating to reflect a changed industry structure and new technology. There are positive aspects of the Bill however, the following issues with the current interception framework need to be resolved to make this Bill sustainable, efficient, and able to meet its main objectives.

Introduce efficiency in the regime and create a level competitive playing field in New Zealand which fits the changed industry structure and new technologies

The Regulatory Impact Statement suggests that the graduated enforcement regime will create a more level playing field between operators of similar sizes and we agree that strict enforcement is crucial to make the regime sustainable. However, the Bill (which continues to place core interception obligations on network operators alone) does not address the unlevel playing field that currently exists between network operators and non-network operators who are free to offer the exact same services in New Zealand without any interception obligations in respect of them. Interception obligations usually introduce increased cost to a service, delay in the time it takes to get a service to market, and can prohibit the introduction of a service altogether where no technical interception capability exists.

Network operators today often resell third party's services which run over the top of network operators' networks (i.e. "over the top services¹"). Telecom, for example, resells Yahoo and Microsoft email service and our customers are asking us to resell Microsoft's cloud-based communications service Office 365. Network operators are

¹ The term "over the top service" is commonly used to describe the delivery of content where a network operator is not involved in the control or distribution of that content. The content is delivered to an end user directly from the over the top service provider, using the network operator solely for the transportation of the data packets without any necessary knowledge of the content or the service provided at any one time.

not involved in the development of these services; we do not control the distribution of the content, and we make much smaller margins on such services. Despite this, network operators are asked to provide interception capability in respect of these services when we resell them. In contrast, where these over the top services are offered to the market directly by the owner of the over the top service itself (e.g. Google), no interception capability is required. This leaves network operators in the invidious position of having to create interception capability for a service even if the operator of that service does not provide such capability. This results in an anticompetitive outcome between competitors, as well as gaps in the surveillance agencies' ability to combat crime due to instances of the service being offered to the market by providers (i.e. non-network operators) who do not have to have interception capability over it.

Despite the clear issues with the current approach, and the fact that over the top services are increasingly prevalent, the Bill continues to place the core interception obligations on network operators alone pursuant to section 9. This approach is unsustainable and inadequate. Over the top communications services are a significant and rapidly increasing part of our communications sector. Many of the larger providers of over the top communications services have New Zealand subsidiary companies and offices – in the same way as Vodafone New Zealand is a subsidiary of Vodafone Group. We see no good reason why they should be treated any differently to providers of network-based communications services.

While it is very difficult to estimate exact usage of these cloud-based services, due to little or no subscriber or traffic reporting by these providers, there is ample evidence that they already carry a meaningful share of communications traffic in New Zealand, and that this share is growing quickly:

Voice calling

- It is estimated that Skype carried over one-third of global international (cross-border) call minutes in 2012². Most of this traffic used the free Skype-Skype calling service, but Skype's chargeable SkypeOut service is also growing rapidly. In New Zealand, for example, we estimate that SkypeOut alone currently accounts for at least 20 million minutes of inbound international minutes per year. Projecting global estimates of Skype's total market share for international calling minutes, this suggests the free Skype-Skype service could be carrying over 200 million minutes of inbound calling minutes to New Zealand.
- Despite continued year-on-year connections growth, and increasing amounts of bundled minutes in mobile plans, call minutes in the New Zealand mobile market have been dropping each year since 2009. Our conclusion is this counter-intuitive effect is driven by increasing substitution from cloud-based services. Network data from December 2012 showed that on any day in that month almost 60,000 distinct Telecom mobile subscribers used viber (a cloud

² Telegeography Report, <http://www.telegeography.com/research-services/telegeography-report-database/index.html>

based mobile VoIP operator), and 21,000 used Skype for mobile. By May 2013, the number of Telecom subscribers using viber on any given day had increased 25% to 78,000 and the number using skype for mobile had increased 50% to 32,000.

Messaging

- In 2011, cloud-based messaging traffic exceeded traditional network-based SMS traffic. In 2013, it will more than double it.³
- In New Zealand, we have little concrete evidence of traffic or market share numbers. However, Telecom network data supports the global evidence. In May 2013, 150,000 Telecom mobile customers used Apple's iMessage service, 140,000 used facebook messenger, 35,000 used Microsoft live messenger, 25,000 used googletalk and 23,000 used WhatsApp messenger.

Telecom proposes several alternatives for a more sustainable regime which achieves the key objectives of the Bill. To be clear, Telecom believes that the Bill's objectives will not be achieved without implementing the proposed alternative approaches. The key underlying principle for each alternative is to place the obligation to develop interception capability for an over the top service on the owner, operator or provider of those services (for example, Microsoft or Google who are the service or application providers) before it can be provided in New Zealand, and removing that obligation from network operators who have no true control over the service, and/or other resellers of those over the top services.

Reduce unnecessary compliance costs and focus on operational importance

We welcome the improvements to the exemption regime. However, the broad application of the definition of "telecommunications service" results in inefficiency where agencies require (often very expensive) interception capability over a service which in practice is not likely to be intercepted on a frequent basis.

We appreciate the difficulties with publicly disclosing the services that will not have interception capability. Therefore, we propose that agencies either confidentially notify operators which particular services must be capable of interception (consistent with the UK regime), or provide the designated officer with a list of types of services that the agencies consider to be of operational importance (e.g. mobile and fixed voice, email, text and instant messaging services), with an ability to add to that list as required. The operational priority list must then be expressly considered when an exemption request is being considered (i.e. if the service which is the subject of an exemption request is not on the list, an exemption for it should be granted).

NETWORK SECURITY

Ensure a proper balancing of interests

³ Informa Telecoms & Media estimate, <http://blogs.informatandm.com/12861/news-release-ott-messaging-traffic-will-be-twice-the-volume-of-p2p-sms-traffic-by-end-2013/>

Telecom, as does any responsible provider of major infrastructure, already considers and takes all reasonable steps to protect its network and its customers' information. We are concerned with the ability for Government to intervene with commercial activities and procurement decisions without any true impartial balancing of commercial and Government interests.

To address this issue, Telecom proposes that where Government puts a network operator to extra expense to go above and beyond what the operator considers is secure from a commercially acceptable point of view (i.e. standards that its customers are satisfied with), Government should subsidise half of the cost of that additional expense. Where normal commercial practice is deemed unsatisfactory for national security reasons, the cost of that decision must be shared – it cannot be lumped onto an organisation.

To further ensure that commercial and Government interests are properly balanced, Telecom proposes that before any direction power is exercised by the Minister, there should be consultation with, and a recommendation from, a technical advisory board made up of equal numbers of national security cleared technical experts from both the telecommunications industry and government agencies. This will ensure the Government gets independent technical expertise and advice in order to enable it to properly assess a network operator's network and the steps that should be taken to proportionately mitigate a perceived national security risk.

Due to the significant adverse consequences of the exercise of a direction power, the affected network operator should have an ultimate right to appeal the exercise of the Ministerial direction to an arbitrator who must consider submissions from the network operator, surveillance agencies, and the technical advisory board.

Clarification of retrospectivity, and notification obligations

Clarification is required to ensure that there is no ability for Government to retrospectively use the direction power for national security purposes unless Government pays the associated costs of doing so. For example, if a network decision was previously approved under the notification regime but new information comes to light which raises new national security concerns with that previously approved decision, the network operator will not be put to any expense to mitigate the newly perceived security risk. This is required to give network operators certainty over investment in their network.

Finally, in order to make the network security provisions of real operational use to Government, we consider that the situations in which engagement and notification is required be narrowed and clarified.

Telecom's submission

PART ONE: LAWFUL INTERCEPTION OBLIGATIONS

We address our main concerns upfront and suggest some potential amendments to the relevant provisions in the shaded boxes, to illustrate how our alternative approaches would operate. We also suggest some further specific amendments to the Bill at Appendix A.

Introduce efficiency in the regime and create a level competitive playing field in New Zealand which fits the changed industry structure and new technologies

If the Bill continues to place primary interception obligations on network operators rather than addressing over the top services directly, it will not result in the most efficient and effective way to ensure interception capability. In this day and age it is not realistic or sustainable to expect network operators to have the full responsibility to intercept over the top services that they do not have control over rather than enforcing against the application provider of those services themselves who do have control over those services.

The current approach fails to level the competitive playing field to ensure that network operators (e.g. Telecom and Vodafone) are not delayed or prevented from offering a service, or are forced to offer a more expensive service than their competitors, due to interception obligations which do not apply to other providers of the same service in New Zealand (e.g. non-network operators). This situation arises particularly where the network operator is merely re-selling a third party's over the top service which, because it operates a network, the network operator must be able to intercept, whereas their non-network operating competitors (or the application provider itself) do not face interception obligations for selling the exact same service to the New Zealand market. For example, with an over the top Microsoft service like Office 365, network operators (like Telecom and Vodafone) who resell the service will have to ensure that the service has interception capability under section 9 because they operate a network. However, if a retailer that does not operate a network (or Microsoft itself⁴) sells the software package directly to a customer in New Zealand they will not have to ensure the service is capable of interception which means it is available to customers without any capability to intercept it.

