Telecommunications (Interception Capability and Security) Bill

Government Bill

As reported from the Law and Order Committee

Commentary

Recommendation

The Law and Order Committee has examined the Telecommunications (Interception Capability and Security) and recommends by majority that it be passed with the amendments shown.

Introduction

This bill seeks to repeal and replace the Telecommunications (Interception Capability) Act 2004 in order to ensure that interception obligations applying to the telecommunications industry are clear, do not impose unnecessary compliance costs, and are sufficiently flexible to respond to current and future operational needs and technological developments. It also seeks to require network operators to engage with the Government on network security matters, inform the Government of certain proposed decisions, courses of action, or changes in relation to an area of "specified security interest", and work with the Government to apply any specific risk-based and proportionate security measures.

The bill is split into four parts: part 1 sets out the preliminary provisions, part 2 interception duties, part 3 network security provisions, and part 4 registration, enforcement, and miscellaneous provisions.

This commentary covers the key amendments that we recommend to the bill. It does not cover minor or technical amendments.

Preliminary provisions

Interpretation

Under section 50 of the Search and Surveillance Act 2012, the Department of Internal Affairs or the New Zealand Customs Service can become law enforcement agencies subject to the criteria set out in that section. We recommend amending the definition of "law enforcement agency" in the bill to include a law enforcement agency that is appointed by Order in Council under section 50 of the Search and Surveillance Act 2012.

We consider that the definition of "security risk" in the bill as introduced is potentially too broad. We therefore recommend deleting "or economic well-being" from the definition of "security risk", and inserting a new definition of "national security" that includes the concept of economic well-being. We also recommend an amendment to clause 49 to exclude its application to minimal risks, and inserting new clauses 48A and 54A (which are discussed later in this commentary), to provide more certainty for network operators.

We recommend amending the definition of "service provider" to clarify that it includes any domestic or international service provider that provides or makes services available in New Zealand. We recommend the consequential deletion of subclause 24(6).

Principles relating to network security

We recommend inserting a new principle to clause 8, to the effect that when the Director of the GCSB is exercising any function or power related to network security, he or she should make decisions as soon as practicable. Consistent with the new principle, we recommend inserting new subclause 33B(2) in part 2 to include a requirement regarding a Minister's determination on an exemption.

Interception duties

Interception accessible

We recommend amending subclause 12(a) to specify that a network operator would be required to provide access only to a point of the public telecommunications network suitable for effecting an interception warrant or other lawful authority. Under the bill as introduced, there is no limit on the access a network operator would be required to provide, which we consider to be inappropriate from security and commercial points of view.

General practice

We recommend changes to the following clauses to set out operational provisions: clauses 17 and 35, to require that affected network operators be notified in writing; clauses 17, 19, 20, 35, 37, and 39, to require reasonable timeframes for procedures to be completed; clauses 20, 38, and 40, to require the Government to consult the telecommunications industry; and clause 30, to require that extensions to applications for exemption, variation, or revocation of exemption be notified within 20 working days.

Submissions

In the bill as introduced, the intended effect of submissions to an appeal, for example, on the ability of the Minister to make a decision is not made clear. We recommend amending clauses 19(1)(a), 35(6)(a), and 39(7) so that an absence of submissions would not prevent a decision being made.

Meaning of "delegate"

We recommend amending the definition of "delegate" in subclauses 19(5), 35(9), 39(11), and 54(5), so that the Minister could delegate only to another Minister, and could not delegate to a chief executive of a department. These clauses would override the delegation provision in section 28 of the State Sector Act 1988.

Duty to assist

The current Act requires all network operators and service providers to take all reasonable steps necessary to effect a warrant or other

lawful interception authority; these steps may include decryption. We recommend amending sub-paragraph 24(3)(b)(vi) and inserting new subclause 24(3A) to explicitly specify the limits of the obligation in relation to decryption. If a telecommunications service provider or network operator provided the encryption, it must take all reasonable steps to assist; if it did not, then it would not be obliged to do so. New subclause 24(3A) is consistent with the limits of existing decryption obligations in clause 10(4).

However, this clause would not require a service provider to execute a warrant where to do so would be in conflict with the law of any other jurisdiction. A service provider would be required to take all "reasonable steps" to execute a warrant, and acting in conflict with another jurisdiction's law would not be considered reasonable.

Minister's powers in determining a new application for exemption

Where an application for exemption or variation of an exemption had been declined, the applicant could apply to the Minister for a decision on the matter. We recommend inserting new clauses 32A, 33A, and 33B, and amending clause 33, to set out the Minister's powers in making such a decision and the process he or she must follow.

Review

The bill provides for a review of a direction issued under clause 35 requiring a service provider to have the same obligations as a network operator. We recommend inserting new subclause 36(2A) to specify the criteria that would have to be met for a person to be considered suitably qualified for the purposes of subsection (3). These criteria include experience in specified fields, no conflict of interest regarding the Minister's direction under clause 35, and an appropriate security clearance.

Ministerial direction relating to resold overseas telecommunications services

Under the bill as introduced, the Minister, on the application of a surveillance agency, could forbid the provision or supply in New Zealand of any telecommunications service that is provided from overseas and resold in New Zealand by a network operator. We rec-

ommend inserting new subclauses 39(2A) and 39(2B) to specify the criteria that the Minister would have to use when deciding whether to make such a direction, giving primacy to national security or law enforcement interests.

Network security

Network operators' duty to engage in good faith

We consider that the broad scope of the requirement to engage might lead to over-reporting and hamper interpretation of the bill. We recommend amending two clauses to address these concerns: subclause 45(1), to require network operators to engage with authorities only regarding risks that might arise from a proposed decision, course of action, or change, if implemented; and clause 48, so that the ability of the Director of the GCSB to issue exemptions would also apply to the duty to engage set out in subclause 45(1). We also recommend the insertion of new clause 54A (discussed later in this commentary), to provide more certainty for network operators.

Areas of specified security interest

As introduced, aspects of this clause are not clear or are too broad. To narrow the scope and improve clarity, we recommend amending paragraph 46(1)(d) to make it clear that it applies to data belonging to the customer or end user, as opposed to data about the customer, and to such data as is held on a public telecommunications network specifically.

We also recommend inserting paragraph 46(2)(a) to allow the Minister to make regulations amending or removing what constitutes an area of specified security interest. However, we recommend rewriting subclause 46(3) to require the Minister to consult registered network operators before making such regulations.

Exemption from section 45 or 47

To ensure the exemption provision is sufficiently flexible, we recommend inserting subclause 48(2) to allow the Director of the GCSB to grant an exemption as he or she sees fit. This would increase the likelihood of exemptions being granted in response to specific circumstances.

We also recommend inserting new paragraph 48(5)(a) to require notices of exemption issued to a class of network operators to be published on an internet site operated by the GCSB. This would avoid the need for a network operator within that class to apply to the GCSB for the exemptions in force.

Consideration of network security risk by Director or Minister

As introduced, the bill does not set out how the Director of, or the Minister for, the GCSB would be required to approach their consideration of network security risk. We recommend inserting new clause 48A to require the Director or the Minister to consider the likelihood of a particular decision compromising or degrading the telecommunications network or impairing the confidentiality, availability, and integrity of telecommunications on the network, and any potential flow-on effects, as set out in subclause 48A(1)(b). This is intended to clarify the matter for the industry.

Guidelines

We recommend inserting new clause 54A to allow the Director of the GCSB to issue guidelines on any requirements applying to network operators under part 3 of the bill. This would help network operators to comply with the legislation.

Registration, enforcement, and miscellaneous provisions

Classified security information in court

We recommend inserting new clauses 96A–96H to set out the court procedures for dealing with classified security information. They include requirements to keep information confidential and hold closed hearings if necessary; to appoint special advocates and allow them to access classified security information, participate in examinations of witnesses, make submissions to the Court, and communicate with the parties they represent; and they impose on the Crown a duty to provide access to the Court to the relevant classified security information.

Minority views

New Zealand Labour Party

The balance between privacy and security has not been met

Privacy is fundamental to an open democracy. Without privacy, there is no democracy. Likewise, security is also fundamental to democracy. Without security, there is no democracy. This creates a dilemma: a crucial public good and a core individual right. No society can maximize both at the same time. The dilemma is how does society ensure that both can co-exist and where they butt up against each other that there is robust debate and careful deliberation on how to achieve the best possible compromise or balance. With advances in technology and our increasing reliance on internet-based communications, this is the core dilemma of the modern age.

Edward Snowden's leaks have revealed that the United States and Britain's intelligence agencies are capable of intercepting vast amounts of internet traffic, that they have developed sophisticated data-mining tools; that the agencies cooperate with the private sector in their collection effort, that they spy on allies and that the government's code breakers have cracked encryption that was previously considered safe. It appears there are more revelations to come.

These revelations have occurred during the passage of this bill through its first reading and select committee. Yet the government has refused to engage in a wider discussion about the implications of these revelations on New Zealand's security environment; our relationship with our allies and the current and planned practices of our intelligence community to align itself with its counterparts.

Also, we have had another significant piece of legislation pass through the House which provides wider powers for the GCSB and importantly, a new power, to spy on New Zealand citizens. The bill gives effect to the Government Communications Security Bureau and Related Legislation Amendment Act (the Act).

Cyber security concerns have become paramount for New Zealand businesses generally. Tech companies are taking security provisions more seriously. The Snowden issue has put this to the fore. The public debate is just beginning. This legislation was an opportunity to allow that debate to happen in a way that embraced the views of the industry, civil society and our security agencies and those concerned

with protecting our economic and sovereign interests and our political alliances. That opportunity has been squandered by a Government which has railroaded through legislation against the cautioning voices of our local telco companies and also those of the increasingly important service providers, or over-the-top companies, such as Google, Facebook and Microsoft.

And the voices of civil society, the representatives of our legal community and many other organisations have been dismissed and ignored.

Labour opposes this bill. It has been rushed, it is ill-conceived, there has been no case made for the extraordinary expansion of powers to the GCSB and various Ministers. Sensible suggestions to improve the bill have mostly been rejected out of hand. Instead the scales have tipped towards unreasonable powers to secret agencies which have not proved their ability to adhere to the rule of law or to be modern and responsible 21st-century organisations. The government has over-reached in this bill.

Specifically, Labour's concerns are listed below.

Expansion of powers

The Government has argued that the bill does not alter the authority of surveillance agencies to intercept telecommunications, or reduce checks and balances on how these agencies can access and use private communications information. Labour and almost all submitters disagree.

The bill is a companion measure to the Act which would give the GCSB the right to carry out surveillance on New Zealanders. More technical in nature, the bill compels telecommunications companies to provide assistance to the GCSB in intercepting and decrypting customer communications and forces them to follow the spy agency's instructions on network security.

This is a fundamental expansion of the State's role in monitoring communications.

It expands the reach of interception obligations to a much wider group of companies—now including service providers as well. It gives the Minister the power to change the obligations impinging on a single company, or on a class of companies.

The Labour Party agrees with Internet NZ's submission that the challenge in this bill is to strike the appropriate balance between addressing national security concerns without introducing a permission-seeking process that is too involved and uncertain to incentivise network operators to innovate and to support a competitive telecommunications market. Part 3 of the bill introduces a regime that must by its very nature introduce transaction costs to the design and build of networks in New Zealand by requiring network operators to pass possible purchase and design decisions through the GCSB for approval.

Cost implications

Labour notes that supplementary submissions to the select committee by several network operators outlined potential significant annual operating costs and the potential capital expenditure costs. The committee did not seek advice on these supplementary submissions and the economic impact was therefore not taken into account.

The case for expansion of powers has not been made

During the hearing of submissions the Labour members consistently asked submitters whether they considered there was a case for the expansion of powers in this bill to the GCSB and to Ministers. Not one submitter agreed that there had been a case made for the expansion of those powers. The committee was not allowed to hear submissions from any of the surveillance agencies, including the GCSB, the SIS, or New Zealand Police, outlining the case for increased interception powers or expanded powers in network design and build. The committee heard one submission from the NZ Police Association, which, while well intentioned was unable to shed light on the rationale for increasing the GCSB and other surveillance agency powers. Labour believes the committee has been asked to change the legislation while blindfolded to the reasoning behind making the changes. This alone is a fundamental reason to oppose the bill and should be a warning to government never to treat a parliamentary committee with such contempt.

Definitions

The bill covers "network operators", "service providers", and "resold overseas telco services" in the name of national security, law enforcement and a vague term, economic well-being. The bill does not define economic well-being and instead gives discretion to the GCSB Director and a Minister to make that call with no requirement for public discussion or reference to an independent group.

We also note that surveillance agencies are defined by the bill as law enforcement or intelligence and security agencies. It is unclear from this definition whether the bill purports to allow foreign agencies as well as New Zealand agencies.

We believe that New Zealand's interests—in terms of national security, economic well-being, and protection of citizens' basic privacy rights—will be best served if New Zealand businesses have the flexibility to innovate, compete, and succeed in creating products and services that provide robust protection for the privacy rights of their customers, while also effectively supporting legitimate interception capabilities required by law where applicable.

"National security" is not defined anywhere in the bill. Yet the bill provides for national security and law enforcement to be given primacy over service availability, compliance costs and innovation. A surveillance agency can use the pretext of not revealing classified information to impose such costs and technical requirements on a service provider (or a class of service providers) which may drive it out of business or frustrate non-commercial operations.

On the application of a surveillance agency (Police, SIS, GCSB, the Department of Internal Affairs, and Customs) the Minister can require a service operator (or a class of service operators) to provide full interception capability like a network operator. There is a provision for the Minister's directions to be looked at by a three-member review panel. However, the Minister retains what we consider to be extraordinary powers and we oppose this.

"Deeming in" powers, unintended consequences and the conflict of law

During the course of the select committee discussions it became clear that the new "deem in" power granted to the Minister to extend interception capability obligations beyond the traditionally recognised

group of network operators who have that obligation under current legislation.

Labour acknowledges the position of network operators in NZ who argue they are at a competitive disadvantage because they are under current law unable to offer innovative services that do not have an interception capability.

However, under the proposed law we see two serious issues which could put at risk future innovation and the offering of services in New Zealand, and which could put NZ law at odds with laws in other jurisdictions.

Microsoft in particular gave a very strong submission describing this provision as a dramatic change in the law. They pointed out that New Zealand's surveillance laws had been designed for an era in which spying meant tapping into someone's analogue phone calls, but the bill took things much further and was no longer about just tapping into the telephone exchange. There were now a diversity of data connections carrying every imaginable service such as games, banking, education services, entertainment, company and government meetings, shopping, email and documents. Many of these were never subject to interception capability obligations in the pre-digital world.

Potentially, the GCSB could use the law change to force any provider of those online services to change their technology or business model, including in ways which might fundamentally undermine the security of those services.

Labour agrees that an obligation to have interception capability on a fundamentally different technology in our view needs to be considered on its merits and given more thought and consideration. It should not be swept up in broad legislation that gives wide powers to surveillance agencies and Ministers.

Encryption

Labour considers this to be one of the most vexed and confusing parts of the bill. The submissions on this matter took up much of the time of the committee and what has ended up in the bill provides a gaping hole in the ability of the law to meet the government's supposed intentions. Labour considers there are inconsistencies and unintended consequences in this part of the bill which are deeply concerning for

New Zealand's technology community and for our economic development.

