Privacy Commissioner
Te Mana Matapono Matatapu

Submission to the Independent Review of Intelligence and Security by the Privacy Commissioner

"A successful response to [terrorism and other] threats depends on entrusting public bodies with the powers they need to identify and follow suspects in a borderless online world. But trust requires verification. Each intrusive power must be shown to be necessary, clearly spelled out in law, limited in accordance with human rights standards and subject to demanding and visible safeguards."

David Anderson QC, Independent Reviewer of Terrorism Legislation, "A Question of Trust" (London, June 2015)

1. Introduction

1.1 This review provides an important and timely opportunity to assess New Zealand's intelligence and security legislation and its continuing fitness for purpose. In line with my statutory functions of providing advice on matters affecting the privacy of the individual, I see room for improvement in a number of key areas.

Key recommendations

1.2 My key recommendations for the review are:

i) Align the intelligence agencies more closely to the public sector governance and accountability framework including the privacy principles (in line with other public sector bodies that have intelligence functions), subject to specific exceptions

ii) Clarify and strengthen the privacy standards for internet and telecommunications (and associated metadata)

iii) Include explicit safeguards and procedures for all privacy intrusive powers such as bulk interception

iv) Strengthen oversight of international information sharing by the intelligence agencies

v) Create an Oversight Board to co-ordinate oversight of the intelligence agencies

Surveillance and secrecy

1.3 As I made clear in a recent speech to intelligence professionals at their annual conference, the societal bargain to be struck is not security OR privacy.[1] We have the opportunity to arrive at a solution where all interests that are important to New Zealanders are recognised and respected.

1.4 Using surveillance to deter violent and criminal activity, or to gather intelligence relating to such activity, may be a justifiable measure. However, the covert activities of the intelligence and security agencies potentially intrude on individual privacy interests. If they believe that they might be monitored by official agencies without their knowledge or consent, it can have a chilling effect on how individuals behave, travel or communicate, and result in self-censorship. The ongoing challenges are to ensure there is an appropriate system of thresholds, limits, checks and balances to avoid the overuse of surveillance and to address the perception that surveillance is used more widely than necessary.

1.5 The risks to the intelligence and security agencies of acting counter to New Zealanders' expectations are evident from historic instances where the agencies went beyond their authorised remit.[2] The reputational impact of agency failures undermines public trust and confidence, often in a disproportionate manner because the need for secrecy means we hear little about routine activities that would put these outlier cases more clearly in proportion.

1.6 Intelligence agencies hold sensitive and important data to help them avert serious threats, but so too do the Police, NZDF, Customs, and MFAT. I challenge the assumption that intelligence agencies can continue to be regarded as a special case that require significant departures from the normal public sector governance and accountability model. My strong view is that the intelligence agencies should be brought more closely in line with other public sector bodies having an intelligence role, subject to any necessary exceptions. Where there is a need for exceptions and carve-outs from normal accountability measures, this should be made explicit, and stringent checks and balances (and oversight measures) developed to fill the accountability gap.

Opportunities

1.7 In this submission I identify 8 challenges and opportunities for the review. Engaging with these challenges and introducing substantive improvements will contribute to:

i) modernising the legislative framework under which the intelligence and security agencies operate,

ii) improving public trust and confidence, and

---

[1] John Edwards, Privacy Commissioner "Privacy versus Security – the False Dichotomy and the Myth of Balance" speech to the New Zealand Institute of Intelligence Professionals Annual Conference (15 July 2015) https://privacy.org.nz/news-and-publications/speeches-and-presentations/privacy-commissioners-speech-to-nz-institute-of-intelligence-professionals/

[2] Well known examples include those involving Sutch, Choudry, Zaoui, and Dotcom.

iii) continuing the ongoing process of better integrating the intelligence and security agencies into New Zealand's public sector framework.

International reviews

1.8 A number of significant reviews of the intelligence and security landscape in particular jurisdictions, and internationally, have been released since 2013.

1.9 It is vital that New Zealand pays attention to international developments and seizes the opportunity to implement international best practice. Our intelligence and security agencies must respond to new and existing security challenges in a proportionate, reasoned and justifiable manner that is consistent with the rule of law. The legislative framework must support and reflect this approach.