Telecom does not consider that the Minister's discretionary ability to deem-in a service provider, or the designated officers' ability to exempt network operators from interception obligations for particular services, will be implemented in a way that resolves this issue. Telecom appreciates that a discretionary approach is required from Government on a service by service basis to avoid barriers to innovate and offer nascent technology to the New Zealand market. However, there needs to be a key principle contained in the Act itself to place the obligation to develop interception capability for an over the top service on the owner or true provider of those services (for example, Microsoft or Google as the application provider) before it can be

⁴ Telecom considers that the likes of Microsoft are already network operators with interception obligations but to ensure enforcement against them, their obligations should be clarified.

provided in New Zealand (as that is the most efficient place for the obligation to sit due to the application provider's level of control over and access to the service). The obligation should be removed from network operators who have no true control over the service and/or other resellers of those over the top services. Where a service is available to the New Zealand market without interception capability network operators should not be prevented from competitively offering that same service to the same market due to interception obligations.

Achieving a more sustainable and effective regime and introducing a level playing field in the New Zealand telecommunications market could be achieved through the following alternative options:

- Option A – clarify that the providers of over the top services are network operators with interception obligations
- Option B – remove interception obligations for all network operators where the service is otherwise available in New Zealand without interception obligations and rely on the duty to assist
- Option C – improve the proposed deem-in process so there is incentive to enforce it
- Option D – place an obligation to develop interception capability on the true provider (e.g. Microsoft/Google) of over the top services (Telecom's preferred option)

These options are described in detail below:

Option A – clarify that the application provider of over the top services are network operators with interception obligations

Where the service is an over the top service, the obligation to have full interception capability should be placed on the application provider of that service, and removed from other network operators who will be left with a duty to assist with interceptions.

- Amend the definition of "public data network" to ensure beyond doubt⁵ that it captures the application provider of over the top services to be provided in New Zealand. Add a new subparagraph (iii) as follows–
(iii) Facilities for uploading, transmitting, sharing or retrieving information.
- New section 29A – exemptions in relation to over the top services
(1) In relation to an over the top service, network operators and service providers (other than the application provider of the service) are exempt from any interception capability obligations for that service, and may

⁵ Telecom considers that the application providers of resold services already satisfy the definition of "network operator" but considering they are not currently enforced against, we consider that the Bill could be further clarified.

continue to provide an over the top service unless it is contrary to a direction made under section 39.

(2) Nothing in this section affects the duty to assist on network operators and service providers under section 24.

- Add the above definitions of "application provider", "over the top service", and "technical modification".

Application providers would have the same graduated interception obligations, and ability to seek and receive exemptions from those obligations, as other network operators.

Option B – remove interception obligations for all network operators where the service is otherwise available in New Zealand without interception obligations and rely on the duty to assist

In order to address the inefficiencies and unlevel playing field that currently exist with the Bill, where an over the top service is available in New Zealand without interception capability (i.e. where the Minister has not "deemed-in" the application provider of an over the top service), network operators should be exempt from interception obligations for that service with reliance instead on the duty to assist surveillance agencies only (i.e. the network operator will be required on a best endeavours basis to intercept the access service on any fixed access line, or against any mobile handset).

If Government is not willing to place interception obligations on the true application provider of an over the top service, where it is most efficient and sustainable to do so, in order to level the competitive playing field, it cannot leave the interception obligation on network operators alone. The anti-competitive outcome of doing so demonstrates the policy issues with the approach in the current interception regime.

Option C – improve the proposed deem-in process so there is incentive to enforce it

The proposed deem-in provisions require amending to ensure that there is incentive for the Minister to enforce interception obligations against the application provider of over the top services being provided in New Zealand (i.e. where those obligations most efficiently and effectively sit).

This can be achieved through a requirement to deem-in a service provider⁶ to have interception capability obligations, where it is more efficient for them to provide the interception capability than someone else due to their level of control over and accessibility to a service. This would need to be coupled with the removal of an interception capability obligation on the other providers of

⁶ Telecom considers that the application providers of resold services already satisfy the definition of "network operator" but considering they are not currently enforced against, we consider that the Bill could be further clarified.

the service, with reliance instead on the duty to assist obligations on those other providers.

- Section 35 – Minister may require service providers or application providers to have same obligations as network operators

(6A) The Minister must make a direction (and subsection 6(b) does not apply) where the Minister believes on reasonable grounds that it is more efficient for the application provider of an over the top service being provided in New Zealand to intercept the service due to the application provider’s level of ownership, control or operation of the service.

(6B) Where the Minister has made a direction under section 6A, the [Minister or designated officer] must exempt network operators or service providers reselling that same service from any interception obligations (other than the duty to assist).

- Add the above definitions of “application provider” and “over the top service”.

Option D – place an obligation to develop interception capability on the application provider (e.g. Microsoft/Google) of over the top services

Impose an obligation on the owner of over the top services to be provided in New Zealand to ensure that the service has full interception capability before it is offered to any service provider, network operator, or directly to any end user in New Zealand. For example, before Microsoft can provide a new VoIP service in New Zealand there must be a function of that service that network operators, service providers, or Microsoft itself, can use to intercept the service when it is offered in New Zealand at no additional expense to the network operator.

Network operators would have a duty to assist the application provider of the service in implementing the interception capability at the application provider’s expense (i.e. on a commercial basis), and network operators and service providers would have a duty to assist the surveillance agencies with actually executing an interception (under section 24).

Where the application provider fails to develop interception capability:

- The agencies could implement the enforcement regime against the application provider; or
- The designated officer could grant an exemption for the service; or
- The Minister could make a direction that the service cannot be offered in New Zealand by any service provider, network operator or the application provider itself (under an amended section 39 power); but

- A network operator will not be solely prevented from offering a service without interception capability where it is otherwise available for sale to end-users in New Zealand without interception capability; and
- Network operators and service providers will still have a duty to assist with the interception of the service on a best endeavours basis.

This approach would require the entity with the actual control over the service to develop a capability when it develops the service which is far more efficient and cost effective and would mean that all instances of the service provided in New Zealand will have interception capability. Further, it would mean that the cost of interception capability is incorporated into the service and is, therefore, shared across the industry rather than falling on network operators alone.

- New section – duty on the application provider of over the top services provided in New Zealand:
 - (1) Where an application provider provides (either directly or indirectly) an over the top service to end-users in New Zealand, the application provider must ensure that the service has full interception capability prior to it being offered in New Zealand by a service provider, network operator, or the application provider itself.
 - (2) The application provider may require a network operator to assist (on reasonable commercial terms to allow the network operator to recover its costs) with the development or implementation of the interception capability (and that network operator has a corresponding duty to assist as though assisting a surveillance agency under section 24(3)) or may otherwise co-ordinate, share or contract for services to meet any part of its obligation under subsection (1) pursuant to section 27.
 - (3) Nothing in this section affects a network operator’s or service provider’s duty to assist surveillance agencies under section 24.
 - (4) An application provider of an over the top service must not charge any person, directly or indirectly, for the costs of anything that the application provider does to meet the requirements of subsection (1) (including requiring a network operator to assist under subsection (2)), unless the application provider imposes the same charge on every person to which the application provider provides the service in New Zealand.
- Amend section 27 – network operators may share resources:
 - (1) Nothing in this Act prevents any person from co-ordinating, sharing, or contracting with another person for interception services (whether equipment or staff, or the execution of a warrant) in order to meet the requirements in the Act.
 - (2) However, any arrangement referred to in subsection (1) does not affect any obligations that apply to the person that have been imposed

by or under this Act, and the primary obligation under this Act remains on that person.

- New definition of “application provider” –

(a) A person (based in New Zealand or overseas) that provides application layer software and/or hardware that enables an over the top service supported by that application to be provided to end-users in New Zealand (whether directly or indirectly or by wholesale or retail).

- New definition of “over the top service” – a telecommunications service which runs over a network operator’s network and:
 - Is a purely resold telecommunications service; or
 - Is provided to the end user by the application provider or another service provider.
- New definition of “technical modification” – includes a technical modification to the service other than through customisable options offered by the application provider of that service to resellers generally.

- New section 29A – exemptions in relation to over the top services

(1) In relation to an over the top service, network operators and service providers (other than the application provider) are exempt from any interception capability obligations for that service, and may continue to provide an over the top service unless it is contrary to a direction made under section 39.

(2) Nothing in this section affects the duty to assist on network operators and service providers under section 24 or [new section above that allows the application provider to require network operators to assist].

(3) An application provider of an over the top service may apply for and/or be granted an exemption under sections 29 and 30, and those sections apply as though the application provider was a network operator.

Focus on telecommunications services that are of operational importance

Telecom’s other main concern with the existing interception regime (which is not satisfactorily addressed by the Bill) is the unnecessary expense arising from the broad application of the definition of “telecommunications service” and the previous exceptions approach to exemptions. These factors have resulted in network operators spending significant amounts of money to make a service intercept capable where an interception is not ever likely to be carried out over it (i.e. where the service is of no operational importance). This is an inefficient and unsustainable approach to interception as network operators are being put to significant expense to make services capable of interception but a large number of those services are not of any significant operational importance to surveillance agencies’ ability to combat crime.

Alternative options to address this issue include:

Option A – introduce an approach more consistent with the UK

Interception obligations in the UK are limited to telecommunications services which are offered to a substantial section of the public in the UK. Any persons who are providing, or propose to provide, public telecommunications services can be compelled by order of the Secretary of State to provide some form of interception capability for a service. Before the Secretary of State can make an order compelling someone to provide interception capability the Secretary of State must consult with (among others) the Technical Advisory Board (which is constituted to represent a balance between the surveillance agencies and the telecommunications industry). Government then contributes a fair contribution to the cost of implementing the interception capability.