The two most significant issues are the duty to assist for a company which has encryption at the core of its business model to provide a decryption capacity to surveillance agencies. The capture of such companies and software services developed in New Zealand could not only be counter-productive to business innovation but could result in reputational issues.

The uncertainty around how this bill applies to companies who are built on a business model which vests the power of decryption in the customer is still unclear. Increasingly, businesses and individuals are looking for ways to store and send their data where they (as customers) have control over decryption. As amended, the bill requires that if a telecommunications service provider or network operator provides the encryption (capacity), it must take all reasonable steps to assist; if it does not, then it is not obliged to do so. The bill has not explored the unintended consequences for New Zealand-based software products, which may be caught up in a duty to assist because they (as the business owner) have control over encryption.

Labour agrees with submitters who argued that encryption is incompatible with lawful intercept. We believe that this section of the bill requires a much wider discussion about what is and isn't possible to intercept lawfully being mindful of the balance between privacy and security and taking into account the impact on new and existing business models.

If New Zealand sees cloud-based technology service companies as an important part of an emerging tech-based economy, why is this bill creating unnecessary and untested risks to that?

There are countless New Zealand tech companies that may find themselves caught up in requirements to provide interception capability and with associated damaged reputational perceptions if this bill proceeds in its current form without wider debate and robust checks and balances to ensure that the over-reach of security requirements is not damaging New Zealand's economic growth. The bill is still unclear on how this requirement may affect existing and future businesses in New Zealand which provide an encryption capacity.

The notification regime and the chilling effect on innovation

Labour agrees with all submitters who argued that the obligations placed on network operators in Part 3 of the bill will have a chilling effect on innovation and competition because the bill provides expansive powers to the GCSB, backed up by a Minister to moderate or restrict the ability of New Zealand network operators to deploy new technologies.

This bill will create a chilling effect on the business development of network operators in New Zealand. As noted in many submissions on this bill, under the regime in Part 3 of the bill, a network provider may seek permission to change part of its network and, while waiting for permission to be granted, lose a business opportunity. Also, if network providers are cognisant of approved additions, the effect on innovation could be dampened and they may elect to follow the known path as opposed to a new path that could take an undue amount of time for permission.

Despite strong recommendations for the bill to include a timeframe within which the GCSB Director must respond to a notification, no such timeframe has been required, instead requiring the GCSB Director to make decisions "as soon as practicable".

This again provides extraordinary discretion to the GCSB and will impact on a network's ability to conduct its business.

There is no system in place to ensure that surveillance agencies can keep up with rapidly developing technology being deployed within the New Zealand environment in terms of expertise or cost. The bill does not provide adequate opportunity for a network operator to challenge or appeal decisions made by the Director or a Minister.

There is no indication that the new roles set out for the GCSB will be adequately resourced to allow them to be performed effectively. Labour believes that recent events where the GCSB has been shown to be lacking in judgement in spying on New Zealand citizens unlawfully provide urgent incentives for a wide-ranging review of its functions and ability to perform those functions before such legislation is enacted.

Conflict of law

Labour is dubious about the assurances given by officials that the bill could require non-New Zealand service providers to provide access

to customer data to the New Zealand government, is not at odds with their domestic legal obligations. There has been strong advice regarding this matter from several submitters that the internet's global nature means that service providers based outside New Zealand may find themselves under conflicting legal obligations.

Under Part 2, Subpart 5 of the bill the Minister may direct service providers to give surveillance agencies access to customer data. Clause 24(6) of the original bill stated that this applied regardless of whether the service provider is New Zealand based.

As noted in the submissions of Google, Facebook and Microsoft, this would create a catch 22 situation. Under the US Electronic Communications Privacy Act, US-based service providers can only disclose customer data to non-US law enforcement agencies if it is directed to do so through a warrant issued by a US court or law enforcement agency.

Yet under the bill as originally drafted, service providers are required to disclose or provide access to customer data to New Zealand, or perhaps other, surveillance agencies.

By complying with the bill, these service providers would be in violation of US law. And by refusing to comply with the bill, these service providers would also be in violation of New Zealand law.

A late amendment to the bill says Clause 24 (6) has been deleted and the commentary now says this section (Duty to assist) would not require a service provider to execute a warrant where to do so would be in conflict with the law in another jurisdiction. It says the service provider is required to take all "reasonable steps" to execute a warrant and acting in conflict with another jurisdiction's law would not be considered reasonable.

This is a very late addition to the bill and should have been discussed with the committee in more depth. Labour believes this is an attempt to appease certain submitters with a piecemeal response rather than address a substantive problem identified in the bill.

And, in the event that a service provider's services are resold in New Zealand by a network operator, under clause 39 of the bill, the Minister may effectively prevent the service provider from doing business in New Zealand. The only concession made here is to set out a list of criteria which the Minister would have to use in making this decision.

Lack of checks and balances and independent oversight

The bill empowers a handful of Ministers, without independent oversight, to order service providers to become intercept capable – and thus potentially to open up years of customer correspondence for collection by the government for the purposes "law enforcement" or "national security".

The directive process, covering both interception and network security, where, on the advice of a security agency, the Minister can issue a direction that could compel a network operator to:

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

Many submitters argued this would impose significant risk and potential financial impacts on providers if a directive was issued, under an arbitrary process. It is essential that any request for a directive is appropriately considered, tested and consulted upon.

The Government has little incentive to consider the financial impact on the impacted service provider. Appeal rights are limited to judicial review. And yet, impacted providers have limited ability to be consulted or participate in the decision making process. There are some costs which will be borne by the surveillance authority incurred by a network operator or service provider in providing interception assistance to an agency.

The bill is silent on whether costs incurred following changes to network operator occurred as a result of complying under Part 3 of the bill will be borne by the network.

Labour supported submissions by all network operators (telcos) that a joint industry/security technical advisory board should be established to evaluate any application for a Ministerial directive as an appropriate check and balance measure and argues strongly that this bill puts too much power in the hands of a surveillance agency with the ultimate decision-making power left in the hands of a Minister who is not required to take external advice.

The Bill of Rights test

Labour supports Internet NZ's submission in calling for a thorough test of the bill against the New Zealand Bill of Rights Act. The New Zealand Law Society in its submission on the Act called for the same.

In its sparingly used direct reporting power to the Prime Minister, the Human Rights Commission, determined that the Ministry of Justice Bill of Rights vet of the Act and the bill fell short.

Just as the Act failed to provide adequate safeguards for peoples' privacy to balance the intrusive power of the State to collect the private information of New Zealanders, as implementing legislation the bill has failed as well, as the Government has refused to add adequate safeguards.

Mitigating measures inadequate and window-dressing

The Government's attempts to provide some measures to address the criticism of the lack of checks and balances, unfettered powers of the GCSB and Ministers and the lack of independent oversight of decision-making has fallen flat in this bill. Requiring the GCSB Director to make decisions on network security operations as soon as practicable, providing a list of criteria that the Minister must use when deciding to make a direction to forbid the resale in New Zealand of a service, and requiring the GCSB and Minister to consider whether its decisions about a network might compromise its availability, integrity or confidentiality are steps forward, but there are no accompanying transparency measures or independent oversight over those decisions. They remain secret with no accountability.

Conclusion

There are many reasons to oppose this bill. It is ill-thought out, rushed and the government has refused to take account of core concerns raised by submitters. There has been no case made for the expanded powers of the GCSB and of Ministers.

Labour robustly opposed its companion law which expands the powers of the GCSB to spy on New Zealand citizens.

The proposed legislation as currently drafted is not clear enough to fully evaluate, but nonetheless raises significant concerns that it may be ineffective and have unintended consequences that undermine its primary objectives.

We therefore oppose this bill and will in government make wide-ranging changes to the GCSB Act and the bill after conducting an extensive inquiry into all security agencies.

Green Party

The Green Party opposes this bill. We are very concerned that the changes to the interception capabilities are being changed at a time when there are so many questions about the role, scope, and ability of the intelligence agencies in New Zealand, and the privacy of New Zealanders. The Green Party firmly believes that there needs to be a wide-ranging, independent inquiry into New Zealand's intelligence services before the power of these services is extended any further.

The Green Party acknowledges the purported intention of this bill to ensure interception capability in situations of criminality, and also the desire to protect telecommunications systems and users from security risks. However, this bill neither ensures effectiveness for those purposes nor protects the rights and freedoms of New Zealanders.

Citizens in a democracy have the right to understand how and when they could be surveilled. This bill raises many questions about the fundamental rights and freedoms of New Zealanders. There are grey areas around the warrant process, and limited accountability to Parliament or the public.

The bill is the mechanism providing access, with very limited oversight, for an unprecedented level of surveillance capability by the Security Intelligence Service, the Government Communications Security Bureau, the New Zealand Police, and potentially the New Zealand Customs Service, and the Department of Internal Affairs. This bill also gives the GCSB unprecedented powers of veto over how network providers can operate their businesses. It is adding a layer of bureaucracy over everything these companies do and is entrusting this agency with the central planning of the telecommunications industry.

The bill goes some way in reducing compliance costs to telecommunications network providers but leaves much in doubt and may restrict development and innovation in information technology. This bill will hold back our ICT sector and could discourage investment and jobs. These changes will slow software development and make our ICT industry susceptible to additional costs and uncertainties, particularly as they will be required to deal with a non-transparent Government department.

The flexibility of exemptions for a network operator, class of network or network service, while appearing practical, also leaves uncertainty in its application.

The bill is uneven in its application of interception capability among providers, and cannot address some technical features of encryption/decryption which brings into question the bill's effectiveness in addressing purported security surveillance needs.

New Zealand First Party

New Zealand First holds the view that the issues covered by this bill are too broad and disparate to be dealt with by a single piece of legislation.

Network security is a pressing issue which requires the timely attention of the House, and the expeditious passing of legislation to facilitate the protection of New Zealand's data networks by way of the exclusion of hardware, of certain types or from certain suppliers, identified as being potentially risk-bearing. This we regard as being a singular issue, which we support.

Interception capability however is both a less urgent concern, and one which has generated a great deal of controversy.

We note that an overwhelming majority of public and industry submissions are opposed to some or all of the proposed legislative changes.

There are unresolved issues and unanswered questions surrounding the cost to network providers, the exclusion of smaller providers, the non-inclusion of over-the-top service providers, and the commercial implications of having OTT providers subject to requirements which may limit the availability of certain products and services to the New Zealand market. In addition several submitters suggested that aspects of the proposed changes may limit innovation and expansion in some areas of information technology in New Zealand. Many submitters were of the opinion that the exclusion of small providers, and of OTT services, would largely negate the effectiveness of the law as proposed.

While these issues remain unresolved, and while existing legislation provides for an alternative framework through which the aims of the bill may be addressed, we feel it is precipitous to proceed with this part of the bill.

New Zealand First suggests that the bill be divided into two distinct bills, in order to address these separate concerns. We may yet choose to pursue this option by way of a supplementary order paper.

In the event that the bill is so separated, New Zealand First will support the network security provisions as outlined. However as the bill presently stands, we are unable to support it in its entirety, due to our concerns as detailed here.

Appendix

Committee process

The Telecommunications (Interception Capability and Security) was referred to the committee on 8 May 2013. The closing date for submissions was 13 June 2013. We received and considered 88 submissions from interested groups and individuals. We heard 17 submissions.

We received advice from the Ministry of Business, Innovation and Employment, the Department of Prime Minister and Cabinet, and the New Zealand Police. The Regulations Review Committee reported to the committee on the powers contained in clauses 3, 19, 20, 29–34, 35–38, 39, and 40.

Committee membership

Jacqui Dean (Chairperson)
David Clendon
Kris Faafoi
Hon Phil Goff
Hon Todd McClay
Ian McKelvie
Mark Mitchell
Richard Prosser
Lindsay Tisch

For this item of business, Steffan Browning replaced David Clendon and Clare Curran replaced any Labour member.

Key to symbols used in reprinted bill

As reported from a select committee

text inserted by a majority

~~text deleted by a majority~~

Hon Amy Adams

Telecommunications (Interception Capability and Security) Bill

Government Bill

Contents

Part 4
Registration, enforcement, and miscellaneous provisions

The Parliament of New Zealand enacts as follows:

1 Title

This Act is the Telecommunications (Interception Capability and Security) Act **2013**.

2 Commencement

(1) **Part 1**, **subpart 4 of Part 2**, and **subparts 1, 2, 7, and 8 of Part 4** come into force on the date that is 3 months after the date on which this Act receives the Royal assent.

(2) The rest of this Act comes into force on the date that is 6 months after the date on which this Act receives the Royal assent.

Part 1
Preliminary provisions

General

3 Interpretation

(1) In this Act, unless the context otherwise requires,—

annual update means an update under **section 64**

applicant means a person that applies for registration under **section 56**

authorised person means any person authorised to execute or assist in the execution of an interception warrant or other lawful interception authority

call associated data, in relation to a telecommunication,—

(a) means information—

(i) that is generated as a result of the making of the telecommunication (whether or not the telecommunication is sent or received successfully); and

(ii) that identifies the origin, direction, destination, or termination of the telecommunication; and

(b) includes, without limitation, any of the following information:

(i) the number from which the telecommunication originates:

(ii) the number to which the telecommunication is sent:
(iii) if the telecommunication is diverted from one number to another number, those numbers:
(iv) the time at which the telecommunication is sent:
(v) the duration of the telecommunication:
(vi) if the telecommunication is generated from a mobile telephone, the point at which the telecommunication first enters a network; but

(c) does not include the content of the telecommunication

chief executive means a person occupying the position of chief executive, by whatever name called, or the person who performs substantially the same function

classified information means information described in **section 96(2) and (3)**

compliance order means an order made by the High Court under **section 87**

customer means a person who receives telecommunications services from, and has an account or billing relationship with, a network operator

designated officer means a person appointed under **section 67**

Director has the same meaning as in section 4 of the Government Communications Security Bureau Act 2003

documents, in **subpart 4 of Part 4**, means documents (within the meaning of section 4(1) of the Evidence Act 2006) in the possession or under the control of the network operator

end-user, in relation to a telecommunications service, means a person who is the ultimate recipient of that service or of another service the provision of which is dependent on that service

equipment, in this Part and **Parts 2 and 3**, means both hardware and software

full interception capability means the capability to intercept a telecommunication as described in **section 10**

information, in **subpart 4 of Part 4**, means information in the possession or under the control of the network operator

infrastructure-level service means any service that provides the physical medium over which telecommunications are transmitted (for example, optical fibre cable), but does not include the device or equipment that generates, transmits, or receives any telecommunication signal

intelligence and security agency means—

(a) the New Zealand Security Intelligence Service; or

(b) the Government Communications Security Bureau

intercept, in relation to a private telecommunication, includes hear, listen to, record, monitor, acquire, or receive the telecommunication—

(a) while it is taking place on a telecommunications network; or

(b) while it is in transit on a telecommunications network

intercept accessible, in relation to a network or service, means the capability described in **section 12**

intercept ready, in relation to a network or service, means the capability described in **section 11**

interception warrant means a warrant that is issued under any of the following enactments:

(a) section 53 of the Search and Surveillance Act 2012:

(b) section 4A(1) or (2) of the New Zealand Security Intelligence Service Act 1969:

(c) section ~~17~~ 15A(1)(a) of the Government Communications Security Bureau Act 2003

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~~

(b) a specified law enforcement agency within the meaning of section 50 of the Search and Surveillance Act 2012 that is approved by an Order in Council under that section to use interception devices

Minister means the Minister of the Crown who, under the authority of any warrant or with the authority of the Prime Minister, is for the time being responsible for the administration of this Act

Minister for Communications and Information Technology means the Minister of the Crown who, under the authority of any warrant or with the authority of the Prime Minister, is for the time being responsible for communications and information technology

Minister ~~of~~ responsible for the Government Communications Security Bureau means the Minister who, under the authority of any warrant or with the authority of the Prime Minister, is for the time being responsible for the administration for the department of State established under the Government Communications Security Bureau Act 2003

Minister of Trade means the Minister of the Crown who, under the authority of any warrant or with the authority of the Prime Minister, is for the time being responsible for trade

national security, in relation to New Zealand, includes its economic well-being

~~**network operations centre** means a unit that a network operator has designated as being responsible for assuring the operation, performance, or security of a telecommunications network and—~~

~~(a) that is equipped with equipment that is appropriate for carrying out that responsibility; and~~

~~(b) whose duties may, without limitation, include 1 or more of the following activities:~~

~~(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~~

network operations centre means any part of an organisation or a network that is responsible for controlling the operation, performance, or security of a public telecommunications network (whether or not any of those activities are outsourced)

network operator means—

(a) a person who owns, controls, or operates a public telecommunications network; or

(b) a person who supplies (whether by wholesale or retail) another person with the capability to provide a telecommunications service

network security risk means any actual or potential security risk arising from—

(a) the design, build, or operation of a public telecommunications network; or

(b) any interconnection to or between public telecommunications networks in New Zealand or with telecommunications networks overseas

number—

(a) means the address used by a network operator or a telecommunications service for the purposes of—

(i) directing a telecommunication to its intended destination; and

(ii) identifying the origin of a telecommunication; and

(b) includes, without limitation, any of the following:

(i) a telephone number:

(ii) a mobile telephone number:

(iii) a unique identifier for a telecommunication device (for example, an electronic serial number or a Media Access Control address):

(iv) a user account identifier:

(v) an Internet Protocol address:

(vi) an email address

other lawful interception authority—

(a) means an authority to access an information infrastructure ~~a computer system of a specified foreign organisation or a foreign person~~ (within the meaning of the Government Communications Security Bureau Act 2003) that is granted under section ~~19~~ 15A(1)(b) of that Act; and

(b) includes an authority to intercept a private communication (whether in an emergency situation or otherwise) that is granted to any member of a surveillance agency under any other enactment

outsourcing arrangement means any arrangement (whether contractual or otherwise) entered into by a network operator

and another person within New Zealand (other than a surveillance agency) that enables the sharing of services for the purpose of meeting any interception capability requirements in this Act

public data network—

(a) means a data network used, or intended for use, in whole or in part, by the public; and

(b) includes, without limitation, the following facilities:

(i) Internet access; and

(ii) email access

public switched telephone network means a dial-up telephone network used, or intended for use, in whole or in part, by the public for the purposes of providing telecommunication between telecommunication devices

public telecommunications network means—

(a) a public switched telephone network; and

(b) a public data network

purely resold telecommunications service means any service—

(a) that is supplied or provided to a network operator (A) ~~(the **customer**) other than for the customer's own use or consumption~~; and

~~(~~

(b) that (A) ~~the customer~~ resells, supplies, or provides to another person~~, body, or organisation~~ without making any technical modification to that service

register means the register of network operators established under **section 58**

Registrar means the person appointed as the Registrar of network operators under **section 68**

responsible Ministers means—

(a) the Minister in charge of the New Zealand Security Intelligence Service; and

(b) the Minister responsible for the Government Communications Security Bureau; and

(c) the Minister of Police

security risk means any actual or potential risk to New Zealand's national security ~~or economic well-being~~

service provider—

(a) means any person who ~~provides~~, from within or outside New Zealand, provides or makes available in New Zealand a telecommunications service to an end-user (whether or not as part of a business undertaking and regardless of the nature of that business undertaking); but

(b) does not include a network operator

significant network security risk means a network security risk that is a significant risk to New Zealand's national security ~~or economic well-being~~

surveillance agency means—

(a) a law enforcement agency; or

(b) an intelligence and security agency

telecommunication device—

(a) means any terminal device capable of being used for transmitting or receiving a telecommunication over a network; and

(b) includes a telephone device

wholesale network service means a service, other than an infrastructure-level service or a purely resold telecommunications service, that—

(a) is provided by a network operator (**network operator A**) only to 1 or more other network operators; and

(b) is provided exclusively over 1 or more networks that are owned, controlled, or operated by network operator A~~; and~~.

~~(c) is not for the other network operator's own consumption; and~~

~~(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.~~

(2) In this Act, unless the context otherwise requires, **network**, **telecommunication**, **telecommunication link**, **telecommunications service**, and **telephone device** have the meanings given to them by section 5 of the Telecommunications Act 2001.

4 Act binds the Crown

This Act binds the Crown.

Purposes and principles

5 Purpose of this Act relating to interception capability

The purpose of this Act in relation to interception capability is to—

(a) ensure that surveillance agencies are able to effectively carry out the lawful interception of telecommunications under an interception warrant or any other lawful interception authority; and

(b) ensure that surveillance agencies, in obtaining assistance for the interception of telecommunications, do not create barriers to the introduction of new or innovative telecommunications technologies; and

(c) ensure that network operators and service providers have the freedom to choose system design features and specifications that are appropriate for their own purposes.

6 Principles relating to interception capability

The following principles must be applied by persons who exercise powers and carry out duties under this Act in relation to interception capability, if those principles are relevant to those powers or duties:

(a) the principle that the privacy of telecommunications that are not subject to an interception warrant or any other lawful interception authority must be maintained to the extent provided for in law:

(b) the principle that the interception of telecommunications, when authorised under an interception warrant or any other lawful interception authority, must be carried out without unduly interfering with any telecommunications.

7 Purpose of this Act relating to network security

The purpose of this Act in relation to network security is to prevent, sufficiently mitigate, or remove security risks arising from—

(a) the design, build, or operation of public telecommunications networks; and

(b) interconnections to or between public telecommunications networks in New Zealand or with networks overseas.

8 Principles relating to network security

(1) The following principles must, as far as practicable, be applied by the Director and each network operator in relation to network security risks:

(a) the principle that network security risks that might arise from a proposed decision, course of action, or change if implemented should be identified and addressed as early as possible:

~~(b) the principle that any proposed decision, course of action, or change that may raise a network security risk should be identified and addressed as early as possible.~~

(c) the principle that the Director and each network operator should work co-operatively and collaboratively with each other in relation to ~~**paragraphs (a) and (b)**~~ the principle in **paragraph (a)**.

(1A) The Director is subject to the principle that any decision or steps required of the Director for the purpose of exercising any function or power under **Part 3** should be made or taken as soon as practicable.

(2) The principle in **subsection (3)** must be taken into account by the Director or the Minister of Government Communications Security Bureau when making any decision or exercising any function or power under **Part 3** in relation to a network security risk.

(3) The principle that the decision or exercise of the function or power should be proportionate to the network security risk.

(4) In **subsection (3)**, a decision or an exercise of a function or power is proportionate to the network security risk if it—

(a) does not impose costs on network operators or telecommunications customers or end-users beyond those reasonably required to enable the network security risk to be prevented, sufficiently mitigated, or removed; and

(b) does not unduly harm competition or innovation in telecommunications markets.

Part 2
Interception capability duties

Subpart 1—Duty to have full interception capability

9 Network operators must ensure public telecommunications networks and telecommunications services have full interception capability

(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 in New Zealand, has full interception capability.

(2) However, **subsection (1)**—

(a) does not require a network operator to ensure that all components of the public telecommunications network or telecommunications service referred to in that subsection have full interception capability; and

(b) is sufficiently complied with if a network operator ensures, in whatever manner the network operator thinks fit, that at least 1 component of that network or service has full interception capability.

(3) Without limiting **subsection (1)**, the duty under that subsection to have full interception capability includes the duty to ensure that the interception capability is developed, installed, and maintained.

10 When duty to have full interception capability is complied with

(1) A public telecommunications network or a telecommunications service has full interception capability if every surveillance agency that is authorised under an interception warrant or any other lawful interception authority to intercept telecom-

munications or services on that network, or the network operator concerned, is able to—

(a) identify and intercept telecommunications without intercepting telecommunications that are not authorised to be intercepted under the warrant or lawful authority; and

(b) obtain call associated data relating to telecommunications (other than telecommunications that are not authorised to be intercepted under the warrant or lawful authority); and

(c) obtain call associated data and the content of telecommunications (other than telecommunications that are not authorised to be intercepted under the warrant or lawful authority) in a useable format; and

(d) carry out the interception of telecommunications unobtrusively, without unduly interfering with any telecommunications, and in a manner that protects the privacy of telecommunications that are not authorised to be intercepted under the warrant or lawful authority; and

(e) undertake the actions referred to in **paragraphs (a) to (d)** efficiently and effectively and,—

(i) if it is reasonably achievable, at the time of transmission of the telecommunication; or

(ii) if it is not reasonably achievable, as close as practicable to that time.

(2) If a network operator, or an employee or agent of a network operator, undertakes the interception of a telecommunication on behalf of a surveillance agency under **subsection (1)**, the interception must be taken to be complete when the network operator provides the call associated data or the content of the telecommunication, or both, to the surveillance agency.

(3) A network operator must, in order to comply with **subsection (1)(c)**, decrypt a telecommunication on that operator's public telecommunications network or telecommunications service if—

(a) the content of that telecommunication has been encrypted; and

(b) the network operator intercepting the telecommunication has provided that encryption.

(4) However, **subsection (3)** does not require a network operator to—

(a) decrypt any telecommunication on that operator's public telecommunications network or telecommunications service if the encryption has been provided by means of a product that is—

(i) supplied by a person other than the operator and is available ~~on retail sale~~ to the public; or

(ii) supplied by the operator as an agent for that product; and

(b) ensure that a surveillance agency has the ability to decrypt any telecommunication.

(5) In **subsection (1)(c)**, **useable format** means—

(a) a format that is determined by a notice issued under **section 40**; or

(b) a format that is acceptable to the network operator and the surveillance agency executing the interception warrant or other lawful interception authority.

Subpart 2—Reduced duties

Preliminary

11 Interception ready

(1) A network operator that is required by or under this subpart to ensure that a network or service is intercept ready—

(a) must pre-deploy access points at suitable and sufficient concentration points on the network or service to allow an interception warrant or any other lawful interception authority relating to any of its customers to be given effect:

(b) must reserve 1 or more network interfaces (that is, delivery ports) to which interception equipment can connect in order to deliver intercepted ~~communications~~ telecommunications to the surveillance agency; and

(c) must reserve, for each reserved interface referred to in **paragraph (b)**, sufficient bandwidth to deliver intercepted ~~material~~ telecommunications content and call associated data to the relevant surveillance agency; and

(d) when presented with an interception warrant or any other lawful interception authority must, free of charge,—

(i) provide ~~access to its~~ a suitable access point in its public telecommunications network or service for interception equipment:

(ii) co-operate with authorised persons and allow them access to its premises:

(iii) provide sufficient environmentally controlled space to house the interception equipment or provide sufficient backhaul to a suitable location where the equipment can be housed:

(e) must, when compliance with the Act is required to be tested, comply with **paragraphs (a) to (d)**.

(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.

12 Interception accessible

A network operator that is required by or under this subpart to ensure that a network or service is intercept accessible must, when presented with an interception warrant or any other lawful interception authority, be willing and able to—

(a) provide ~~access to its~~ a suitable access point in its public telecommunications network or service for interception equipment:

(b) co-operate with authorised persons and allow them access to its premises:

(c) provide sufficient environmentally controlled space to house the interception equipment or provide sufficient backhaul to a suitable location where the equipment can be housed.

Lower-level compliance duties

13 Network operators with fewer than 4 000 customers

(1) **Subsection (2)** applies if—

(a) a network operator makes and keeps a record of the number of customers it has each month; and

(b) the network operator has an average of less than 4 000 customers over a 6-month period; and

(c) the network operator has made and kept the record referred to in **paragraph (a)** for each month of the 6-month period referred to in **paragraph (b)**; and

(d) the network operator has notified the Registrar within 10 days after the last day of the 6-month period referred to in **paragraph (b)** of the matters described in **paragraphs (b) and (c)**.

(2) If this section applies, the network operator—

(a) does not have to comply with **sections 9 and 10**; but

(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.

(3) **Subsection (2)** continues to apply to the network operator as long as the network operator—

(a) continues to make and keep a record of the number of customers it has each month; and

(b) continues to maintain an average of less than 4 000 customers per month over each successive 6-month period.

(4) If the network operator referred to in **subsection (2)** subsequently has an average of 4 000 or more customers over a 6-month period (**disqualifying 6 months**),—

(a) the exemption in **subsection (2)(a)** ceases to have effect on the date that is 6 months after the disqualifying 6 months; and

(b) the network operator must comply with **subsection (2)(b)** until the date that the exemption ceases to have effect.

(5) This section is subject to **section 19**.

(6) The record referred to in **subsection (1)(a)** must be made on the same working day of each month (or the next available working day, if that is not practicable).

~~(7) In this section, **customer** means a person who has an account or a billing relationship with the network operator.~~

14 Infrastructure-level services

(1) A network operator does not have to comply with **sections 9 and 10** in respect of any infrastructure-level service provided by the network operator.

(2) This section is subject to **section 19**.

15 Wholesale network services

(1) A network operator does not have to comply with **sections 9 and 10** in respect of any wholesale network service provided by the network operator.

(2) A network operator who does not comply with **sections 9 and 10** in respect of a wholesale network service provided by the network operator must ensure that the wholesale network service is intercept accessible.

~~(3) Nothing in this section applies to—~~

~~(a) purely resold telecommunications services; or~~

~~(b) any wholesale network service that is provided to, or by, a network operator that is not subject to the laws of New Zealand.~~

(4) This section is subject to **section 19**.

Ministerial directions and regulations relating to lower-level compliance duties

16 Overview of sections 17 to 19

(1) The purpose of **sections 17 to 19** is to enable the Minister, on the application of a surveillance agency, to,—

(a) in the case of a network or service that by the operation of **section 13 or 15** is subject to a lower-level compliance duty, direct that the network or service or part of the network or service must instead be subject to a higher-level compliance duty:

(b) direct that an infrastructure-level service or part of that service must be subject to a higher-level compliance duty.

(2) The following duties are ranked according to the level of interception capability that is required to fulfil the duty (with the duty set out in **paragraph (a)** being the highest level compliance duty):

(a) the duty to comply with **sections 9 and 10**:
(b) the duty to be intercept ready:
(c) the duty to be intercept accessible.

(3) This overview is by way of explanation only. If any provision of this Part conflicts with this overview, the other provision prevails.