The UK approach is a more efficient approach to interception as it allows a focus on services of interest whilst retaining confidentiality over which services are and are not capable of interception.

Option B – introduce a mandatory operational importance consideration to the exemption regime

Whilst Telecom considers that the exemption regime in the Bill introduces improvement, in order to balance considerations and avoid exemptions being considered in a conservative way (i.e. agencies might possibly want to intercept the service one day in the future), Telecom proposes the introduction of an operationally focused consideration. That could be in the form of considering similar existing services and whether warrants have been frequently exercised in respect of them and/or a requirement that the surveillance agencies collaborate to provide a list of the types of services that they consider to be of significant operational importance (e.g. voice, instant messaging, email, text) for consideration with regard to exemption applications. Where the service does not appear on that list there should be a presumption in favour of granting the exemption (although an exemption can still be granted where the service does appear on the list).

The agencies would have flexibility to add to the list on a forward looking basis and it should be reviewed annually to ensure that it is consistent with what interceptions have been undertaken in practice (i.e. to ensure that agencies have not been too liberal in preparing the list). A duty to assist will remain on network operators and service providers in respect of all services.

Amend section 32 – exemption process – to include the following as a mandatory consideration in favour of granting an exemption for a particular service:

- (a) Whether the service appears on the current list of operational priorities provided by surveillance agencies [or, alternatively whether similar services have been intercepted previously];

Option C – narrow the definition of telecommunications service

The other alternative is to narrow the definition of telecommunications service but we appreciate the sensitivities around publicly announcing what services are able to be intercepted.

Clarify that the obligation to intercept applies to services crossing the network operator's network at the level of service that the network operator provides (section 9)

New technology means that many telecommunications services can roam across different networks. Accordingly, the Bill should clarify that a network operator's interception obligations are to ensure that its network is intercept capable but that the network operator is only required to ensure services it provides (not including over the top services it is reselling) on its public network are intercept capable. There is no obligation to have a service specific capability on the operator's network if it is not also the provider of the service. ETSI provides that⁷:

"The format of the information a NWO/AP/SvP can be expected to deliver is based on the level of the service it provides. For example, when a NWO provides Internet Access, at best, the NWO can be expected to provide a copy of the IP packets it transports. Only an E-mail service provider should be asked, for example, to have E-mail information delivered in the format of E-mail."

For example, where a voice communication leaves Telecom's network and travels across a private network between a customer's two sites, or where it enters Vodafone's network, Telecom will no longer have any visibility or control over that communication and should not be required to intercept it (but will still have a duty to assist with interception under section 24).

Further, if the warrant is for all communications to and from an individual, Telecom would only be required to intercept the service that it provides. For example, where Telecom is only providing connectivity and the target is using an email service provided by a third party (e.g. Gmail), Telecom will only be obliged to intercept the network connection at the pipe level since that is the service that Telecom is providing.

Section 9

(1) A network operator must ensure that every public telecommunications network that the operator owns, controls, or operates, and every telecommunications service that the operator provides on those networks, has full interception capability.

(2) However, subsection (1) -

⁷ ETSI Technical Specification TS 102 232-1 V3.3.1 (2013-02) "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery"

....

(c) does not require a network operator to ensure that telecommunications services that it does not provide or supply (e.g. they are provided or supplied by a third party over its network) has full interception capability, and is sufficiently complied with if a network operator ensures that it can comply with section 10 at the level of service it provides or supplies.

Encryption obligations (section 10(3)-(4) and section 24(4)(vi)-(5))

As with the current regime, the Bill confirms that network operators are not required to decrypt encryption that has been applied by a third party.

Many over the top services which are resold by network operators have had encryption applied to them by third parties (i.e. the application provider of the service) and the network operator is not provided with any means to decrypt the telecommunications from the application provider (e.g. a decryption key or a clear point for interception). It is unclear how the provisions relating to third party encryption apply with over the top services that are accessible from any location.

For example, in order to comply with its interception capability obligations for an encrypted resold over the top service, a network operator must be able to isolate and intercept a communication but does not need to decrypt a communication where it has not applied the encryption. However, without decrypting the communication the network operator is unable to isolate it in the first place due to its lack of visibility of the communication across its network. This issue again highlights that the interception obligations for these over the top services should be placed on the application provider of those services as they can overcome these issues by building interception capability into their network and/or application. Network operators should only have a duty to assist with intercepting communications where encryption applied by a third party prevents the network operator from being able to identify and intercept the communication.

Obligation relating to network operators with fewer than 4,000 customers (section 13)

This lower level of compliance should be applied on a per service basis as opposed to being based on a network operator's overall customer base. Otherwise this approach leaves larger network operators facing a competitive disadvantage in niche product markets if required to comply with more onerous interception obligations than a small company with the same customer base for the same service.

We propose that the onus is on a network operator to advise the designated officer where they have a service with less than 4,000 end-users (i.e. end point identifiers such as an email address or phone number) and seek the application of this section for that service on the basis of the number of end-users. The network operator would be required to report to the designated officer where the number of end users on that

service⁸ exceeds 4,000. This model of investment in capability is much better suited to the introduction of new and innovative services where it is unknown as to what the market uptake will be. Investment in capability prior to launch may not prove to be warranted in the long term.

If this section is not applied on a per service basis (which is our preferred approach) there is a slight conflict between the different levels of interception required. For example, a network operator of less than 4,000 customers (who must be intercept ready under section 13) may be providing some infrastructure level services (section 14 requires no capability for those services) and wholesale network services (section 13 requires interception accessible for those services). We have suggested some drafting in Appendix A to address this conflict and clarify the level of interception obligation required.

Obligation relating to wholesale network services (section 15)

This section appears to place intercept accessible obligations on a network operator ("the network operator") selling a wholesale network service to another network operator ("the reseller") where the reseller is using the wholesale network service as an input into another service that the reseller provides to an end-user (which the reseller would have full interception obligations for). However, it seems that where the reseller makes no technical modifications to the service the reseller has no interception obligation and it appears that the network operator will have full interception obligations for the service (see subsection 3).

The network operator does not know how the reseller intends to use the wholesale network service; it may be for internal consumption, resold to an end-user or a component of a product that the reseller offers to end-users. The interception obligation on the network operator should remain intercept accessible only regardless of what the reseller does with that service. The network operator can assist under section 27 (outsourcing obligations), or at the request of agencies (under the section 24 duty to assist) since the network operator's interception obligation for such services is to be intercept accessible.

It may be that in practice a wholesaler may build beyond the minimum intercept access interception capability for use by resellers as part of a commercial arrangement, however the wholesaler should not be required to build capability beyond intercept access as this would be unnecessary duplication of capability that may be achieved more efficiently in the wholesaler network operator's customer's network.

Further, there may be practical difficulties for the network operator in determining whether the reseller is registered as a network operator. Therefore, the network operator should be able to request confirmation from the Registrar as to whether or not the reseller is registered as a network operator.

⁸ A service in this context should be class of service from a customer perspective (e.g. PSTN, Email, internet access) divided into the number of different types of platforms providing those classes of service as each platform requires a separate interception solution in general.

We propose the removal of subsection 3 as we consider that it complicates the approach and may result in unintended consequences.

Duty to assist (section 24)

We seek clarification that whilst the obligation to have interception capability in place arises throughout the Act, the obligation to actually execute an interception warrant for an agency arises under the duty to assist. We consider that the Act and section 24 is already drafted in this way but we seek confirmation that this is what should occur in practice.

This is consistent with the UK and USA regimes whereby governments pay the operational expense of actually executing an interception warrant. Considering that network operators face the full cost of implementing interception capability in New Zealand it is reasonable for network operators to recover the operational expense (e.g. employee resource) required to actually execute interceptions for agencies.

Ability for wholesaler to recover the cost of assistance due to a network operator's non-compliance (section 25)

Because of network security and interference concerns it is not realistic or appropriate, nor is it necessary for a wholesaler to provide another network operator with direct access to its network to install equipment and undertake an interception.

Rather where a network operator does not have the ability to give effect to a warrant and interception access to the wholesaler's network is required, that wholesaler should be requested to assist with undertaking the interception under the duty to assist (section 24) – i.e. an agency should request assistance from the wholesale network operator. This approach would also enable the network operator to view the warrant to ensure that the access request is legal.

Where the situation in section 25(1)(a) and (b) arises, (i.e. where the wholesaler has the ability to charge the non-compliant network operator for assistance on a commercial basis) the surveillance agency must make it clear to the wholesaler that the request to assist is due to the network operator's non-compliance so that the wholesaler knows to charge the network operator directly as opposed to seeking its operational costs from the surveillance agency. It should also be clarified that if the network operator fails to pay those charges within the reasonable payment date specified in the wholesaler's invoice, the wholesaler can require the surveillance agency to initiate the enforcement regime against the network operator (as an alternative to other debt recovery options available). Finally, the network operator should be liable for any loss or harm caused to the wholesaler as a result of this requirement.

Section 25 – Wholesaler may charge

(1) A wholesaler who is required...to assist another network operator with undertaking an interception warrant, may charge the other network operator, on a commercial basis including for any access, space, power, employee time, and use of equipment...for the purpose of giving effect to the warrant or lawful authority if...