17 Application for direction

(1) A surveillance agency may make an application for a direction under **section 19** only if the surveillance agency considers that the interception capability or lack of interception capability on a network or a service adversely affects national security or law enforcement.

(2) The surveillance agency must, when applying for a direction, notify the affected network operator ~~of the application and the time frame by~~ in writing of the application and specify in the notice a time, which must be reasonable in the circumstances, within which submissions may be made to the Minister on the application.

18 Process following application for direction

(1) The affected network operator may make submissions to the Minister in relation to the application for direction within the time ~~frame~~ specified in the notice referred to in **section 17(2)**.

(2) The Minister must consult with the responsible Ministers and the Minister for Communications and Information Technology.

(3) The matters that the Minister must take into account are—
(a) whether the current level of interception capability on the affected network or service adversely affects national security or law enforcement; and
(b) whether the cost of compliance would have a serious adverse effect on the business of the network operator; and
(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: and

(d) any other matter that the Minister considers relevant in the circumstances.

(4) The Minister must give primacy to the matter described in **subsection (3)(a)**.

19 Direction

(1) The Minister must not make a direction under this section unless the Minister—

(a) has taken into account the views, if any, of the persons referred to in **section 18(2)** and the affected network operator; and

(b) has taken into account the matters set out in **section 18(3) and (4)**; and

(c) is satisfied on reasonable grounds that the direction is necessary for reasons of national security or law enforcement or both.

(2) The Minister may,—

(a) in the case of a network or service that under **section 13** must be intercept ready, direct that the network or service or part of the network or service must instead comply with **sections 9 and 10**:

(b) in the case of an infrastructure-level service that under **section 14** does not have to comply with **sections 9 and 10**, direct that the service or part of that service must instead—

(i) be intercept accessible; or

(ii) be intercept ready; or

(iii) comply with **sections 9 and 10**:

(c) in the case of a wholesale network service that by the operation of **section 15** must be intercept accessible, direct that the service or part of the service must instead—

(i) be intercept ready; or

(ii) comply with **sections 9 and 10**.

(3) The Minister must issue the direction in writing to the affected network operator.

(3A) The Minister must specify in the direction a time, which must be reasonable in the circumstances, by which the network operator must comply with the direction.

(4) The reasons for the decision must be set out in the direction, except those parts of the reasons that would reveal classified information.

(5) The Minister must not delegate to any person, other than another Minister, the power to make a direction under this section.

20 Regulations

(1) The Governor-General may, by Order in Council, on the recommendation of the Minister, make regulations—

(a) requiring all or part of a specified class of network or service to which **section 13** applies to comply with **sections 9 and 10**:

(b) requiring all or part of a specified class of infrastructure-level service to which **section 14** applies to—

(i) be intercept accessible; or

(ii) be intercept ready; or

(iii) comply with **sections 9 and 10**:

(c) requiring all or part of a specified class of wholesale network services to which **section 15** applies to—

(i) be intercept ready; or

(ii) comply with **sections 9 and 10**.

(2) The Minister must not recommend the making of regulations under **subsection (1)** unless the Minister ~~has~~—

(aa) has consulted with the telecommunications industry in accordance with the process set out in **subsection (3)**:

(a) has taken account of the matters set out in **section 18(3) and (4)**; and

(b) has consulted with the responsible Ministers and the Minister for Communications and Information Technology~~.~~; and

(c) is satisfied that the commencement of the regulations allows for a reasonable time for compliance.

(3) The consultation process referred to in **subclause (2)(aa)** requires that the Minister—

(a) publish, on an Internet site operated by the Ministry, a notice that—

(i) sets out the effect of the proposed regulations (**proposal**); and

(ii) invites submissions on the proposal to be made by a specified date; and

(b) consider the submissions (if any) on the proposal.

Subpart 3—Related duties

21 Certain facilities not required to be intercept capable

A network operator is not required to have an interception capability on a telecommunication link that is used to interconnect 2 or more public telecommunications networks.

Compare: 2004 No 19 s 9

22 Design of networks not affected by this Part

This Part does not authorise a surveillance agency or the Minister to—

(a) require any person to adopt a specific design or feature for any network or service; or

(b) prohibit any person from adopting any specific design or feature for any network or service.

Compare: 2004 No 19 s 10

23 ~~Infrastructure-level services~~ Duties relating to infrastructure-level services

A network operator that provides an infrastructure-level service must, despite anything to the contrary in any deed, contract, or other enactment or rule of law,—

(a) ensure that the Registrar is advised of the names of all existing customers that purchase infrastructure-level services from the provider; and

(b) ensure that the Registrar is advised of the names of any new customer—

(i) at least 10 working days before providing or activating the infrastructure-level service to the customer; or

(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 to the customer.

24 Duty to assist

(1) A surveillance agency to whom an interception warrant is issued, or any other lawful interception authority is granted, may, for the purpose of requiring assistance in the execution of the warrant or lawful authority, show to either or both of the persons referred to in **subsection (2)**,—

(a) in the case of an interception warrant issued to an intelligence and security agency, a copy of the relevant parts of the warrant; or

(b) in any other case, a copy of the warrant or evidence of lawful authority.

(2) The persons are—

(a) a network operator; or

(b) a service provider.

(3) A person who is shown under **subsection (1)** a copy of an interception warrant or the relevant parts of the warrant, or evidence of any other lawful interception authority, must assist the surveillance agency by—

(a) making available any of the person's officers, employees, or agents who are able to provide any reasonable technical assistance that may be necessary for the agency to intercept a telecommunication or otherwise give effect to the warrant or lawful authority; and

(b) taking all other reasonable steps that are necessary for the purpose of giving effect to the warrant or lawful authority, including, but not limited to, assistance to—

(i) identify and intercept telecommunications without intercepting telecommunications that are not authorised to be intercepted under the warrant or lawful authority; and

(ii) obtain call associated data relating to telecommunications (other than telecommunications that are not authorised to be intercepted under the warrant or lawful authority); and

(iii) obtain call associated data and the content of telecommunications (other than telecommunications that are not authorised to be intercepted under the warrant or lawful authority) in a useable format; and

(iv) carry out the interception of telecommunications unobtrusively, without unduly interfering with any telecommunications, and in a manner that protects the privacy of telecommunications that are not authorised to be intercepted under the warrant or lawful authority; and

(v) undertake the actions referred to in **subparagraphs (i) to (iv)** efficiently and effectively and,—

(A) if it is reasonably achievable, at the time of transmission of the telecommunication; or

(B) if it is not reasonably achievable, as close as practicable to that time; and

(vi) decrypt telecommunications where the ~~operator or provider~~ person has provided ~~or applied~~ the encryption.

(3A) **Subsection (3)(b)(vi)** does not require the person to—

(a) decrypt any telecommunication on that person's public telecommunications network or telecommunications service if the encryption has been provided by means of a product that is—

(i) supplied by the person as an agent for that product; or

(ii) supplied by another person and is available to the public; and

(b) ensure that a surveillance agency has the ability to decrypt any telecommunication.

(4) A network operator or service provider must consult with the surveillance agency executing the warrant or lawful authority, regarding the most efficient way to undertake the decryption referred to in **subsection (3)(b)(vi)**.

(5) For the purposes of this section, a network operator may intercept a telecommunication on behalf of a surveillance agency.

~~(6) This section applies to a network operator or a service provider regardless of whether the network operator or service provider is—~~

~~(a) operating from within or outside New Zealand; or~~

~~(b) has any interception capability or any other duties under this Act.~~

(7) In **subsection (3)(b)(iii)**, **useable format** means—

(a) the format determined by a notice issued under **section 40**; or

(b) a format that is acceptable to—

(i) the network operator or service provider; and

(ii) the surveillance agency executing the warrant or lawful authority.

25 Wholesalers may charge

~~(1) A wholesaler who is required under an interception warrant or any other lawful interception authority to provide another network operator with access to the wholesaler's network may charge the other network operator, on a commercial basis, for any access, space, power, or any other thing or service that the wholesaler is required to provide for the purpose of giving effect to the warrant or lawful authority if—~~

~~(a) it is technically feasible to give effect to the warrant or lawful authority on the other network operator's network; and~~

~~(b) the wholesaler's assistance is sought because the other network operator did not comply with any obligation under this Part.~~

(1) If—

(a) a wholesaler is required under an interception warrant or any other lawful interception authority to provide another network operator (**A**) with an access point to the wholesaler's network; and

(b) the wholesaler's assistance is sought because A did not comply with any obligation under this Part,—

the wholesaler may charge A, on a commercial basis, for any access, space, power, or any other thing or service that the wholesaler is required to provide for the purpose of giving effect to the warrant or lawful authority.

(1A) A designated officer may notify A in writing that the wholesaler is entitled to charge A under this section.

(2) In this section, **wholesaler** means a network operator who provides wholesale network services.

26 Duty to minimise impact of interception on third parties

Every person who, under an interception warrant or any other lawful interception authority, intercepts or assists in the interception of a telecommunication must take all practicable steps that are reasonable in the circumstances to minimise the likelihood of intercepting telecommunications that are not authorised to be intercepted under the warrant or lawful authority.

Compare: 2004 No 19 s 14

27 Network operators may share resources

(1) Nothing in this Act prevents network operators from co-ordinating, sharing, or contracting for ~~interception~~ services (whether equipment or staff) in order to meet the interception capability requirements in the Act.

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

28 Obligations relating to arrangements for interception services

(1) Before a network operator enters into a contract or engages with any person for the provision of services to enable the network operator to comply with its obligations under this Part, the network operator must notify the Director in accordance with **section 47**, and comply with **section 63**.

(2) A network operator must ensure that any person that it enters into a contract or engages with for the provision of services to enable the network operator to comply with its obligations under this Part, complies with any applicable provisions of this Part.

Subpart 4—Exemptions

29 Exemptions

(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**:

(b) grant a network operator or class of network operators an exemption from all or any of the requirements of **section 13**:

(c) grant a network operator or a class of network operators an exemption from all or any of the requirements of **section 23**:

(d) vary or revoke an exemption referred to in **paragraph (a), (b), or (c)**.

(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 intercepted under an interception warrant or any other lawful authority.

(3) An exemption under **subsection (1)**—

(a) may, without limitation, apply to all or part of a specified service or network or class of service or network; and

(b) may be subject to any terms and conditions specified by the designated officer.

(4) The designated officer may grant an exemption under **subsection (1)** with or without application from a network operator.

30 Application for exemption

(1) A network operator may apply to a designated officer for an exemption or a variation or revocation of an exemption under **section 29(1)**.

(2) The designated officer must notify the applicant of receipt of the application as soon as practicable.

(3) The designated officer must advise the applicant of the decision as soon as practicable and no later than 20 working days after receipt of the application.

(4) The designated officer may extend the time ~~frame~~ referred to in **subsection (3)** if—

(a) the application relates to multiple services; or

(b) the application raises new or complex technical or legal issues; or

(c) responding within that time ~~frame~~ would cause unreasonable interference with the operations of a surveillance agency.

~~(5) If **subsection (4)** applies, the designated officer must as soon as practicable give the applicant a notice of extension.~~

(5) If **subsection (4)** applies, the designated officer must—

(a) extend the time referred to in **subsection (3)** to a date not later than 3 months after receipt of the application, or to any later date to which the designated officer and the applicant have agreed; and

(b) give the applicant a notice of extension within 20 working days of receiving the application.

(6) The notice of extension must set out the reasons for the extension and the new time ~~frame~~ by which the designated officer must respond.

31 Effect of application for exemption or variation

(1) ~~An applicant who has applied for an exemption under **section 29(1)** is~~The effect of an application under **section 29(1)** is that, from the date that receipt of the application is notified, ~~exempt from the obligation to which the application for exemption relates, until~~ to the date that the decision on the application is notified~~.~~—

(a) in the case of an application for exemption, the applicant is treated as being exempt from the obligation for which the exemption is sought; or

(b) in the case of an application to vary an exemption, the exemption is treated as being in force as varied.

(2) **Subsection (1)** does not apply to an applicant if—

(a) the designated officer considers, on reasonable grounds, that the applicant is persistently or repeatedly seeking the same or a similar exemption or variation in relation to the same matter, or seeking the same outcome, despite the application being refused; and

(b) the designated officer has notified the applicant accordingly.

32 Decision-making process

(1) The designated officer must, when considering whether to grant, vary, or revoke an exemption under **section 29(1)**, take account of all the following matters:

(a) national security or law enforcement interests; and

(b) the number of customers or end-users of the relevant network or service; and

(c) the cost of compliance with the obligation for which an exemption is sought; and

(d) whether compliance could be achieved appropriately by another means; and

(e) any other matter that the designated officer considers relevant in the circumstances.

(2) The designated officer must, when taking account of the matters set out in **subsection (1)**, give primacy to **subsection (1)(a)**.

(3) The designated officer must consult each of the surveillance agencies, as well the applicant (if any), on the proposed decision.

(4) The reasons for the decision must be set out in the decision, except those parts of the reasons that would reveal classified information.

(5) The designated officer must issue a written notice of the decision to the applicant or, in the case of a class exemption, to the class of network operators who are affected by the decision.

~~(6) Subpart 1 of Part 3 of the Legislation Act 2012 does not apply to an exemption issued under this section.~~

(6) An exemption applying to a class of network operators that is granted, varied, or revoked under **section 29** is not a disallowable instrument for the purposes of the Legislation Act 2012 and does not have to be presented to the House of Representatives under section 41 of that Act.

Application to Minister

32A Application to Minister

(1) A network operator whose application for an exemption or variation of an exemption has been wholly or partly declined, or whose exemption has been or is to be revoked, may apply to the Minister for a decision.

(2) An application to the Minister must be made within 20 working days after the date on which the designated officer's decision on the application is issued, or the exemption is to be revoked.

(3) The Minister must notify receipt of the application as soon as practicable.

(4) An application to the Minister must not be materially different from the original application.

33 ~~Decision making at ministerial level~~ Minister may grant, vary, or revoke exemption

~~(1) A network operator whose application for an exemption or variation of an exemption has been wholly or partly declined, or whose exemption has been or is to be revoked, may apply to the Minister for a decision.~~

~~(2) For the purpose of an application to the Minister, the Minister has all the functions, powers, and duties of a designated officer under this subpart, and **sections 29 to 32** apply with all necessary modifications except that references to a designated officer must be read as references to the Minister.~~

~~(3) The Minister must consult with the responsible Ministers and the Minister for Communications and Information Technology before making a decision on the application.~~

~~(4) An application to the Minister must not be materially different from the original application.~~

(1) The Minister may, in accordance with **section 33B**,—

(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**:

(b) grant a network operator or class of network operators an exemption from all or any of the requirements of **section 13**:

(c) grant a network operator or a class of network operators an exemption from all or any of the requirements of **section 23**:

(d) vary or revoke an exemption referred to in **paragraph (a), (b), or (c)**.

(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 intercepted under an interception warrant or any other lawful authority.

(3) An exemption under **subsection (1)**—

(a) may, without limitation, apply to all or part of a specified service or network or class of service or network; and

(b) may be subject to any terms and conditions specified by the Minister.

33A Effect of application for exemption or variation

(1) The effect of an application under **section 32A** is that from the date that the designated officer's decision is issued under **section 32(5)** to the date that the Minister's decision on the application is notified—

(a) in the case of an application for exemption, the applicant is treated as being exempt from the obligation for which the exemption is sought; or

(b) in the case of an application to vary an exemption, the exemption is treated as being in force as varied.

(2) **Subsection (1)** does not apply to an applicant if—

(a) the Minister considers, on reasonable grounds, that the applicant is persistently or repeatedly seeking the same or a similar exemption or variation in relation to the same matter, or seeking the same outcome, despite the application being refused; and

(b) the Minister has notified the applicant accordingly.

33B Decision-making process

(1) The Minister must consult the responsible Ministers and the Minister for Communications and Information Technology before making a decision on the application.

(2) The Minister must decide the application as soon as is practicable.

(3) The Minister must, when considering whether to grant, vary, or revoke an exemption, take account of the following matters:

(a) national security or law enforcement interests; and

(b) the number of customers or end-users of the relevant network or service; and

(c) the cost of compliance with the obligation for which an exemption is sought; and

(d) whether compliance could be achieved appropriately by another means; and

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

(4) The Minister must, when taking account of the matters set out in **subsection (3)**, give primacy to **subsection (3)(a)**.

(5) The reasons for the decision must be set out in the decision, except those parts of the reasons that would reveal classified information.

(6) The Minister must issue a written notice of the decision to the applicant or, in the case of a class exemption, to the class of network operators who are affected by the decision.

(7) An exemption applying to a class of network operators that is granted, varied, or revoked under **section 33** is not a disallowable instrument for the purposes of the Legislation Act 2012 and does not have to be presented to the House of Representatives under section 41 of that Act.

34 Regulations relating to class exemptions

(1) The Governor-General may, by Order in Council, on the recommendation of the Minister, make regulations—

(a) granting, subject to **subsection (2)**, a class of network operators an exemption from all or any of the requirements of **sections 9 and 10**:

(b) granting a class of network operators an exemption from all or any of the requirements of **section 13**:

(c) granting a class of network operators an exemption from all or any of the requirements of **section 23**.

(2) Regulations 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 intercepted under an interception warrant or any other lawful authority.

(3) Regulations under **subsection (1)** may, without limitation, apply to all or part of a specified service or network or class of service or network.

(4) The Minister must not recommend the making of regulations under **subsection (1)** unless the Minister has—

(a) taken account of the matters set out in ~~**section 32(1)**~~ **sections 33B(3) and (4)**; and

(b) consulted ~~with~~ the responsible Ministers and the Minister for Communications and Information Technology.

Subpart 5—Ministerial directions

Minister may require service providers to have same obligations as network operators

35 Minister may require service providers to have same obligations as network operators

(1) The Minister may, at the application of a surveillance agency in accordance with this section, direct that a telecommunications service provider—

(a) comply with one of the following duties:

(i) the duty to comply with **sections 9 and 10**:

(ii) the duty to be intercept ready:

(iii) the duty to be intercept accessible; and

(b) be treated as having the same obligations and rights as a network operator under this Part (except for **sections 13 to 20, and 23**) and **Parts 1 and 4**.

(2) A surveillance agency may make an application for a ministerial direction under this section only if—

(a) the surveillance agency considers that lack of interception capability on the telecommunications service offered by that provider adversely affects national security or law enforcement; and

(b) at the time of application, 1 or more telecommunications service offered by that provider is a service over

which the surveillance agency could lawfully execute an interception warrant or any other lawful interception authority.

(3) The surveillance agency must, when applying for a ministerial direction, notify the affected service provider ~~of the application~~ in writing that it is applying for a direction under this section and ~~the time frame in~~ specify in the notice a time, which must be reasonable in the circumstances, within which submissions may be made to the Minister on the application.

(4) The affected service provider may make submissions to the Minister on the application.

(5) The Minister must consult with the responsible Ministers and the Minister for Communications and Information Technology.

(6) The Minister must not make a direction unless—

(a) the Minister has taken into account the views, if any, of the Ministers referred to in **subsection (5)** and the affected service provider; and

(b) the Minister has taken account of the matters set out in **subsection (7)**; and

(c) the Minister is satisfied on reasonable grounds that the direction is necessary for reasons of national security or law enforcement, or both.

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

(a) whether the current level of interception capability on any services provided by the affected service provider adversely affects national security or law enforcement; and

(b) whether the cost of compliance would have a serious adverse effect on the business of the affected service provider; and

(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; and

(d) any other matter that the Minister considers relevant in the circumstances.

(8) The Minister must give primacy to the matter described in **subsection (7)(a)**.

(9) The Minister must not delegate to any person, other than another Minister, the power to make a direction under this section.

36 Review

(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.

(2A) In **subsection (2)**, a person is suitably qualified if the person—

(a) has experience in—

(i) telecommunications technology; or

(ii) national security or law enforcement; or

(iii) competition in telecommunications markets; or

(iv) international relations or international law; and

(b) does not have any conflict of interest in relation to the direction; and

(c) has or is able to obtain an appropriate security clearance.

(3) The review panel must—

(a) review all relevant submissions made to the Minister, and take into account all other relevant information; and

(b) make recommendations to the Minister on whether the service provider should be treated as a network operator.

(4) The Minister must, after considering the recommendations of the review panel, vary ~~or,~~ confirm, or revoke the direction.

(5) A summary of the review panel's recommendations and reasons must be provided to the affected service provider, except those parts of the reasons that would reveal classified information.

37 Direction notice

(1) If the Minister makes a direction under **section 35**, a written notice of the direction must be provided to the affected ~~party~~ service provider together with reasons, except those parts of the reasons that would reveal classified information.

(2) The direction—

(a) must state which of the duties referred to in **section 35(1)(a)** that the ~~telecommunications~~ affected service provider must comply with; and

(aa) must specify a time, which must be reasonable in the circumstances, by which the duty or duties must be complied with; and

(b) may be subject to any terms and conditions specified by the Minister.

(3) The effect of the direction is that this Part (except for **sections 13 to 20, and 23**) and **Parts 1 and 4** apply to the affected service provider as if the service provider were a network operator under this Act.

(4) The Minister may, after consulting the Ministers referred to in **section 35(5)**, revoke the direction at any time.

38 Regulations relating to service providers

(1) The Governor-General may, by Order in Council, on the recommendation of the Minister, make regulations specifying that a class of service providers must—

(a) comply with one of the following duties:

(i) the duty to comply with **sections 9 and 10**:

(ii) the duty to be intercept ready:

(iii) the duty to be intercept accessible; and

(b) be treated as having the same obligations and rights as a network operator under this Part (except for **sections 13 to 20, and 23**) and **Parts 1 and 4**.

(2) Regulations under **subsection (1)** may, without limitation, apply to all or part of a telecommunications service or class of telecommunications service.

(3) The Minister must not recommend the making of regulations under **subsection (1)** unless ~~he or she~~ the Minister—

(aa) has consulted the telecommunications industry in accordance with the process set out in **subsection (3A)**; and

(a) has taken account of the matters set out in **section 35(7) and (8)**; and

(b) has consulted with the Ministers referred to in **section 35(5)**.

(3A) The consultation process referred to in **subsection (3)(aa)** requires that the Minister—

(a) publish, on an Internet site operated by the Ministry, a notice that—

(i) sets out the effect of the proposed regulations (**proposal**); and

(ii) invites submissions on the proposal to be made by a specified date; and

(b) consider the submissions (if any) on the proposal.

(4) The effect of the regulations is that this Part (except for **sections 13 to 20, and 23**) and **Parts 1 and 4** apply to a service provider falling within a class specified in the regulations, as if the service provider were a network operator under this Act.

Ministerial direction relating to resold overseas telecommunications services

39 Ministerial direction relating to resold overseas telecommunications services

(1) This section applies to any telecommunications services that are provided from outside New Zealand and resold in New Zealand by a network operator.

(2) The Minister may, on the application of a surveillance agency, and after taking into account the matters in **subsections (2A) and (2B)**, direct that a service to which this section applies must not or must no longer be provided or supplied in New Zealand if the Minister is satisfied the direction is necessary to address a significant risk to national security or law enforcement.

(2A) The matters that the Minister must take into account are—

(a) national security or law enforcement interests; and

(b) the cost to, and impact on, the network operator; and

(c) the effect on competition or innovation in telecommunications markets; and

(d) any other matter that the Minister considers relevant.

(2B) The Minister must, when taking into account the matters set out in **subsection (2A)**, give primacy to **(2A)(a)**.

(3) A surveillance agency must ~~notify the affected network operator~~—

(a) notify the affected network operator in writing that it has applied for a direction under this section; and

(b) ~~of the date by~~ specify in the notice a time, that is reasonable in the circumstances, within which the network operator 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.

(5) The network operator may make submissions to the Minister, but must make them by the date specified in the notice referred to in **subsection (3)**.

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

(7) The Minister must take into account the views, if any, of affected network operators and those of the Ministers referred to in **subsection (6)**.

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

(8A) The time or times by which the network operator must comply with the requirements of the direction must be specified in the direction and must be reasonable in the circumstances.

(9) The direction may be subject to any terms and conditions specified by the Minister.

(10) The Minister may, after consulting the Ministers referred to in **subsection (6)**, revoke the direction at any time.

(11) The Minister must not delegate to any person, other than another Minister, the power to make a direction under this section.

Subpart 6—Formatting

40 Notice relating to formatting

(1) The Minister may, by notice in the *Gazette*, determine the format in which call associated data and the content of a telecom-

munication must be able to be obtained under an interception warrant or any other lawful interception authority.

(1A) Before making a determination under **subsection (1)**, the Minister must consult the telecommunications industry by—

(a) publishing, on an Internet site operated by the Ministry, a notice that—

(i) sets out the effect of the proposed notice (**proposal**); and

(ii) invites submissions on the proposal to be made by a specified date; and

(b) considering the submissions (if any) on the proposal.

(2) The notice may incorporate by reference all or part of any standard, specification, or requirement that is published by or on behalf of any body or person in any country, including any standard from the European Telecommunications Standards Institute.

(3) The notice is a disallowable instrument~~, but not a legislative instrument,~~ for the purposes of the Legislation Act 2012 and must be presented to the House of Representatives under section 41 of that Act.

41 Effect of changes to material incorporated by reference

(1) This section applies if—

(a) a network operator has an interception capability that conforms with a standard, specification, or requirement that has been incorporated by reference under **section 40(2)**; and

(b) that standard, specification, or requirement is later amended or replaced.

(2) If this section applies, the network operator is not under any duty to ensure the interception capability conforms to any changes to, or replacement of, the standard, specification, or requirement so long as the network operator ensures that the interception capability continues to conform to the earlier standard, specification, or requirement.

42 Formatting before commencement of this Act

A public telecommunications network or a telecommunications service that immediately before the commencement of this Act complied with section 8(1)(c) of the Telecommunications (Interception Capability) Act 2004 by obtaining the call associated data and the content of telecommunications in a format that was able to be used by a surveillance agency—

(a) is not subject to **section 10(5)(a) or 24(7)(a)** of this Act; and

(b) may continue to use the format that it used immediately before the commencement of this Act for the purpose of **section 10(1)(c) or 24(3)(b)(iii)** of this Act.

Part 3
Network security

43 Application of this Part

This Part applies to network operators.

~~**44 Definition of Minister**~~

~~In this Part, unless the context otherwise requires, **Minister** means the Minister responsible for the Government Communications Security Bureau.~~

45 Network operators' duty to engage in good faith

(1) A network operator must engage with the Director as soon as practicable after becoming aware of any network security risk~~, or~~ that may arise if the proposed decision, course of action, or change ~~that may raise a network security risk~~ is implemented.

(2) A network operator must act honestly and in good faith when engaging with the Director in relation to any matter in this Part.

(3) A network operator must provide the Director with access to any of its employees, contractors, or agents that, in the Director's opinion, are best placed to assist the Director in relation to a matter under this Part.

Disclosure

46 Areas of specified security interest

(1) In this section and **section 47**, an **area of specified security interest**, in relation to a network operator, ~~includes~~ means—

(a) network operations centres:

(b) lawful interception equipment or operations:

(c) any part of a public telecommunications network that manages or stores—

~~(i) aggregated customer information, including authentication credentials; or~~

(i) aggregated information about a significant number of customers:

(ia) aggregated authentication credentials of a significant number of customers:

(ii) administrative (privileged user) authentication credentials:

(d) any place in a public telecommunications network where data belonging to a customer or end user aggregates in large volumes, being either data in transit or stored data:

(e) any area prescribed under **subsection (2)**.

(2) The Governor-General may, by Order in Council, on the recommendation of the Minister, ~~prescribe additional areas of specified security interest.~~ responsible for the Government Communications Security Bureau, make regulations—

(a) amending or removing an area of specified security interest listed in **subsection (1)**:

(b) prescribing additional areas of specified security interest.

~~(3) The Minister must not recommend the making of regulations under **subsection (2)** unless the Minister is satisfied that the regulations are necessary to—~~

~~(a) keep up to date with changes in technology; or~~

~~(b) address changes in the way that networks are being used that may give rise to a security risk; or~~

~~(c) address any significant changes in architectural approach to the design of a public telecommunications network.~~

(3) The Minister must not recommend the making of regulations under **subsection (2)** unless—

(a) the Minister has consulted network operators registered under **Part 4**; and

(b) the Minister is satisfied that the regulations are necessary or desirable to—

(i) keep up to date with changes in technology; or

(ii) address changes in the way that networks are being used that may give rise to a security risk; or

(iii) address any significant changes in architectural approach to the design of a public telecommunications network.

(4) In this section,—

administrative (privileged user) authentication credentials means the authentication credentials of a privileged user

authentication credentials means any information (for example, passwords or usernames) used to ascertain the identity of a user, process, or device

privileged user means a person who has authorisations that enable the person to, among other things, alter, bypass, or circumvent network security protections.

47 Network operator must notify Director

(1) A network operator must notify the Director of any proposed decision, course of action, or change made by or on behalf of the network operator regarding—

(a) the procurement of any equipment, system, or service that falls within an area of specified security interest; or

(b) any change to any equipment, system, or service that falls within an area of specified security interest; or

(c) any change to the ownership, control, oversight, or supervision of any equipment, system, or service that falls within an area of specified security interest.

(2) The network operator must—

(a) comply with **subsection (1)(a)** before any steps are taken, as part of the procurement decision-making process, to approach the market (whether by request for quote, tender, or otherwise) or comply with **subsec-**

tion (1)(b) or (c) during the development of a business or change proposal; and

(b) ensure any notice given to the Director in compliance with **subsection (1)** is given within sufficient time for the Director to consider whether to take action under **section 49**.

48 Exemption from section 45(1) or 47

(1) The Director may, by written notice, exempt a network ~~operators~~ operator or a class of network operators from any of the requirements in **section 45(1) or 47** if the Director is satisfied that the matter to which the exemption relates will not give rise to a network security risk.

(2) The exemption may be granted for any period specified by the Director and on any terms and conditions that the Director thinks fit.

(3) The Director may by written notice vary or revoke an exemption granted under this section.

(4) The Director may give a notice under this section relating to a network operator directly to the network operator concerned.