(5) The surveillance agency must request assistance from the wholesaler under section 24 and must notify the wholesaler that the conditions in subsection (1)(a) and (b) have been met, and provide the wholesaler with a copy of the interception warrant or other lawful interception authority.

(6) Where a network operator fails to pay the amount charged by the wholesaler under subsection (1) by the reasonable invoice payment date, the wholesaler may require the relevant surveillance agency to initiate the enforcement regime against the network operator to recover payment. This section does not limit other debt recovery options available to the wholesaler.

(7) The network operator indemnifies the wholesaler for any loss or harm caused arising from or in connection with this duty to assist.

Clarify the ability to share resources (section 27)

We seek clarification that this provision allows an entity with interception obligations to outsource those obligations to any third party (not necessarily another network operator) upon notification to surveillance agencies (we suggest via an industry liaison). This will remove duplication of interception capability across the industry which will introduce cost efficiencies. It may also result in agencies dealing with fewer specialised individuals who are providing interception services across a number of different network operators.

This option alone is not sufficient to address Telecom's primary concern with placing interception obligations on the application provider of over the top services because there is nothing to force the application provider to develop capability over their services in the first place, nor any compulsion on the application provider of the over the top service to assist a reseller of the service with interception obligations.

Further, it should be made clear that where a network operator has outsourced its interception obligations, it will not be in breach of the Act (including the duty to assist) where it is prevented from sharing a warrant with the entity it has outsourced to.

- Section 24 – Duty to assist

(1) A surveillance agency...may...show to either or both of the persons referred to in subsection (2) [an interception warrant]...

(2) The persons are

(a) A network operator; or

(b) A service provider; or

(c) An agent of a network operator or application provider under section 27.

- Section 27 – Network operators or application providers of over the top services may outsource obligations

(1) Nothing in this Act prevents any person ~~network operators~~ from coordinating, sharing, or contracting with any other person for interception services (whether equipment or staff, or the execution of a warrant) in order to meet the requirements in the Act.

(2) However, any arrangement referred to in subsection (1) does not affect any obligations that apply to any person ~~a network operator~~ and that have been imposed by or under this Act, and the primary obligations under this Act remain on that person.

- New section – failure to comply with obligations due to inability to share an interception warrant or other lawful authority

(1) A person shall not be in breach of this Act where they are unable to comply with their obligations due to an inability to share an interception warrant with their outsourced agent under section 27.

Introduce further considerations into the exemption process (section 32)

The exemption process makes significant improvements to the existing regime however, further mandatory considerations are necessary to ensure that balanced consideration is given to an exemption application, and to remove the current unlevel playing field that exists between network operators and non-network operators.

Further, we consider that the primacy given to national security or law enforcement may have unintended consequences by forcing the designated officer to always make a decision in favour of surveillance agencies' interests even where it is not necessary to do so. We propose that subsection (2) should be deleted and it should be left to the designated officer to appropriately balance the various considerations.

Section 32 – Exemption decision making process

- (1) The designated officer must, when considering whether to grant, vary, or revoke an exemption...take account of all the following matters:
- (b) National security or law enforcement interests;
 - (c) The number and type of customers or end-users of the relevant network or service;
 - (d) The cost of compliance with the obligation for which an exemption is sought compared to the importance of the service for law enforcement or national security purposes and the likelihood of interception being undertaken on the service;
 - (e) Whether compliance could be achieved appropriately or more efficiently by another means;
 - (f) Whether the service appears on the current list of operational priorities provided to the designated officer [or, alternatively whether similar

services have been intercepted previously];

(g) Whether compliance 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 technologies;

(h) Any other matter that the designated officer considers relevant in the circumstances.

...

Delete subsection (2).

Ability to extend LI obligations to service providers (section 35)

The change in industry structure and new technologies means that, particularly with over the top services, it is often more efficient for someone other than a network operator re-selling the service to implement interception capability. The Act was first implemented when it was assumed that network operators would be providing all services on their networks, and would therefore be best placed to ensure full interception capability of those services. It is also more efficient for the agencies to intercept at the service layer as they can target specific services as opposed to all traffic.

Accordingly, unless separate obligations are placed on the application provider of over the top services (which is Telecom's recommended approach), the considerations before deeming in a service provider should be similar to the considerations for granting an exemption to a network operator. There should also be an express consideration as to whether it is more efficient for an entity to have interception obligations than network operators in particular circumstances (for example, where a network operator is merely reselling an over the top service and therefore, does not have true control over that service).

Section 35 –

(7) The matters that the Minister must take into account are:

(a) National security or law enforcement interests;

(b) The cost of compliance compared to the importance for national security or law enforcement purposes of the service having interception capability and the likelihood of interception being undertaken on the service;

(c) Whether the new duties 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 technologies;

(d) Whether it is more efficient for a service provider or application provider of

over the top services to provide interception capability due to its level of ownership, control, or operation of a service;

(e) Any other matter that the Minister considers relevant in the circumstances.

- Insert definition of “application provider” and “over the top service”.

Any right to review a direction to deem a service provider to have lawful interception obligations under section 36 should be by the Technical Advisory Board which is further discussed below.

Ministerial direction relating to resold overseas telecommunications services (section 39)

Section 39 appears to be directed at situations where an agency considers that the provision of a service in New Zealand gives rise to a significant risk to national security or law enforcement.

However, the direction power can only be applied against network operators. Stopping only network operators from providing the service will not address the national security risk as non-network operators can still offer that exact service in New Zealand (and without interception capability). For example, if surveillance agencies are concerned that Skype (if it could be purchased by customers from Vodafone (a network operator), Harvey Norman and from Microsoft directly) raised a national security or law enforcement risk, this power would only be applicable against Vodafone as a network operator⁹. Harvey Norman or Microsoft would still be free to sell the service to New Zealand customer who can use the service over any network operator’s network.

Accordingly, this direction should only be applied pan-industry (i.e. if the direction is exercised the service should not be provided in New Zealand at all). This could be achieved through making the direction against the application provider of the over the top service as they would then be prevented from offering any instance of the service for sale in New Zealand either by selling it directly to customers, or by wholesaling it to other retailers or network operators to resell.

This direction power should not create yet another way for Government to enforce unilateral obligations/prohibitions on network operators which prevent them from competing to offer the same service that its non-network operating competitors are free to offer. Further, the power should only be applicable where there are concerns over the lack of interception capability, not the type of interception capability in place. If a provider goes to the expense of making a service interception capable in compliance with the Act, it should not still be available to Government to prevent the service from being offered.

⁹ Telecom considers that the actual provider of the over the top service is a network operator but they have not been enforced against to date.

Section 39 – Ministerial direction relating to ~~resold overseas telecommunications services~~ over the top services provided from overseas

(1) This section applies to any ~~telecommunications services~~ over the top services that are provided from outside New Zealand and are available for purchase by end-users in New Zealand ~~by a network operator~~.

...

(3) A surveillance agency must notify the affected providers of the service –

(c) That it has applied for a direction under this section; and

(d) Of the reasonable date by which the affected providers may make submissions to the Minister.

(4) An application by the surveillance agency must include the reasons why the agency considers the ~~interception capability or~~ lack of interception capability on the service gives rise to a significant risk to national security or law enforcement.

(4A) The Minister will only exercise this direction in a way that prevents the service from being offered in New Zealand and it will not be applied only against an individual or class of providers where the service is otherwise available in New Zealand from other providers.

(5) The affected parties may make submissions to the Minister by the reasonable date specified in the notice referred to in subsection (4).

(6) The Minister must consult with the technical advisory board, the responsible Ministers, the Minister for Communications and Information Technology, and the Minister of Trade.

(7) The Minister must take into account the views of affected parties and those of the technical advisory board and Ministers referred to in subsection (6).

(8) The Minister must issue the direction in writing to the affected parties together with reasons except those parts of reasons that would inappropriately reveal classified information.

...

- Add definition of “over the top service”

Other

Given the changes in technology and, in particular the dominant presence of over the top services provided from overseas, the Bill should expressly provide for extra-territorial effect in relation to persons providing services in New Zealand.

We also consider that a single point of contact for the surveillance agencies would assist with liaison between Government and the telecommunications industry. Further, costs for industry could be mitigated by providing a single agency that requests interceptions and receives all interception product on behalf of agencies.

Finally, Telecom is concerned with the ability for the Governor General to add another government department to the definition of law enforcement agency. The interception of private communications is a very serious imposition on peoples' rights to privacy and it should be strictly limited to the Police, SIS and GCSB with other government departments escalating serious criminal matters to the Police. Further, network operators would face significantly increased costs should more government agencies be given the right to intercept.

PART TWO: NETWORK SECURITY OBLIGATIONS

Telecom considers that there already exists a sufficient commercial incentive for network operators to adequately consider and ensure that their networks are secure. Indeed, in many cases and particularly for corporate customers, security of network is a large part of what our customers are purchasing from us.

As it is our current practice, we are comfortable with a duty to engage with Government on significant matters of network security (with guidance from agencies as to what might amount to that), and we welcome advice from agencies about security concerns with particular suppliers and/or equipment.

However, we are concerned that the proposed Bill introduces excessive delay, cost, scrutiny and involvement by Government in commercial procurement decisions without properly balancing commercial interests. The administrative burden imposed by these obligations will be significant and seem unnecessary in light of the low likelihood of these powers being administered.

Duty to engage in good faith (section 45)

Network operators are required to pro-actively engage with agencies when they become aware of any actual or potential network security risk (i.e. an actual or potential risk to New Zealand's national security or economic well-being).