(5) A notice under this section that relates to a class of network operators—

(a) must be published on an Internet site operated by the Government Communications Security Bureau; and

(b) is not a disallowable instrument for the purposes of the Legislation Act 2012 and does not have to be presented to the House of Representatives under section 41 of that Act.

Process for preventing or mitigating network security risks

48A Consideration of network security risk by Director or Minister

(1) When considering whether a network security risk or significant network security risk is raised under this Part, the Director, or if the case requires, the Minister responsible for the Government Communications Security Bureau,—

(a) must consider the likelihood that the matter giving rise to the risk will lead to—

(i) the compromising or degrading of the public telecommunications network; and

(ii) the impairment of the confidentiality, availability, or integrity of telecommunications across the network; and

(b) must consider the potential effect that an event described in **paragraph (a)(i) or (ii)** will have on the provision of—

(i) central or local government services:

(ii) services within the finance sector:

(iii) services within the energy sector:

(iv) services within the food sector:

(v) communication services:

(vi) transport services:

(vii) health services:

(viii) education services; and

(c) may consider any other matter that the Director or Minister considers relevant.

(2) In **subsection (1)(a)** the **matter giving rise to the risk** means—

(a) any proposed decision, course of action, or change, that if implemented will give rise to the network security risk or significant network security risk; or

(b) any decision that has been implemented, binding legal arrangement, or course of action or change that has commenced that gives rise to the network security risk or significant network security risk.

49 Process for addressing network security risks

(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 of action, or change by a network operator that, in the Director's opinion, would, if implemented, raise a network security risk other than a minimal network security risk,—

(a) the Director must advise the network operator of the matter as soon as practicable; and

(b) the network operator must not ~~take any further steps to~~ implement or give effect to the proposed decision, course of action, or change—

(i) unless and to the extent that those ~~steps~~ actions are consistent with or give effect to a proposal or part of a proposal (relating to the proposed decision, course of action, or change) accepted by the Director under **section 50** or a direction of the Minister under **section 54** on a matter relating to the proposal; or

(ii) unless the Director has referred a matter (arising from the proposal) to the Minister responsible for the Government Communications Security Bureau under **section 52** and the Minister does not make a direction in respect of the proposal~~.~~; or

(iii) unless the Director has notified the network operator that the Director has not accepted the proposal but has decided not to refer the matter to the Minister under **section 52**.

(2) The Director must provide a written notice to the network operator that relates to the matter referred to in **subsection (1)**.

(3) The network operator must, as soon as practicable ~~(having regard to the seriousness and imminence of the risk)~~, respond in writing to the notification~~,~~ by providing the Director with a proposal to prevent or sufficiently mitigate the network security risk.

(4) A notice under **subsection (2)** and a proposal under **subsection (3)** must comply with any requirements prescribed in regulations made under **section 110**.

50 Assessment of response by network operator

(1) The Director must assess whether the proposal will, if implemented, prevent or sufficiently mitigate the network security risk.

(2) If the Director is satisfied that the proposal or part of the proposal will, if implemented, prevent or sufficiently mitigate the network security risk, the Director ~~may~~ must accept the proposal or that part of the proposal and advise the network operator accordingly in writing.

51 Network operator must implement response

The network operator must implement those parts of the proposal accepted by the Director under **section 50(2)** (unless later modified by agreement with the Director).

52 Director may refer matter to Minister

If the Director considers that the proposal or part of the proposal does not prevent or sufficiently mitigate a significant network security risk, the Director ~~may~~—

(a) may refer the matter to the Minister responsible for the Government Communications Security Bureau to make a direction under **section 54**; and

(b) must, if a referral is made, inform the network operator that it may make submissions on the matter directly to the Minister, and specify ~~the time frame for making those submissions.~~ a time, which must be reasonable in the circumstances, by which those submissions must be made.

Ministerial direction

53 Failure to comply

(1) This section applies if,—

(a) despite being advised under **section 49**, a network operator has entered into a binding legal arrangement, implemented a decision, or commenced a course of action or change that gives rise to a significant network security risk; or

(b) a network operator fails to comply with a requirement of this Part or a requirement to supply information or a class of information under **section 73** and has entered into a binding legal arrangement, implemented a decision, or commenced a course of action or change that gives rise to a significant network security risk.

(2) If this section applies, the Director ~~may~~—

(a) may refer the matter to the Minister responsible for the Government Communications Security Bureau to make a direction under **section 54**; and

(b) must, if a referral is made, inform the network operator that it may make submissions on the matter directly to the Minister, and specify ~~the time frame for making those submissions~~ a time, which must be reasonable in the circumstances, by which those submissions must be made.

54 Minister may make direction

(1) The Minister responsible for the Government Communications Security Bureau may make a direction under this section only if—

(a) the Minister has been referred a matter under **section 52 or 53**; and

(b) the Minister has considered any submissions from the network operator; and

(c) the Minister is satisfied that exercising his or her powers under this section is necessary to prevent, sufficiently mitigate, or remove a significant network security risk.

(2) A direction under this section may require a network operator to take steps, as specified by the Minister, to prevent, or sufficiently mitigate or remove, the significant network security risk, and those steps may include—

(a) requiring the network operator to cease a particular activity or to do or refrain from doing a particular activity in the future; or

(b) directing the network operator to make changes to, or remove, any particular system, equipment, service, component, or operation on or related to the network.

(2A) A direction under this section may provide for any other relevant matter.

(2B) The Minister must ensure that any time by which a network operator must comply with a requirement of the direction is specified in the direction and is reasonable in the circumstances.

(3) The Minister must—

(a) consult with the Minister for Communications and Information Technology and the Minister of Trade before making a direction under this section; and

(b) be satisfied that the direction complies with **section 8(2) to (4)** and is consistent with the purpose in **section 7**.

(4) The Minister must issue the direction in writing to the affected network operator together with reasons, except those parts of the reasons that would reveal classified information.

(5) The Minister must not delegate to any person, other than another Minister, the power to make a direction under this section.

54A Guidelines

(1) The Director may issue guidelines on any requirements under this Part that apply to network operators.

(2) Any guidelines issued under this section are not binding.

(3) However, in any proceeding relating to this Act, evidence of a network operator's compliance with any guidelines issued under this section is to be treated as evidence of compliance with the applicable requirements.

Part 4
Registration, enforcement, and miscellaneous provisions

Subpart 1—Registration

Network operators must register

55 Network operators must register

(1) A person that is, on the commencement of this section, a network operator must be registered on the register within 3 months after that commencement.

(2) A person that, after the commencement of this section, becomes a network operator must be registered on the register within 3 months after the person becomes a network operator.

56 Application for registration

An application for registration must—

(a) be made to the Registrar; and

(b) contain the information specified in **section 57**; and

(c) be accompanied by a certificate signed by the chief executive of the network operator confirming that the information contained in the application is true and correct; and

(d) otherwise be made in the form or manner required by the Registrar.

57 Registration information

(1) The information referred to in **section 56(b)** is as follows (to the extent that the information is applicable):

(a) the name of the network operator:

(b) the name and contact details of a suitable employee of the network operator who will be responsible for dealing with issues raised by a surveillance agency relating to interception capability or an interception warrant or any other lawful interception authority:

(c) the name and contact details of a suitable employee of the network operator who will be responsible for dealing with issues raised by the Director relating to network security:

(d) the total number of the network operator's customers; ~~and~~:

(e) in the case of a network operator that offers retail services, an estimate of the total number of end-users across all telecommunications services and all public telecommunications networks; ~~and~~:

(f) the total number of connections for wholesale network services:

(g) the geographical coverage of the network operator's telecommunications services and public telecommunications networks (for example, by reference to the name of a region or to national coverage):

(ga) the particulars of any outsourcing arrangement (including the date of the arrangement, the names of the parties to it, and its general nature):

(h) the types of telecommunications services provided by the network operator (for example, mobile, email, or Voice over Internet Protocol services):

(i) an address for service of notices under this Act:

(j) whether the network operator is subject to—
  (i) the duty to comply with **sections 9 and 10**; or
  (ii) the duty to be intercept ready; or
  (iii) the duty to be intercept accessible.

(2) The information specified in this section must be prepared as at the date of the application (or, in the case of an annual update, as at the date of that update).

Register

58 Register of network operators

(1) The ~~New Zealand~~ Commissioner of Police must establish a register of network operators (the **register**).

(2) The Registrar must maintain the register.

59 Purpose of register

The purpose of the register is to assist any surveillance agency in the exercise or performance of its powers, functions, or duties under this Act.

60 Contents of register

The register must contain—

(a) the information referred to in **section 57** in relation to each network operator:

(b) the information provided to the Registrar under **section 23** (which relates to infrastructure-level services).

61 Operation of and access to register

(1) The register may be kept as an electronic register or in any other manner that the Registrar thinks fit.

(2) The register must be available for access and searching by surveillance agencies (including by any employee or other person acting on behalf of a surveillance agency) at all times unless suspended under **subsection (4)**.

(3) The register is not available for access or searching by any person other than a designated officer or a surveillance agency (or any employee or other person acting on its behalf).

(4) The Registrar may refuse access to the register or suspend its operation, in whole or in part, if the Registrar considers that it is not practical to provide access to the register.

62 Registrar must keep register secure

(1) The Registrar must take reasonable steps to ensure that the register is not available for access or searching by any person other than a designated officer or a surveillance agency (or any employee or other person acting on its behalf).

(2) This section and **section 61** do not limit the Official Information Act 1982.

Changes to register

63 Network operators must notify Registrar of key changes

(1) A network operator must give to the Registrar written notice of any relevant change no later than 20 working days before the change takes effect.

(2) However, if it is not reasonably practicable to comply with **subsection (1)**, the network operator must give to the Registrar written notice of the relevant change as soon as is reasonably practicable.

(3) A network operator must give to the Registrar written notice of a threshold change no later than 10 working days after the date on which the change was identified, or ought reasonably to have been identified, by the operator.

(4) In this section,—

relevant change means a change to any of the following:

(a) the name of the network operator:

(b) the name and contact details of a suitable employee of the network operator who will be responsible for dealing with issues raised by a surveillance agency relating to interception capability or an interception warrant or any other lawful interception authority:

(c) the name and contact details of a suitable employee of the network operator who will be responsible for dealing with issues raised by the Director relating to network security:

(d) the geographical coverage of the network operator's telecommunications services and public telecommunications networks:

(da) the outsourcing arrangements of the network operator:

(e) the types of telecommunications services provided by the network operator

threshold change means a change in circumstances that has the effect of changing the interception capability duties that apply to the network operator under this Act.

64 Annual update

(1) A network operator must give to the Registrar each year ~~on 1~~ in November an annual update of information on the register relating to that operator.

(2) The annual update must—

(a) specify any changes to the information referred to in **section 57** that have occurred since the network operator last gave information to the Registrar (whether in a notice under **section 63**, the previous annual update, or an application under **section 56**); and

(b) confirm that, apart from the changes under **paragraph (a)**, all other information referred to in **section 57** that is currently held by the Registrar remains correct; and

(c) be in the form (if any) required by the Registrar; and

(d) be accompanied by a certificate signed by the chief executive of the network operator confirming that the information contained in the annual update is true and correct.

(3) An annual update does not need to be provided in the year during which this section comes into force.

65 Registrar may deregister person

The Registrar may remove a person from the register if the Registrar is satisfied that the person has—

(a) ceased to exist; or

(b) ceased to have the obligations of a network operator under this Act; or

(c) otherwise ceased to be a network operator.

66 Registrar may amend register

The Registrar may amend the register if—

(a) a notice under **section 63** or an annual update contains information that is different from the information entered on the register:

(b) a network operator informs the Registrar of information that is different from the information entered on the register:

(c) the Registrar is satisfied at any time that the register contains an error or a mistake or omits information given to the Registrar.

Subpart 2—Registrar and other designated officers

67 Appointment of designated officers

(1) 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.

(2) A copy of the notice under **subsection (1)** must be published on an Internet site maintained by or on behalf of the New Zealand Police.

68 Appointment of Registrar

(1) The Commissioner of Police must, by notice in the *Gazette*, appoint one of the designated officers as the Registrar of network operators.

(2) A copy of the notice under **subsection (1)** must be published on an Internet site maintained by or on behalf of the New Zealand Police.

69 Power of designated officer to delegate

(1) The Registrar or any other designated officer may delegate to any person, either generally or particularly, any of the Registrar's or other designated officer's functions, duties, and powers except the power of delegation.

(2) A delegation—

(a) must be in writing; and

(b) may be made subject to any restrictions and conditions the Registrar or designated officer thinks fit; and
(c) is revocable at any time, in writing; and
(d) does not prevent the performance or exercise of a function, duty, or power by the Registrar or designated officer.

(3) A person to whom any functions, duties, or powers are delegated may perform and exercise them in the same manner and with the same effect as if they had been conferred directly by this Act and not by delegation.

(4) A person who appears to act under a delegation is presumed to be acting in accordance with its terms in the absence of evidence to the contrary.

Subpart 3—Secret-level government-sponsored security clearance

70 Network operator must nominate employee to apply for clearance

(1) A network operator must, within 10 working days after being required to do so under **subsection (2), (3), or (4)**,—
(a) nominate a suitable employee to apply for a secret-level government-sponsored security clearance (a **clearance**); and
(b) notify the employee of the nomination; and
(c) give written notice of the name and contact details of that employee to the Registrar.

(2) A designated officer may, by written notice served on a network operator, require the operator to comply with **subsection (1)** unless **section 13~~(2)~~** applies.

(3) If a network operator is notified that an application under **section 71** has been declined or that an application has not been made within the time referred to in **section 71(2)**, the network operator must comply again with **subsection (1)** (to nominate another employee).

(4) If a network operator is notified that its employee's clearance has expired or been revoked for any reason, the network operator must comply again with **subsection (1)** (to re-nominate

the same employee (unless his or her clearance was revoked) or to nominate another employee).

71 Nominated person must apply

(1) A designated officer must, by written notice served on the employee nominated under **section 70**, specify the manner in which the employee must apply for a clearance.

(2) The employee must, within 10 working days after being notified under **subsection (1)**, apply for the clearance.

Subpart 4—General information-gathering powers

72 Designated officer may require information in order to assist surveillance agency

(1) If a designated officer considers it necessary or desirable for any specified purpose, the designated officer may, by written notice served on any network operator, require the operator—

(a) to supply to the designated officer or a surveillance agency any information or class of information specified in the notice; or

(b) to produce to the designated officer or a surveillance agency, or to a person specified in the notice acting on the agency's behalf, any document or class of documents specified in the notice; or

(c) if necessary, to reproduce, or assist in reproducing, in usable form, information recorded or stored in any document or class of documents specified in the notice.

(2) In **subsection (1)**, **specified purpose** means the purpose of assisting any surveillance agency to do 1 or more of the following:

(a) enforce compliance with the duties under this Act relating to interception capability:

(b) execute an interception warrant or any other lawful interception authority:

(c) otherwise perform or exercise any of its functions, powers, or duties under this Act in relation to interception capability or an interception warrant or any other lawful interception authority.

(3) A network operator must comply with the notice in the manner specified in the notice.

(4) A designated officer may exercise the power under **subsection (1)** at the request of a surveillance agency (in which case, the officer must promptly supply information or documents obtained under **subsection (1)** to the surveillance agency).