It is very difficult to ascertain what Government will consider to amount to a risk to national security or economic well-being. This will result in network operators facing unnecessary compliance costs and commercial delays, and government having the same issue with filtering the irrelevant information received. Further, it is not clear when a failure to engage on something will amount to a breach of the Act until the agencies retrospectively determine that the matter did in fact amount to a national security risk and should have been brought to their attention.

We consider that the duty to engage should arise where the network operator becomes aware of any actual or potential significant risk to national security. It is also necessary for Government to better define what amounts to a risk to New Zealand's national security or economic well-being and to provide guidance to operators to assist with understanding the situations in which they should engage with the GCSB.

Areas of specified security interest (section 46)

We consider that the notification regime should be removed with reliance instead on a duty to engage with the GCSB (pursuant to section 45) and Government collaboratively engaging with network operators regarding practices, vendors and support arrangements that are acceptable and unacceptable to them. The GCSB will then have the direction power available where industry does not address those concerns adequately.

Based on the Bill there is a large difference between what the Government considers to be a NOC and what Telecom believes is material to securing the network. The government definition is too broad and will result in unwarranted interference.

With respect to other parts of the network additional guidance is required as to what other parts of the network are relevant, even a small service could be because of the customer base. We would therefore have to provide great detail to the GCSB for them to be able to assess the security risk, and they would need significant resource to do a thorough job. Further, this approach of the GCSB acting as a gatekeeper is likely to result in a sense of false security as operators may begin to rely on the GCSB review to detect and rectify security issues rather than do a thorough job themselves, and if the GCSB are not thorough standards will slip. It would be preferred for the GCSB to collaboratively discuss with network operators practices, vendors and support arrangements that are acceptable and unacceptable to them. This would leave a hopefully small number of exceptional cases when they should be engaged to investigate further or provide advice, rather than engaging them on almost every Telecom network project as most parts of the Telecom network carry significant volumes of aggregated traffic.

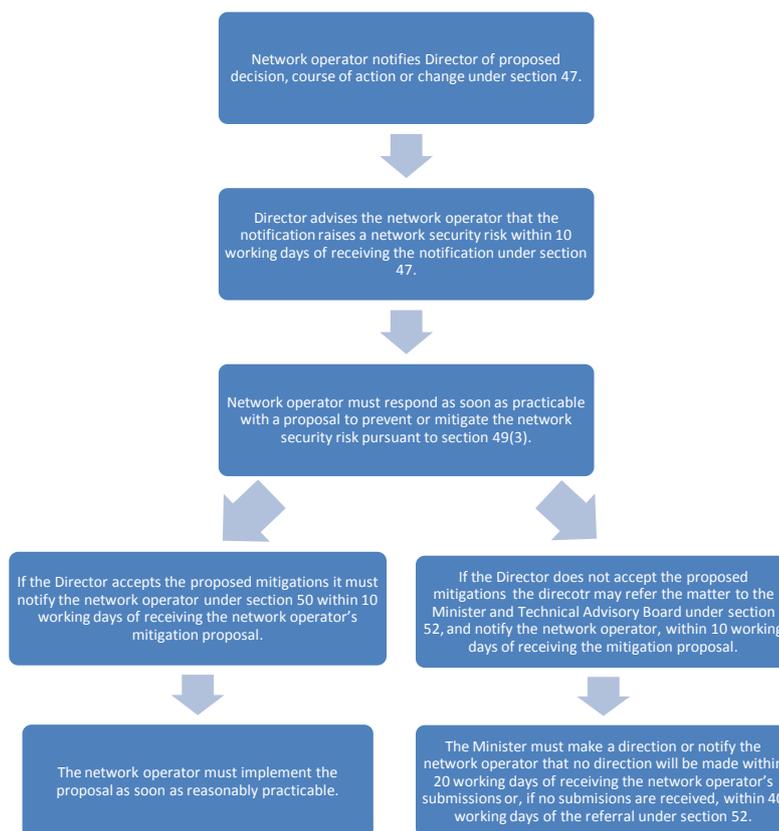
[Process for addressing a security risk \(section 49\)](#)

Leaving the question of whether in practice the types of powers proposed will be capable of effectively minimising network intrusions aside (to be clear, we do not believe they will be), the approval and direction powers do not facilitate a collaborative or transparent partnership between industry and agencies (which would be better achieved through industry agreed standards).

To ensure that the interests of the telecommunications industry and surveillance agencies are properly balanced, Telecom proposes that where Government puts a network operator to extra expense to go above and beyond what the operator considers is secure from a commercially acceptable point of view (i.e. standards that its customers are satisfied with), Government should pay half of that additional expense.

Further, as with the UK regime, Telecom proposes that before any direction power is exercised by the Minister, there must first be consultation with a technical advisory board made up of equal numbers of national security cleared technical experts and surveillance agency representatives for a recommendation (including sharing the network operator's submissions with that board) to the Minister. This also takes into account that Government may not have the technical expertise necessary to properly assess a network operator's network and, therefore, the ability to appropriately advise of steps that should be taken to proportionately mitigate a perceived national security risk. The members of the technical advisory board will need to enter into strict confidentiality obligations considering that they may be privy to information about a competitor's network.

Given the amount of procurement decisions that a company the size of Telecom makes, any delays in the process for assessing network security risks are undesirable and would slow down the network operator's commercial operations. Accordingly, set timeframes for the process for addressing network security risks should be imposed. Telecom suggests the following:



Further, the Director can initiate the security risk process as a result of information obtained or received under the Act. In order to provide operators with certainty about the significant investments they are making in their networks, it must be ensured that the direction power is not used in a way that it undoes a previously approved notification (for example, where new information comes to light that means that a provider of equipment that was previously thought not to be of risk now raises security concerns so can no longer be used). Where this situation arises, Government should be required to pay all associated costs with having to comply with a direction that relates to a previously approved notification (or before the enactment of the Bill).

Where the director considers there to be a security risk and the network operator's proposal to mitigate is not sufficient, the director can escalate the matter (section 52)

In order to ensure that a network operator can properly submit on the matter, upon notification of escalation under this section, the Director should be required to provide details of the perceived threat to allow the network operator a proper opportunity to submit (bearing in mind that the operator will have national security cleared people

who deal with top secret information under this regime). This is consistent with the administrative law requirement that parties should have sufficient information to make fully informed submissions.

Given the significant adverse impact that any direction will have on a network operator, the affected network operator should then have a right to appeal the exercise of the Ministerial direction to an arbitrator within 60 days. The arbitrator must consider submissions from the network operator and Technical Advisory Board. Arbitration has the additional advantage of ensuring confidentiality of proceedings, which would be appropriate given the sensitive nature of any proposed direction regarding network security.

[Obligation on network operators to register \(section 55\)](#)

Only a very few entities currently consider themselves to be network operators that attract interception obligations. Unlike today where only a few network operators are focused upon, Government needs to take enforcement seriously to ensure that the obligations are competitively neutral between similar providers.

There should be an annual audit of the entities who have registered as network operators compared to those entities Government considers to be network operators. Government should then take pro-active steps to approach the network operators who have failed to register and require that they do so. Where there is a failure to register Government should initiate the enforcement process.

[Requirement to provide information to the Registrar](#)

There is a requirement on network operators to provide certain information upon registration. Given the confidential and commercially sensitive nature of this information, any registration information provided to the Registrar under the Act should expressly be kept under an obligation of confidence, should only be used for the purpose for which it has been provided under the Act, and must be destroyed immediately once it has been superseded or is no longer required for the purposes for which it was provided. Before any disclosure of this information is made to any third party under a legal compulsion, the Registrar should be required to notify the affected network operator of the request and provide them with an opportunity to input into the response to the request.

The provision and updating of this information will result in compliance costs to network operators and we do not consider the actual operational use of this information by agencies for the purposes of performing their functions under the Act justifies the time and expense involved with compliance. We also comment on the following particular categories of information requested:

- Section 57(1)(e) requires a network operator providing retail services to estimate the total number of end-users across all telecommunications services and all telecommunications networks (for example, the number of people in each household). The compliance cost involved in the provision of this information would be significant. Further, if a network operator already has full interception (for example, checking census information to ascertain the number of end-users in a household) obligations, or obligations that are based on the type of service

they provide rather than the number of end-users, this information is not relevant for assessing interception obligations and should not be required. Instead the ability for a designated officer to specifically request such information under section 72 should be relied upon to avoid putting the entire industry to the expense of complying with this reporting obligation.

- We do not agree that geographic location of services is essential information since this information is not required today and interception and network security obligations are not impacted by the geographical location of a service.

Pursuant to section 63, we do not consider that information about geographical coverage or the types of services provided should amount to relevant information which needs updating other than on an annual basis. This information does not impact on the level of interception obligation and merely introduces further compliance cost for companies.

Finally, we consider that there should be a review 12 months following enactment to assess whether the registration information has been of operational importance, or whether the type of registration information required can be reduced. Further, where access to the register or operation of it is suspended due to it not being practical (section 62(1)) network operators should be advised that they are no longer required to provide the registration information or that only a portion of the registration information is required.

Other

The designated officer (see section 67) who determines exemptions should be an individual agreed on and central to all three surveillance agencies. We would be concerned if only one agency had the power to appoint that individual considering the importance of the determination of exemption applications.

Under section 72 a designated officer may require information from a network operator. We consider that this ability should be extended to apply against a service provider (for example, in the situation where there is a dispute between an agency and an entity as to whether or not the entity qualifies as a network operator). However, we are concerned that section 72(2)(b) which requires the supply of information or documents for the purpose of assisting with the execution of an interception warrant would enable surveillance agencies to circumvent the processes in the Search and Surveillance Act, GCSB and SIS Acts as agencies could perceivably avoid obtaining a warrant and request customer information under this section. Accordingly, we consider that this ability to request information should not extend to obtain the content of telecommunications.

APPENDIX A – Further suggested amendments to the Bill

The following are comments on the proposed drafting in the Bill.

Provision	Concern	Proposed amendment
Application provider (new definition)	To address the inclusion of over the top services (see main submission).	<u>(1) A person (based in New Zealand or overseas) that provides application layer software and/or hardware that enables an over the top service supported by that application to be provided to end-users in New Zealand (whether directly or indirectly or by wholesale or retail).</u>
End user	It is unclear what the intended purpose of the following wording is - "or of another service the provision of which is dependent on that service".	Clarification sought, or deletion of the wording "or of another service the provision of which is dependent on that service".
Infrastructure-level service	Provide further guidance of what is included in this definition.	Infrastructure level services means - any service that provides the physical medium over which telecommunications are transmitted (for example, <u>copper cables, optical fibre cable, distribution frames, joints, other passive components etc</u>), but does not include the device or equipment that generates, transmits, or receives any telecommunication signal.
Intercept	This definition is really intended to refer to the transmission of content to surveillance agencies and should be amended to ensure that network operators will continue to have the ability to monitor and receive communications for network purposes.	Interception, in relation to a private telecommunication, includes hear, listen to, record, monitor, acquire, <u>or the receipt of</u> receive the telecommunication <u>by a person</u> – (a) while it is taking place on a telecommunications network; or (b) while it is in transit on a telecommunications network.
Law enforcement agency	Given the impact to individual's rights to privacy we do not consider that it is appropriate to extend the ability to intercept private communications to other government departments. Important criminal matters should be referred to the Police.	Law enforcement agency means – (a) the New Zealand Police; or (b) any government department declared by the Governor General, by Order in Council, to be a law enforcement agency for the purposes of this Act.
Network operations centre	The existing broad definition would cover numerous aspects that have no direct impact	Network operations centre means a unit that a network operator has <u>primarily</u> designated as being responsible for

	upon what happens in the network and, therefore, this definition should be more limited in scope.	<p>assuring <u>controlling</u> the operation, performance, or security of a telecommunications network and –</p> <p>(a) that is equipped with equipment that is appropriate for carrying out that responsibility; and</p> <p>(b) whose duties may, without limitation, include 1 or more of the following activities:</p> <ul style="list-style-type: none"> (i) controlling network elements; (ii) controlling security access systems. (i) monitoring alarms and alerts; (ii) identifying faults and arranging for those faults to be rectified; (iii) monitoring network congestion; (iv) monitoring the continued delivery of services.
Over the top service (new definition)	A new definition of over the top service is required.	<p><u>“Over the top service” means – a telecommunications service which runs over a network operator’s network and:</u></p> <p><u>(a) Is a purely resold telecommunications service; or</u></p> <p><u>(b) Is provided to the end user by the application provider or another service provider.</u></p>
Purely resold telecommunications service		<p>Purely resold telecommunications service means any service –</p> <p>(a) that is supplied or provided to a network operator <u>or service provider</u> (the customer) other than <u>primarily</u> for the customer’s own use or consumption; and</p> <p>(b) that the customer resells, supplies, or provides to another person, body or organisation without making any technical modification to that service.</p>
Security risk (and significant security network risk)	<p>It is unclear what will amount to an actual or potential risk to New Zealand’s national security or economic well-being.</p> <p>This definition requires narrowing, together with a guidance paper (with input from</p>	-

	industry) which provides some practical guidance around what might amount to a risk to New Zealand's national security or economic well-being.	
Service provider	The definition only covers the situation where a provider is providing a service to an "end user" which means that over the top service providers could wholesale only in New Zealand to avoid being captured by the duty to assist, deem-in and other provisions.	Service provider – (a) means any person (<u>whether operating from within or outside New Zealand</u>) who provides a telecommunications service to an end-users (whether or not as part of a business undertaking and regardless of the nature of that business undertaking) in New Zealand (whether directly or indirectly or by wholesale or retail); but (b) does not include a network operator.
Technical modification (new definition)	Provide a definition of what amounts to a technical modification.	<u>Technical modification – includes a technical modification to the service other than through customisable options offered by the application provider of that service to resellers generally.</u>
Useable format (appears in section 10(5), 24(7) and section 40)	We would like clarification that compliance consistent with ETSI standards is an acceptable useable format. It should be clear that network operators can satisfy their obligations if they can deliver content in a manner that is consistent with a notified standard (e.g. ETSI), or in a format that has been agreed between the network operator and agencies (or a mix of the various agreed formats).	Express ETSI standards as an agreed useable format. Amend section 10(5) – (a) a format that is <u>not inconsistent with a standard</u> determined by a notice issued under section 40... Amend section 24(7) – (a) a format that is <u>not inconsistent with a standard</u> determined by a notice issued under section 40... Amend section 40 – (1) The Minister may, by notice in the Gazette, determine <u>a format by which the delivery of call associated data and the content of telecommunications must not be inconsistent with.</u>

Wholesale network service	The wholesaler will not know what the service will be used for.	<p>...</p> <p>(c) is not <u>solely</u> for the other network operator's own consumption. and</p> <p>(d) is or becomes a constituent part of a service that the other network operator provides to an end-user or any other person, body, or organisation.</p>
Section 6 - Principles relating to interception capability	Certain principles relating to network security (section 8) should be added to the principles relating to interception capability.	<p>...</p> <p><u>(c) The principle that surveillance agencies and network operators should work co-operatively and collaboratively with each other.</u></p> <p><u>(d) The principle that the decisions or exercise of functions should be proportionate to the likelihood of interception and be the most efficient and effective way of achieving the purposes of the Act.</u></p> <p><u>(e) the principle that the exercise of functions should not impose unreasonable costs on network operators which are disproportionate to the likelihood of interception being required.</u></p> <p><u>(e) The principle that the exercise of functions should not unduly harm competition in telecommunications markets.</u></p>
Section 8 – Principles relating to network security	Introduce a new consideration to balance the cost of mitigating a potential network security risk with the likelihood of the risk occurring, and to ensure that consideration is given effect to.	<p>...</p> <p>(2) The principle in subsection (3) must be taken into account <u>given effect to...</u></p> <p>....</p> <p>(3) The principle that the decision or exercise of the function or power should be proportionate to the network security risk.</p> <p>(4) In subsection (3), a decision or an exercise of a function or power is proportionate to the network security risk if it -</p> <p>(a) does not impose costs on network operators or telecommunications customer or end-users beyond those reasonable required to enable the network security risk to be prevented, mitigated, or removed <u>taking into account the likelihood of the network security risk actually occurring.</u></p>

		<p>...</p> <p><u>(c) is applied in a way that has the least adverse impact on a network operator as is possible in the circumstances.</u></p>
Section 9 – Network operators must ensure public telecommunications networks and telecommunications services have full interception capability	Clarify that an interception obligation relates to services that cross the network operator’s network and the network operator must be able to intercept at the level of the service it provides.	<p>(1) A network operator must ensure that every public telecommunications network that the operator owns, controls, or operates, and every telecommunications service that the operator provides <u>on those networks</u> in New Zealand, has full interception capability.</p> <p>(2) However, subsection (1) -</p> <p>....</p> <p><u>(c) does not require a network operator to ensure that telecommunications services that it does not provide or supply (e.g. they are provided or supplied by a third party over its network) has full interception capability, and is sufficiently complied with if a network operator ensures that it can comply with section 10 at the level of service it provides or supplies.</u></p>
Section 10 – When duty to have full interception capability is complied with	Make the obligations in section 1(a) and (d) consistent.	<p>(1) A public telecommunications network or a telecommunications service has full interception capability if...able to:</p> <p>(a) Identify and intercept telecommunications without <u>unduly</u> intercepting telecommunications that are not authorised to be intercepted under the warrant or lawful authority...</p>
Section 11 - Intercept ready	Introduce standards of reasonableness and practicability.	<p>(11)(1) A network operator that is required by or under this subpart to ensure that a network or service is intercept ready—</p> <p>(a) must, <u>to the extent reasonably practicable</u>, pre-deploy access points at <u>reasonably</u> suitable and sufficient concentration points...</p> <p>(b) must, <u>to the extent reasonably practicable</u>, reserve 1 or more network interfaces...in order to deliver intercepted <u>content communications</u> to the surveillance agency; and</p> <p>(c) must reserve, <u>to the extent reasonably practicable</u>, for each reserved interface referred to in paragraph (b), sufficient bandwidth to deliver intercepted <u>content material</u></p>