73 Director of Government Communications Security Bureau may require information

(1) If the Director considers it necessary or desirable for any specified purpose, the Director may, by written notice served on any network operator, require the operator—

(a) to supply to the Director any information or class of information specified in the notice; or

(b) to produce to the Director, or to a person specified in the notice acting on his or her behalf, any document or class of documents specified in the notice; or

(c) if necessary, to reproduce, or assist in reproducing, in usable form, information recorded or stored in any document or class of documents specified in the notice.

(2) In **subsection (1)**, **specified purpose** means the purpose of—

(a) enforcing compliance with the duties under this Act relating to network security; or

(b) otherwise performing or exercising any of the Director's functions, powers, or duties under this Act in relation to network security.

(3) A network operator must comply with the notice in the manner specified in the notice.

74 Time for compliance

A network operator must comply with a notice under **section 72 or 73** as soon as practicable after receiving the notice, but in any event not later than—

(a) 20 working days after the date of the notice; or

(b) a later time that is specified in the notice.

75 Network operator must comply despite any other enactment or any breach of confidence, etc

(1) A network operator must comply with a notice under **section 72 or 73** despite anything to the contrary in any deed or contract or any other enactment.

(2) A network operator must comply with a notice under **section 72 or 73** even if compliance involves—

(a) the disclosure of commercially sensitive information; or

(b) a breach of an obligation of confidence.

(3) However, every person has the same privileges in relation to providing information and documents under **section 72 or 73** as witnesses have in proceedings before a court.

76 Miscellaneous provisions

(1) Information supplied in response to a notice under **section 72(1)(a) or 73(1)(a)** must be—

(a) given in writing; and

(b) accompanied by a certificate that confirms that, to the best of the network operator's knowledge, the information supplied complies with requirements of the notice.

(2) If a document is produced in response to a notice under **section 72 or 73**, a surveillance agency referred to in **section 72(4)** or the Director (as the case may be), or the person to whom the document is produced, may—

(a) inspect and make records of that document; and

(b) take copies of the document or extracts from the document.

Subpart 5—Compliance testing

77 Designated officer may require compliance testing

(1) If a designated officer considers it necessary or desirable for the purposes of assisting a surveillance agency to perform or exercise any of its functions, powers, or duties under **Part 2**, the officer may, by written notice served on a network operator, require the operator to test its equipment and procedures to—

(a) ensure that the equipment and procedures comply with the duties that apply to the operator by or under **Part 2**; and

(b) identify any deficiencies in the equipment and procedures in terms of that compliance.

(2) The notice may specify various times for completing the testing in stages and a final date for completing the testing.

(3) Each of those times must be reasonable in the circumstances and must be set after having regard to any submissions made under **section 78(1)(b)**.

(4) The network operator must comply with the notice within the time or times and in the manner specified in the notice.

78 Process for consulting on times

(1) A designated officer must, before serving a notice under **section 77**,—

(a) serve on the network operator written notice stating—

(i) that the officer may exercise a power under **section 77**; and

(ii) ~~of~~ the telecommunications service to which the notice under **section 77** may relate; and

(iii) ~~of~~ the reasons why the officer is considering exercising that power; and

(b) give to the network operator an opportunity to make written submissions relating to the time or times within which the operator must carry out the testing under a notice under **section 77**.

(2) A designated officer must serve the notice under **subsection (1)** at least 10 working days before it serves a notice under **section 77**.

Subpart 6—Certification

79 Designated officer may require certification as to compliance

(1) A designated officer may, by written notice served on a network operator, require a chief executive of the operator to certify that, after due inquiry, the chief executive is satisfied as to 1 or more of the following:

(a) that adequate resources have been allocated by the operator to secure compliance with its duties under **Part 2**:

(b) that the operator maintains and operates interception capability in compliance with this Act:

(c) that the operator is otherwise complying with **Part 2**.

(2) If a chief executive is unable to give the certification because the chief executive is not satisfied as referred to in **subsection (1)**, the chief executive must, instead of giving the certification, give written notice to the designated officer of the reasons for being unable to give the certification (including details of any failure to comply with this Act and whether the operator has applied for, or intends to apply for, an exemption under **subpart 4 of Part 2**).

(3) The certification (or notice under **subsection (2)**) must be given within the time and in the manner specified in the notice under **subsection (1)**.

(4) The time specified in the notice under **subsection (1)** must be reasonable in the circumstances.

80 Due inquiry

(1) A chief executive who is required to make **due inquiry** about a matter under **section 79** does not fail to do so if—

(a) he or she receives information or advice about the matter from another person who he or she believes on reasonable grounds is reliable and competent; and

(b) the information or advice received—

(i) is of the same kind and standard as that which could reasonably be expected to be supplied in the ordinary course of management of businesses of the same kind to persons in the same kind of position; and

(ii) does not state or indicate that further information, advice, or investigation is or may be required; and

(c) he or she has no reason to believe that the information or advice is or may be incorrect.

(2) Nothing in **subsection (1)** limits the ways in which a chief executive may make due inquiry about a matter.

81 Designated officer may give certificate to surveillance agency

A designated officer may give any information obtained under this subpart to a surveillance agency.

Subpart 7—Enforcement

82 Interpretation

In this subpart,—

(a) a non-compliance with this Act is **minor** if it consists of a failure to comply with any of **sections 23, 28, 47, 49(3), 55, 56, 63, 64, 70, 71(2), 72 to 76, 77(4), and 79**; and

(b) a non-compliance with this Act is **serious** if it consists of a failure to comply with any of **sections 9, 10, 11, 12, 13, 15, ~~23,~~ 24, 26, 39, 51, 54, and 83(4)**.

Breach notices and enforcement notices

83 Breach notice may be issued for minor non-compliance

(1) This section applies if a surveillance agency considers on reasonable grounds that—

(a) a person (**A**) has not complied with any of the duties under this Act; and

(b) the non-compliance is minor.

(2) The surveillance agency may serve a notice on A under this section (a **breach notice**) that requires A, within the time and in the manner specified in the notice, to comply with the duties referred to in **subsection (1)(a)**.

(3) The breach notice must identify the duties that have not been complied with.

(4) A must comply with the breach notice within the time and in the manner specified in the notice (and a failure to so comply is serious).

(5) The time specified in the breach notice must be reasonable in the circumstances.

84 Breach notice may request consent to enter and inspect in connection with duties under Part 2

(1) This section applies if a breach notice relates to a failure to comply with a duty under **Part 2**.

(2) A breach notice may request a network operator to consent to the surveillance agency entering a relevant place for the purpose of gathering evidence relating to the failure referred to in **subsection (1)** by—

(a) inspecting and making records of information, documents, or equipment that is related to the network operator's duties under **Part 2**; and

(b) taking copies of those documents or extracts from those documents.

(3) If a breach notice contains a request under **subsection (2)**, the notice must also—

(a) advise the network operator of the reason for the request; and

(b) advise the network operator that the evidence that is gathered may be admissible in proceedings relating to the failure referred to in **subsection (1)**; and

(c) advise the network operator that it may either consent to the request or refuse to consent to the request.

(4) If the network operator consents to the request, the surveillance agency (including any employee or other person acting on its behalf) may carry out an entry, an inspection, and any other action referred to in **subsection (2)** in accordance with the terms of the consent.

(5) In this section, **relevant place** means a place—

(a) that is owned, occupied, or controlled by the network operator; and

(b) that the surveillance agency believes on reasonable grounds contains information, documents, or equipment that is related to the network operator's duties under **Part 2**.

85 Enforcement notice may be issued for serious non-compliance

(1) This section applies if a surveillance agency considers on reasonable grounds that—

(a) a person has a duty under this Act; and
(b) the person has not complied with that duty; and
(c) the non-compliance is serious.

(2) The surveillance agency may serve a notice on a person under this section (an **enforcement notice**) to inform that person that the surveillance agency—
(a) is satisfied that the person has not complied with the duties specified in the notice and that the non-compliance is serious; and
(b) may make an application to the High Court under this subpart on or after a specified date.

86 Application for compliance order or pecuniary penalty order

(1) A surveillance agency may apply to the High Court for an order under **section 87 or 92** (or both) only if—
(a) it has given an enforcement notice; and
(b) the application is made on or after the date specified under **section 85(2)(b)**.

(2) No person other than a surveillance agency (or an employee or other person acting on its behalf) may make an application for an order under **section 87 or 92**.

Compliance orders

87 Power of High Court to order compliance

(1) If a person has not complied with any of the duties under this Act and the non-compliance is serious, the High Court may, for either or both of the purposes specified in **subsection (2)**, make a compliance order requiring that person—
(a) to do any specified thing; or
(b) to cease any specified activity.

(2) The purposes are—
(a) to remedy, mitigate, or avoid any adverse effects arising or likely to arise from, any non-compliance with the duties referred to in **subsection (1)**:
(b) to prevent any further non-compliance with those duties.

(3) A compliance order may be made on the terms and conditions that the High Court thinks fit, including the provision of security or the entry into a bond for performance.

88 Right to be heard

Before deciding an application for a compliance order, the High Court must—

(a) hear the applicant; and

(b) hear any person against whom the order is sought who wishes to be heard.

89 Decision on application

After considering an application for a compliance order, the High Court may—

(a) make a compliance order under **section 87**; or

(b) refuse the application.

90 Appeals to Court of Appeal

(1) A party to a proceeding relating to an application for a compliance order or any other person prejudicially affected may, with the leave of the Court of Appeal, appeal to that court if the High Court—

(a) has made or refused to make a compliance order; or

(b) has otherwise finally determined or has dismissed the proceedings.

(2) On an appeal to the Court of Appeal under this section, the Court of Appeal has the same power to adjudicate on the proceedings as the High Court had.

91 Effect of appeal

Except where the Court of Appeal otherwise directs,—

(a) the operation of a compliance order is not suspended by an appeal under **section 90**; and

(b) every compliance order may be enforced in the same manner and in all respects as if that appeal were not pending.

Pecuniary penalty orders

92 Pecuniary penalty for contravention of duties or compliance order

(1) This section applies if the High Court is satisfied, on the application of a surveillance agency, that a person—

(a) has not complied with any of the duties under this Act and that the non-compliance is serious; or

(b) has acted in contravention of a compliance order.

(2) The court may order the person to pay to the Crown any pecuniary penalty that the court determines to be appropriate.

(3) Proceedings under this section may be commenced within 3 years after the matter giving rise to the contravention was discovered or ought reasonably to have been discovered.

93 Amount of pecuniary penalty

(1) The amount of any pecuniary penalty under **section 92** must not exceed $500,000.

(2) In the case of a continuing contravention of a compliance order, the High Court may, in addition to any pecuniary penalty ordered to be paid under **section 92**, impose a further penalty of $50,000 for each day or part of a day during which the contravention continues.

94 Considerations for court in determining pecuniary penalty

In determining an appropriate pecuniary penalty, the High Court must have regard to all relevant matters, including—

(a) the purposes of this Act; and

(b) the nature and extent of the contravention; and

(c) the nature and extent of any loss or damage suffered by any person, or gains made or losses avoided by the person in contravention, because of the contravention; and

(d) the circumstances in which the contravention took place; and

(e) whether or not the person in contravention has previously been found by the court in proceedings under this

Act, or any other enactment, to have engaged in any similar conduct.

Civil proceedings

95 Rules of civil procedure and civil standard of proof apply

(1) The proceedings under this subpart are civil proceedings, and the usual rules of court and rules of evidence and procedure for civil proceedings apply (including the standard of proof).

(2) This section is subject to **subpart 8**.

Subpart 8—Protecting classified information

95A Application of subpart

This subpart applies to any proceedings in a court relating to the administration or enforcement of this Act.

96 Classified security information and other terms defined

(1) In this subpart, **classified security information** means information—

(a) that is relevant to any proceedings in a court that relate to the administration ~~and~~ or enforcement of this Act (or to any intended proceedings); and

(b) that is held by a surveillance agency; and

(c) that the head of the surveillance agency certifies in writing cannot be disclosed except to the extent provided in ~~**section 97**~~ this subpart because, in the opinion of the head of the surveillance agency,—

(i) the information is information of a kind specified in **subsection (2)**; and

(ii) disclosure of the information would be disclosure of a kind specified in **subsection (3)**.

(2) Information falls within **subsection (1)(c)(i)** if it—

(a) might lead to the identification of, or provide details of, the source of the information, the nature, content, or scope of the information, or the nature or type of the assistance or operational methods available to the surveillance agency; or

(b) is about particular operations that have been undertaken, or are being or are proposed to be undertaken,

in relation to any of the functions of the surveillance agency; or

(c) has been provided to the surveillance agency by the government of another country or by an agency of a government of another country or by an international organisation, and is information that cannot be disclosed by the surveillance agency because the government or agency or organisation by which the information has been provided will not consent to the disclosure.

(3) Disclosure of information falls within **subsection (1)(c)(ii)** if the disclosure would be likely—

(a) to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; or

(b) to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by the government of another country or any agency of such a government, or by any international organisation; or

(c) to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial; or

(d) to endanger the safety of any person.

(4) In this subpart,—

non-Crown party, in relation to proceedings, means a person (other than the Crown) that is a party to the proceedings

intended party has the meaning set out in **section 96C(1)(a)(i)**

intended proceedings means the proceedings that an intended party intends to commence as notified under **section 96C(1)(a)(ii)**

representative includes a barrister or solicitor engaged to act on behalf of a party

special advocate means a person appointed under **section 96C(2)**.

96A Obligation to provide court with access to classified security information

(1) The Crown must, after proceedings are commenced, provide the court with access to the classified security information that is relevant to those proceedings.

(2) If a special advocate is appointed before proceedings are commenced, the Crown must provide the court with access to the classified security information that is relevant to the intended proceedings.

(3) The court must keep confidential and must not disclose any information provided as classified security information, even if it considers that the information does not meet the criteria set out in **section 96(2) and (3)**, unless the head of the surveillance agency that holds the information consents to its release.

(4) **Subsection (3)** applies both during and after completion of the proceedings.

96B Court orders

(1) The court may, in order to comply with **section 96A(3)**, make 1 or more of the following orders:

(a) an order forbidding publication of any report or account of the whole or any part of the evidence adduced or the submissions made in the proceedings:

(b) an order forbidding the publication of the name of any witness or witnesses, or any name or particulars likely to lead to the identification of any witness or witnesses:

(c) an order forbidding the publication of classified security information or information about classified security information:

(d) an order excluding any person from the whole or any part of the court's proceedings, including—

(i) the non-Crown party or the non-Crown party's representative; or

(iii) staff of the court.

(2) An order made under **subsection (1)**—

(a) may be made for a limited period or permanently; and

(b) if it is made for a limited period, may be renewed for a further period or periods by the court; and

(c) if it is made permanently, may be reviewed by the court at any time.

96C Appointment of special advocate

(1) This section applies if—

(a) it appears to a court that—

(i) a person (the **intended party**) is or may be entitled to commence proceedings to which this subpart will or may apply but it is necessary for a special advocate to be appointed before the proceedings can be commenced; and

(ii) the intended party has notified the Crown that the party intends to commence those proceedings and that the party will apply for the appointment of a special advocate; or

(b) proceedings have been commenced and information presented, or proposed to be presented, in those proceedings includes classified security information; or

(c) proceedings have been commenced but the non-Crown party's claim cannot be fully particularised without the non-Crown party being able to consider classified security information.