		<p>to the relevant surveillance agency <u>or other mutually agreed delivery point</u>; and</p> <p>(d) when presented with an interception warrant or any other lawful interception authority must, free of charge,...</p> <p>(i) provide <u>an access to its network or service point at a suitable point in its network</u> for interception equipment <u>by a surveillance agency</u>...</p> <p>(iii) provide, to the extent reasonably practicable, sufficient environmentally controlled space to house the interception equipment or provide sufficient backhaul to a suitable location where the equipment can be housed.</p> <p>(2) A network operator referred to in section 13 or 14 is not eligible for reimbursement under section 100 if the network operator's network or service was intercept ready only.</p> <p><u>(2) A network operator who complies with subsection (1)(d)(i) shall be indemnified by any person who accesses its network in respect of any damage or loss caused to the network operator as a result of such access.</u></p>
Section 12 - Intercept accessible	Introduce standards of reasonableness and practicability.	<p>...</p> <p>(a) provide, <u>to the extent reasonably practicable, an access point at a suitable point in its network</u> to its network or service for interception equipment <u>by a surveillance agency</u>.</p> <p>(c) provide, <u>to the extent reasonably practicable,</u> sufficient environmentally controlled space to house the interception equipment...</p> <p><u>(2) A network operator who complies with subsection (1)(c) shall be indemnified by any person who accesses its network in respect of any damage or loss caused to the network operator as a result of such access.</u></p>
Section 13 – Network operators with fewer than 4,000 customers	The default level of compliance for operators of less than 4,000 customers should be intercept ready unless the services being provided are infrastructure level services, or wholesale network services in which case the lower levels of interception obligation will apply.	<p>(2)(b) must instead ensure that every public telecommunications network that the operator owns, controls, or operates, and every telecommunications service that the operator provides in New Zealand is intercept ready at all times, <u>unless the service being provided is a wholesale network service or infrastructure level service in which case the lower level of compliance in section 12 or 14 will apply</u></p>

	Further, this section should apply at the service level as opposed to at the overall customer base level (see our main submissions above).	<p><u>to that service.</u></p> <p>(7)customer means a person who is <u>receiving telecommunications services from</u>, and who has an account or billing relationship with the network operator.</p> <p><u>(8) This section does not apply to over the top services.</u></p>
Section 14 – Infrastructure level services	Refer to section 13 above.	(1) A network operator does not have to comply with sections 9, and 10 <u>or 13</u> in respect of any infrastructure-level service provided by the network operator.
Section 15 – Wholesale network service	Refer to section 13 above. Remove the carve out for resold telecommunications services.	<p>(1) A network operator does not have to comply with sections 9, and 10 <u>or 13</u> in respect of any wholesale network service provided by the network operator.</p> <p><u>(1A) a network operator can require the Registrar to confirm whether the entity it is selling a service to is a network operator for the purposes of ascertaining whether the service being provided will amount to a wholesale network service.</u></p> <p>(3) Nothing in this section applies to—</p> <p>(a) purely resold telecommunications services; or</p> <p>(b) any wholesale network services that is provided to, or by, a network operator that is not subject to the laws of New Zealand.</p>
Section 17 – Application for direction	Ensure notice is in writing and that a reasonable timeframe is provided for submissions.	<p>...</p> <p>(2) The surveillance agency must, when applying for a direction, notify the affected network operator <u>in writing</u> of the application and the <u>reasonable</u> time frame by which submissions may be made to the Minister on the application.</p>
Section 18 – Process following application for direction	Ensure that a reasonable timeframe is provided for submissions.	(1) The affected network operator may make submissions to the Minister in relation to the application for direction within the <u>reasonable</u> timeframes specified in the notice...
Section 19 – Direction (to deem-up)	Ensure a reasonable timeframe is given for complying with the direction.	<u>(3A) The Minister must allow a reasonable timeframe for the affected network operator to comply with the direction.</u>

Section 20 - Regulations	Ensure a reasonable timeframe is given for complying with the deem-up direction.	<u>(3) The Minister must allow a reasonable timeframe for the affected network operator to comply with the direction.</u>
Section 22 – Design of networks not affected by this Part	To be consistent with the purposes of the Act, this should be extended to design of networks and services.	Section 22 - Design of networks <u>or services</u> not affected by this Part (a) require any person to adopt a specific design or feature for any network <u>or service</u> ; or (b) prohibit any person from adopting any specific design or feature for any network <u>or service</u> .
Section 23 – Infrastructure-level services	The reporting obligation regarding new customer names is overly onerous.	(b)(ii) If it is not reasonably practicable to comply with subparagraph (i), as soon as is reasonably practicable before providing or activating the infrastructure level service.
Section 24 – Duty to assist	Add wording to ensure that a warrant can be shared with an agent where a network operator or service provider has outsourced its obligations under section 27.	(2) The persons are – (a) a network operator; or (b) a service provider; <u>or</u> (c) <u>an agent of a network operator or application provider under section 27.</u>
Section 25 – Wholesaler may charge	It is not appropriate or necessary to allow a third party direct access to a wholesaler’s network, rather the wholesaler should assist where required.	Section 25 – Wholesaler may charge (1) A wholesaler who is required...to <u>assist</u> another network operator <u>with undertaking an interception warrant</u> , may charge the other network operator, on a commercial basis <u>including</u> for any access, space, power, <u>employee time, and use of equipment</u> ...for the purpose of giving effect to the warrant or lawful authority if... (5) <u>The surveillance agency must request assistance from the wholesaler under section 24 and must notify the wholesaler that the conditions in subsection (1)(a) and (b) have been met, and provide the wholesaler with a copy of the interception warrant or other lawful interception authority.</u> (6) <u>Where a network operator fails to pay the amount charged by the wholesaler under subsection (1) by the reasonable invoice payment date, the wholesaler may</u>

		<p><u>require the relevant surveillance agency to initiate the enforcement regime against the network operator to recover payment. This section does not limit other debt recovery options available to the wholesaler.</u></p> <p><u>(7) The network operator indemnifies the wholesaler for any loss or harm caused arising from or in connection with this duty to assist.</u></p>
Section 26 – Duty to minimise impact of interception on third parties	The intention is to ensure that non-target content is not disclosed to a surveillance agency by a network operator or service provider.	Every person...must take all practicable steps that are reasonable in the circumstances to minimise the likelihood of <u>disclosing intercepting</u> telecommunications that are not authorised to be intercepted under the warrant or lawful authority.
Section 27 – Network operators may share resources	Ensure that a network operator or over the top service provider can share resources.	<p>Section 27 – Network operators <u>or application providers of over the top services</u> may <u>outsource obligations</u></p> <p>(1) Nothing in this Act prevents <u>any person</u> network operators from co-ordinating, sharing, or contracting <u>with any other person</u> for interception services (whether equipment or staff, <u>or the execution of a warrant</u>) in order to meet the requirements in the Act.</p> <p>(2) However, any arrangement referred to in subsection (1) does not affect any obligations that apply to <u>any person</u> a network operator and that have been imposed by or under this Act, <u>and the primary obligations under this Act remain on that person.</u></p>
<u>Introduce a new section – failure to comply with obligations due to inability to share an interception warrant or other lawful authority</u>	Where a specific warrant prohibits a network operator or application provider of over the top services from sharing it with its outsourced agent and the surveillance agency does not amend the warrant, the network operator or application provider of over the top services will not be in breach of their	<u>Any person shall not be in breach of this Act where they are unable to comply with their obligations due to an inability to share an interception warrant with their outsourced agent under section 27.</u>

	obligations under the Act.	
Section 28 – Obligations relating to arrangement for interception services	Add a reasonableness requirement.	(2) A network operator <u>must take reasonable steps</u> to ensure that any person that it enters into a contract...
Section 29 – Exemptions	There should be no restrictions on what an exemption can be granted for so long as there remains the section 26 duty to minimise the impact on non-targets.	(1) A designated officer may, in accordance with section 32 – (a) grant, subject to subsection (2), a network operator or class of network operators an exemption from all or any of the requirements of sections 9 and 10 to 15. (b) grant a network operator or class of network operators an exemption from all or any of the requirements of section 13. (2) An exemption under subsection (1)(a) must not affect the requirements in section 10 that relate to the ability to protect the privacy of telecommunications that are not authorised to be interception under an interception warrant or any other lawful authority. (2) <u>For the avoidance of doubt, an exemption must not affect the duty in section 26.</u>
Section 30 – Application for exemption	Ensure prompt notification of any extension requirement and a long stop date.	(5) If subsection (4) applies, the designated officer must, as soon as reasonably practicable, <u>and no later than 20 working days after receipt o the application,</u> give the application notice of the extension. (6) ...and the new time frame by which the designated officer must respond <u>which must not exceed a period of 3 months from the receipt of the application.</u>
Section 36 – Review	The review of any direction should be to the Technical Advisory Board.	(1) If a direction is made under section 35, the affected service provider may request a review of the Minister’s decision. (2) On receiving a request for review, the Minister must appoint 3 suitably qualified persons to form a review panel refer the request to the Technical Advisory Board. (3) The review panel <u>Technical Advisory Board</u> must... (4) The Minister must, after considering the