(2) The court may, on the application of an intended party or non-Crown party, appoint a barrister or solicitor as a special advocate to represent the intended party's or the non-Crown party's interests on the terms that the court may direct if the court is satisfied that it is necessary to do so in order to ensure either or both of the following:

(a) that the intended party can properly prepare and commence proceedings:

(b) that a fair hearing will occur.

(3) The court must, before appointing a person as a special advocate, be satisfied that the person—

(a) holds an appropriate security clearance that allows the person to see information that is or may be classified security information; and

(b) is suitably qualified and experienced to fulfil the role of a special advocate.

(4) A special advocate appointed to represent an intended party may, after the proceedings are commenced, continue to act as the special advocate on behalf of that person (as a non-Crown party), subject to the terms that the court may direct.

(5) The court may make directions as to the terms of the appointment, and on the matters referred to in **sections 96F and 96G(3)**, before or after the proceedings are commenced.

(6) The appointment of a special advocate does not create an obligation requiring the intended party to commence proceedings.

(7) The surveillance agency to which the proceedings or intended proceedings relate must meet the actual and reasonable costs of a special advocate on a basis—

(a) agreed between the special advocate and the head of the surveillance agency; or

(b) determined by the court (in default of agreement).

96D Nomination of person for appointment

(1) Each of the following may nominate a barrister or solicitor to be appointed as the special advocate:

(a) the Crown:

(b) the intended party or the non-Crown party (as the case may be).

(2) The court may appoint a person nominated under **subsection (1)** or another person.

96E Role of special advocates

(1) The role of a special advocate is to represent an intended party or a non-Crown party.

(2) In particular, a special advocate may—

(a) prepare and commence proceedings on behalf of the person:

(b) examine and cross-examine witnesses:

(c) make oral and written submissions to the court:

(a) assist in the settlement of the proceedings.

(3) At all times, a special advocate must act in accordance with his or her duties as an officer of the High Court.

(4) A special advocate must keep confidential and must not disclose classified security information, except as expressly provided or authorised under this Act.

96F Court may provide access to classified security information to special advocate

(1) A special advocate may, before or after the commencement of proceedings, apply to the court for access to the classified security information.

(2) The court may provide access to the classified security information to the special advocate on the terms that the court may direct.

96G Communication between special advocate and other persons

(1) A special advocate may communicate with the relevant party or the relevant party's representative on an unlimited basis until the special advocate has been provided with access to the classified security information.

(2) After the special advocate has been given access to the classified security information, he or she must not communicate with any person about any matter connected with the classified security information except in accordance with this section.

(3) A special advocate who, after having been given access to the classified security information, wishes to communicate with the relevant party, the relevant party's representative, or any other person not referred to in **subsection (4)** may do so on the terms that the court may direct.

(4) A special advocate may, without the approval of the court, communicate about any matter connected with the classified security information with—

(a) the court:

(b) the Crown's security-cleared representative:

(c) the head of the surveillance agency to which the proceedings relate, or the surveillance agency's security-cleared representative.

(5) In this section, **relevant party** means the intended party or non-Crown party.

96H Protection of special advocates from liability

(1) To the extent that a special advocate is acting in accordance with the requirements of this Act, he or she is not guilty of—

(a) misconduct within the meaning of section 7 or 9 of the Lawyers and Conveyancers Act 2006; or

(b) unsatisfactory conduct within the meaning of section 12 of that Act.

(2) This subpart applies despite the requirements of any practice rules made and approved under the Lawyers and Conveyancers Act 2006.

(3) No person is personally liable for any act done or omitted to be done in good faith, in his or her capacity as a special advocate, in accordance with the requirements or provisions of this Act.

97 ~~Procedure~~ Other matters relating to procedure in proceedings involving classified security information

~~(1) This section applies to any proceedings in a court relating to the administration and enforcement of this Act.~~

(2) The court must determine the proceedings on the basis of information available to it (whether or not that information has been disclosed to or responded to by all parties to the proceedings).

(3) If information presented, or proposed to be presented, in the proceedings by the Crown includes classified security information,—

(a) except where proceedings are before the Court of Appeal or the Supreme Court, the proceedings must be heard and determined by the Chief High Court Judge, or by 1 or more Judges nominated by the Chief High Court Judge, or both; and

(b) the court must, on a request by the Attorney-General and if satisfied that it is ~~desirable~~ necessary to do so for the protection of (either all or part of) the classified security information, receive or hear (the relevant part or all of) the classified security information in the absence of all or any of—

(i) the ~~defendant~~ non-Crown party; ~~or~~ and

(ii) ~~any or all~~ the barristers or solicitors (if any) representing the ~~defendant~~ non-Crown party; ~~or~~ and

(iii) journalists; ~~or~~ and

(iv) members of the public.; ~~or~~

~~(v) all of the above; and~~

~~(c) the court may, if satisfied that it is desirable to do so in order to ensure that a fair hearing will occur, appoint a barrister or solicitor as a special advocate to represent the defendant's interests on the terms that the court may direct.~~

~~(4) A special advocate referred to in **subsection (3)(c)**—~~

~~(a) must be a person who holds an appropriate security clearance that allows the person to see the classified security information:~~

~~(b) must not disclose the classified security information to the defendant (or any barrister or solicitor representing the defendant).~~

(5) Without limiting **subsection (3)**,—

(a) the court may approve a summary of the classified security information that is presented by the Attorney-General except to the extent that a summary of any particular part of the information would itself involve disclosure that would be likely to prejudice the interests referred to in **section 96(3)**; and

(b) on being approved by the court, a copy of the summary must be given to the ~~defendant~~ non-Crown party.

~~(6) Nothing in this section limits section 27 of the Crown Proceedings Act 1950 or any rule of law that authorises or requires the withholding of a document or the refusal to answer a question on the ground that the disclosure of the document or the answering of the question would be injurious to the public interest.~~

(7) **Subsections (2) to ~~(6)~~ (5)** apply despite any enactment or rule of law to the contrary.

97A Nothing in this subpart limits other rules of law that authorise or require withholding of document, etc

Nothing in this subpart limits section 27 of the Crown Proceedings Act 1950 or any rule of law that authorises or requires the withholding of a document or the refusal to answer a question on the ground that the disclosure of the document or the

answering of the question would be injurious to the public interest.

98 Ancillary general practices and procedures to protect classified security information

(1) Any general practices and procedures that may be necessary to implement the procedures specified in ~~**section 97**~~ this subpart and to ensure that classified security information is protected in all proceedings to which ~~that section relates~~ this subpart applies must be agreed between the Chief Justice and the Attorney-General as soon as practicable after the commencement of this section, and revised from time to time.

(2) General practices and procedures may be agreed under **subsection (1)** on the following matters:

(a) measures relating to the physical protection of the information during all proceedings to which ~~**section 97**~~ this subpart relates:

(b) the manner in which the information may be provided to the court:

(c) measures to preserve the integrity of the information until any appeals are withdrawn or finally determined.

(3) **Subsection (2)** does not limit **subsection (1)**.

Subpart 9—Miscellaneous provisions

Costs

99 Costs of interception capability on public telecommunications network or telecommunications service

The costs of developing, installing, and maintaining an interception capability on a public telecommunications network or a telecommunications service must be paid for by the network operator concerned.

100 Costs incurred in assisting surveillance agencies

(1) A surveillance agency must pay for the actual and reasonable costs incurred by a network operator or a service provider in providing assistance to the agency under **section 24**.

(2) A surveillance agency must pay the costs referred to in **subsection (1)** by the date specified for payment, whether in an invoice or other appropriate document given to the agency by a network operator or a service provider, being a date not less than 1 month after the date of the invoice or other appropriate document.

(3) This section—

(a) does not apply to a network operator that is complying with duties only under **section 11**; and

(b) is subject to **section 101**.

101 Surveillance agency not required to pay costs

(1) This section applies if a surveillance agency believes on reasonable grounds that—

(a) a network operator has not complied with any of the duties under this Act; and

(b) the non-compliance has—

(i) materially increased the costs incurred by the agency in the execution of an interception warrant or authority; or

(ii) materially increased the time that would otherwise be required to execute an interception warrant or authority; or

(iii) otherwise materially prejudiced the agency in executing an interception warrant or authority.

(2) The surveillance agency is not required to pay the costs referred to in **section 100** that are incurred by the network operator in providing assistance to the agency under **section 24** in relation to the execution of the interception warrant or authority.

(3) In this section, **interception warrant or authority** means an interception warrant or other lawful interception authority.

102 Dispute about costs must be referred to mediation or arbitration

(1) This section applies to any dispute about the reasonableness of the costs that are incurred, or are claimed to have been incurred, in the performance of the duties imposed by this Act that arises between,—

(a) in the case of costs under **section 99**, the Crown and a network operator; or

(b) in the case of costs under **section 100**, a surveillance agency and a network operator or a service provider.

(2) If a dispute to which this section applies is unable to be resolved by agreement between the parties, the dispute must be referred to—

(a) mediation; or

(b) if the parties are unable to resolve the dispute at mediation, arbitration.

(3) If a dispute is referred to arbitration under **subsection (2)(b)**, the provisions of the Arbitration Act 1996 apply to that dispute.

Protection from liability

103 Protection from liability

(1) This section applies to—

(a) every network operator; and

(b) every service provider; and

(c) every surveillance agency and the Director; and

(d) the Registrar and every other designated officer; and

(e) every person employed or engaged by a person referred to in **paragraphs (a) to (d)**.

(2) No person to whom this section applies is liable for an act done or omitted to be done in good faith—

(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.

(3) This section does not apply in relation to compliance with a direction given under **section 39 or 54**.

Other miscellaneous provisions

104 Notices

(1) A notice served for the purposes of this Part must—

(a) be in writing; and

(b) be signed by a designated officer or by any person purporting to act with the authority of a surveillance agency; and

(c) be served in accordance with **section 105**.

(2) All documents purporting to be signed by a designated officer or by or on behalf of a surveillance agency must, in all courts and in all proceedings under this Act, be treated as having been so signed with due authority unless the contrary is proved.

105 Service of notices

(1) Any notice required or authorised to be served on any person for the purposes of this Part may—

(a) be served on a company, within the meaning of the Companies Act 1993, in a manner provided for in section 388 of that Act:

(b) be served on an overseas company in a manner provided for in section 390 of the Companies Act 1993:

(c) be served on any other body corporate in a manner in which it could be served if the body corporate were a company within the meaning of the Companies Act 1993:

(d) be served on an individual—

(i) by delivering it personally or by an agent (such as a courier) to the person; or

(ii) by sending it by post addressed to the person at the person's usual or last known place of residence or business; or

(iii) by sending it by fax or email to the person's fax number or email address provided by the person for the purpose; or

(iv) in any other manner that a High Court Judge directs.

(2) Section 392 of the Companies Act 1993 applies for the purposes of **subsection (1)(a) to (c)**.

(3) In the absence of proof to the contrary, a notice, document, or notification sent to a person in accordance with—

(a) **subsection (1)(d)(ii)** must be treated as having been served on the person when it would have been delivered in the ordinary course of post, and, in proving the

delivery, it is sufficient to prove that the letter was properly addressed and posted:

(b) **subsection (1)(d)(iii)** must be treated as having been served on the person on the second working day after the date on which it is sent.

(4) If a person is absent from New Zealand, a notice served on the person's agent in New Zealand in accordance with **subsection (1)** must be treated as having been served on the person.

106 Powers not limited

This Act does not limit any power that a surveillance agency or any other person has under any other enactment.

107 Repeal

The Telecommunications (Interception Capability) Act 2004 (2004 No 19) is repealed.

108 Consequential amendments

Amend the enactments specified in the Schedule as set out in that schedule.

108A Savings provision for exemptions

(1) An exemption granted under section 11 of the Telecommunications (Interception Capability) Act 2004 that is in force immediately before the commencement of this section—

(a) continues in force on the same terms and conditions (including as to expiry) as if granted under **section 29** of this Act; and

(b) may be amended or revoked under that section.

(2) For the purposes of **subsection (1)**, an exemption from the requirements of a provision of the Telecommunications (Interception Capability) Act 2004 (the **2004 Act provision**) must be treated as being an exemption from the requirements of a provision of this Act that, with or without modification, replaces, or corresponds to, the 2004 Act provision.

109 Transitional provision relating to network operators

If a network operator has, at the date of first registration, less than 4 000 customers,—

(a) **section 13(2)** applies to the network operator, as long as—

(i) the network operator keeps a record of the number of customers it has each month in accordance with **section 13(6)**; and

(ii) the network operator maintains, from the date of first registration, an average of less than 4 000 customers over each 6-month period; and

(b) **section 13(3) and (4)** applies to the network operator accordingly.

110 Regulations

The Governor-General may, by Order in Council, make regulations providing for any matters contemplated by this Act, necessary for its administration, or necessary for giving it full effect.

Schedule

s 108

Consequential amendments

Crimes Act 1961 (1961 No 43)

In section 216K(4), definition of **network operator**, replace "section 3(1) of the Telecommunications (Interception Capability) Act 2004" with "**section 3(1)** of the Telecommunications (Interception Capability and Security) Act **2013**".

Films, Videos, and Publications Classification Act 1993 (1993 No 94)

In section 122A, definition of **network operator**, replace "section 3(1) of the Telecommunications (Interception Capability) Act 2004" with "**section 3(1)** of the Telecommunications (Interception Capability and Security) Act **2013**".

Income Tax Act 2007 (2007 No 97)

In section EX 20B(11)(b), replace "Telecommunications (Interception Capability) Act 2004" with "Telecommunications (Interception Capability and Security) Act **2013**".

National Animal Identification and Tracing Act 2012 (2012 No 2)

In Schedule 2, clause 1(1), definition of **call associated data**, replace "section 3(1) of the Telecommunications (Interception Capability) Act 2004" with "**section 3(1)** of the Telecommunications (Interception Capability and Security) Act **2013**".

In Schedule 2, clause 1(1), definition of **network operator**, replace "section 3(1) of the Telecommunications (Interception Capability) Act 2004" with "**section 3(1)** of the Telecommunications (Interception Capability and Security) Act **2013**".

Search and Surveillance Act 2012 (2012 No 24)

In section 55(3)(g), replace "section 3(1) of the Telecommunications (Interception Capability) Act 2004" with "**section 3(1)** of the Telecommunications (Interception Capability and Security) Act **2013**".

Search and Surveillance Act 2012 (2012 No 24)—*continued*

In section 70, definitions of **call associated data** and **network operator**, replace "section 3(1) of the Telecommunications (Interception Capability) Act 2004" with "**section 3(1)** of the Telecommunications (Interception Capability and Security) Act **2013**".

Telecommunications Act 2001 (2001 No 103)

In section 69C, definition of **sharing arrangement**, paragraph (c)(vii)(A), replace "Telecommunications (Interception Capability) Act 2004" with "Telecommunications (Interception Capability and Security) Act **2013**".

Legislative history

8 May 2013	Introduction (Bill 108–1), first reading and referral to Law and Order Committee

Wellington, New Zealand:
Published under the authority of the House of Representatives—2013