		<p>recommendations of the review panel <u>Technical Advisory Board</u>, vary or confirm the direction.</p> <p>(5) A summary of the review panel's <u>Technical Advisory Board's</u> recommendations...</p>
<p>Section 39 – Ministerial direction relating to resold overseas telecommunications services</p>	<p>This power should only be applied pan-industry not in a way that prevents a segment of providers from offering a service that is otherwise available in New Zealand.</p>	<p>Section 39 – Ministerial direction relating to resold overseas telecommunications services <u>over the top services provided from</u> overseas</p> <p>(2) This section applies to any telecommunications services <u>over the top services</u> that are provided from outside New Zealand and <u>are available for purchase by end-users</u> in New Zealand by a network operator.</p> <p>...</p> <p>(3) A surveillance agency must notify the affected <u>providers of the service</u> –</p> <p>(c) That it has applied for a direction under this section; and</p> <p>(d) Of the <u>reasonable</u> date by which the <u>affected providers</u> may make submissions to the Minister.</p> <p>(4) An application by the surveillance agency must include the reasons why the agency considers the interception capability <u>or lack of interception capability</u> on the service gives rise to a significant risk to national security or law enforcement.</p> <p>(4A) <u>The Minister will only exercise this direction in a way that prevents the service from being offered in New Zealand and it will not be applied only against an individual or class of providers where the service is otherwise available in New Zealand from other providers.</u></p> <p>(5) The <u>affected parties</u> may make submissions to the Minister <u>by the reasonable date specified in the notice referred to in subsection (4).</u></p> <p>(6) The Minister must consult with <u>the technical advisory</u></p>

		<p><u>board</u>, the responsible Ministers, the Minister for Communications and Information Technology, and the Minister of Trade.</p> <p>(7) The Minister must take into account the views of affected <u>parties</u> and those of the <u>technical advisory board</u> <u>and</u> Ministers referred to in subsection (6).</p> <p>(8) The Minister must issue the direction in writing to the affected <u>parties</u> together with reasons except those parts of reasons that would <u>inappropriately</u> reveal classified information.</p> <p>...</p>
New section to provide for a review of the above power.	The ability to request the Technical Advisory Board to review the decision (provided for in section 36) should be available.	See section 36 with the above proposed amendments.
Section 42 – Formatting before commencement of this Act	Replace “telecommunications” with “content”.	A public telecommunications network...by obtaining the call associated data and <u>telecommunications content</u> in a format..
Section 45 – Network operators’ duty to engage in good faith	This obligation should be narrowed and clarified to ensure that the duty is efficient and effective.	(1) A network operator must engage with the Director as soon as practicable after becoming aware of any <u>significant</u> network security risk, or proposed decision, course of action, or change that may raise a <u>significant</u> network security risk.
Section 49 – Process for addressing network security risks	Impose time limits.	<p>(1) If, as a result of information obtained or received by the Director under this Act, the Director becomes aware of a proposed decision, course or action, or change by a network operator that, in the Director’s opinion, would raise a network security risk -</p> <p>(a) the Director must advise the network operator of the matter as soon as practicable <u>but within 10 working days of receiving the notification under section 47</u>.</p>
Section 50 – Assessment of response by network operator	Impose time limits.	(2) If the Director is satisfied that the proposal...will...prevent or mitigate the network security risk, the Director must <u>accept</u> the proposal...in writing <u>within 10 working days of receiving the network operator’s mitigation</u>

		<u>proposal under section 49(3).</u>
Section 52 – Director may refer the matter to Minister	Impose time limits.	<p>If the Director considers that the proposal or part of the proposal does not prevent or mitigate a significant network security risk, the Director may –</p> <p>(a) refer the matter to the Minister to make a direction under section 54 <u>within 10 working days of receiving the network operator’s mitigation proposal under section 49(3);</u> and</p> <p><u>(aa) at the same time as referring the matter to the Minister, refer the matter to the Technical Advisory Board to make a recommendation to the Minister before deciding to make a direction under section 54; and</u></p> <p>(b) inform the network operator <u>in writing</u> that it may make submissions on the matter directly to the Minister, and specify the <u>reasonable</u> time frames for making those submissions.</p>
Section 54 – Minister may make direction	Impose time limits.	<p>...</p> <p>(1)(c) the Minister <u>having considered the recommendation of the Technical Advisory Board is satisfied on reasonable grounds</u> that exercising his or her powers under this section is necessary to prevent, mitigate, or remove a significant network security risk;</p> <p>...</p> <p>(3)(b) be satisfied <u>on reasonable grounds</u> that the direction complies with section 8(2) to (4) and is consistent with the purpose in section 7.</p> <p><u>(3A) The Minister must issue the direction, or advise that no direction will be issued, in writing to the affected network operator within 20 working days of the receipt of the network operator’s submissions, or within 40 working days of the referral under section 52 if no submissions are received.</u></p>
Section 57 – Registration information	<p>Ensure the protection and proper treatment of information provided to the Registrar.</p> <p>Ensure that the information is required for operational use.</p>	<p>(1) The information referred to in section 56(b) is as follows (to the extent that the information is applicable):</p> <p>...</p> <p>(c) in the case of a network operator that offers retail</p>

	Limit the information to be provided upon registration to ensure that it is necessary for the purposes of the Act.	<p>services, an estimate of the total number of end-users across all telecommunications services and all public telecommunications networks.</p> <p><u>(3) All information provided to the Registrar under this section must:</u></p> <p><u>(a) only be used for the purpose for which it was provided under the Act;</u></p> <p><u>(b) be destroyed as soon as it has been superseded by updated information, or is no longer required for the purpose for which it was obtained; and</u></p> <p><u>(c) be kept under an obligation of confidence.</u></p> <p><u>(4) Within 12 months of the Act receiving Royal Assent, the Registrar shall audit whether the registration information has been necessary for surveillance agencies to carry out their functions under the Act and where certain information has not been required for that purpose, that information shall no longer be required.</u></p>
Section 61 – Operation of and access to register	Where the registration information is not necessary for surveillance agencies to carry out their functions under the Act the registration information should no longer be required.	<u>(5) Where the Registrar suspends the operation of the register under subsection (4) the Registrar shall notify in writing all network operators that the provision of certain registration information is no longer required.</u>
Section 62 – Registrar must keep register secure	Given the magnitude and sensitive nature of information being provided to the Registrar, further protections of the information are required.	<p><u>(1) The Registrar must use all reasonable endeavours take reasonable steps to ensure that the register is not available for access or searching by any person other than a designated officer...</u></p> <p><u>(3) The relevant network operators will be advised and given the opportunity to input into any request under the Official Information Act which relates to the information provided by a network operator to the Registrar under this Act.</u></p>
Section 63 – Network operators must notify Registrar of key changes	Remove the requirement to provide anything other than an annual update of the geographical coverage or types of telecommunications services provided since that information alone is not likely to result in the altering of level of interception obligation on a particular network operator. It therefore	<p>(d) the geographical coverage of the network operator's telecommunications services and public telecommunications networks.</p> <p>(e) the types of telecommunications services provided by the network operator.</p>

	results in compliance cost (e.g. having processes to monitor changes to this information) for no real operational value.	
Section 64 – Annual update	Ensure the amount of confidential information held by the Registrar is kept to a minimum by ensuring that superseded information is deleted upon it being updated.	<u>(4) Upon an annual update, all superseded information will be destroyed.</u>
Section 67 – Appointment of designated officers	The appointment of a designated officer should be agreed upon by the surveillance agencies given the important nature of their role in deciding exemption applications.	<u>(1) Upon consultation and agreement between the surveillance agencies, the Commissioner of Police must, by notice in the Gazette, appoint 1 or more suitable persons as designated officers for the purposes of this Act.</u>
Section 72 – Designated officer may require information in order to assist surveillance agency	The request for information should be extended to service providers to allow agencies an opportunity to assess whether a service provider is in fact a network operator where there is disagreement between the surveillance agency and the entity in question.	<u>(1) If a designated officer considers it necessary or desirable for any specified purpose, the designated officer may, by written notice service on any network operator or service provider...</u>
Section 83 – Breach notice may be issued for minor non-compliance	The timeframe for complying with a breach notice should be reasonable.	<u>(4) A must comply with the breach notice within the reasonable time period and in the manner specified in the notice...</u>
Section 84 – Breach notice may request consent to enter and inspect in connection with duties under Part 2	This audit request should be extended to service providers to allow surveillance agencies an opportunity to assess whether a service provider is in fact a network operator where there is disagreement between the surveillance agency and the entity in question.	<u>(2) A breach notice may request a network operator or service provider to consent to the surveillance agency entering a relevant place...</u>
Section 85 – Enforcement notice may be issued for serious non-compliance	Ensure that, even for instances of serious non-compliance, an opportunity to rectify the issue is provided before more serious enforcement action is taken.	<u>(2)(c) and may request that the person remedy the non-compliance within a reasonable period of time.</u> <u>(3) Before issuing an enforcement notice the surveillance agency should first consult with the person regarding the</u>

		<u>surveillance agency's concerns about non-compliance.</u>
Section 97	Where appropriate the preferred approach will be to involve a national security cleared employee on behalf of the defendant.	
Section 100	The operator or service provider's operational expense for assisting an agency to execute a warrant should still be available under section 11.	(3) this section - (a) does not apply to a network operator that is complying with duties only under section 11. ...
Section 103	Ensure adequate protection is given to operators under the Act. We refer to the indemnity in section 231 of the Insurance (Prudential Supervision) Act 2010 as providing analogous protection for banks and statutory managers.	(2) No person to whom this section applies is liable for an act done <u>or purported to be done</u> or omitted to be done in good faith <u>arising from or in the course of</u> - (a) in the performance of a duty imposed by or under this Act; or (b) in the exercise of a function or power conferred by or under this Act. ... <u>(4) The Crown will indemnify any person described in section 103(1) for any liability that arises from the performance of a duty under the Act or in the exercise (or purported exercise) of a power conferred under the Act.</u>