Oversight

1.10 Oversight is a critical topic for this review. Because of the covert nature of the work of the intelligence and security agencies, and the secrecy of the information gathered and generated, the agencies are not generally subject to the routine scrutiny of the public or the media. Mechanisms such as the Official Information Act have limited reach due to the broad scope of national security withholding grounds. Citizens' rights of complaint are limited if they never learn of infringements of their rights.

1.11 Specialist oversight is therefore a proxy accountability mechanism for the public and can perform an important role in providing assurance about the role and work of the intelligence and security agencies. It is crucial that the oversight framework is comprehensive and that gaps and weaknesses are addressed by this review.

2. The challenges and opportunities of this review

Public confidence

2.1 **Improving public trust and confidence in the functions and activities of the intelligence and security agencies.**

2.1.1 The focus of my submission is to identify principled and practical measures to enhance the current checks and balances and to address gaps.

2.1.2 The opportunity to make improvements to the current framework is a valuable chance to improve public trust and confidence.[3] Key measures I suggest for improvement include:

---

[3] On the importance of trust, see David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review* [Anderson report] (London, June 2015), pp 245-246. On the emerging "credibility gap" that has undermined public confidence, see the Independent Surveillance Review *"A Democratic Licence to Operate"* (London, July 2015) [the ISR report].

- Enhancing transparency
- Updating the legislative framework to address identified weaknesses, uncertainty and ambiguity with the goals of:
  - Improving clarity, public understanding and accessibility
  - Building in key process standards and safeguards
  - Demonstrably protecting democratic rights and freedoms such as freedom of expression and communications privacy
- Ensuring adequacy of funding and resourcing for agency accountability and compliance activities
- Addressing weaknesses and gaps in oversight.

2.1.3 International events such as the rise of terrorism have required governments to ensure their intelligence agencies are fully equipped to respond to new threats. At the same time, whistle-blowers, courts, oversight agencies, politicians and civil society groups have all raised questions about the proportionality and necessity of certain intelligence gathering and assessment techniques, leading to governmental reviews and recommendations for reform. As a result, media interest in the activities of intelligence agencies worldwide has intensified.

2.1.4 Public attitudes to the intelligence agencies in the face of this media scrutiny fall on a wide spectrum from those who unquestioningly support the work of the agencies, to those who call for the curtailing of their special powers, or even their abolition. Our own biennial survey of public attitudes to privacy conducted in 2014 showed a fairly high level of concern about surveillance. 63% of respondents were concerned about the surveillance in New Zealand by overseas governments, while 52% were concerned about surveillance by New Zealand government agencies, including the intelligence agencies.

2.1.5 Intelligence agencies, like any public service department, are accountable for the exercise of their powers and must apply limited resources and triage their responses to the most serious threats. Nevertheless, the combination of routine secrecy with extraordinary powers demands appropriate and ongoing vigilance. New Zealanders need to be assured that the use of surveillance powers by the intelligence agencies is proportionate and accompanied by checks that ensure accountability.

Protecting democratic rights and freedoms

"There is no privacy without respect for security; there is no liberty without respect for privacy; security requires both certain liberties and privacy. It is therefore unfruitful (indeed misleading) to cast debates about privacy, liberty and security as a matter of choice or 'balancing' between these rights, still less to think of trade-offs between these rights… There is no metric for 'weighing' different rights, or even for comparing the 'weight' of different rights in particular cases. But it is feasible to set out robust standards that must be met in adjusting rights to one another and to devise and establish structures to do so."

Panel of the Independent Surveillance Review (London, July 2015)

2.2 Both security and privacy must be protected

Rejecting a simple dichotomy of security versus privacy

2.2.1 Old paradigms that give presumptive weight to national security without due regard to democratic rights and freedoms are outdated and should be discarded.

2.2.2 I suggest that the public is entitled to both privacy and security. The challenge is to craft a legislative framework that supports and enables key interests to be protected in appropriate circumstances. This is not so much a question of "balance", in the sense of a seesaw between privacy and security, but rather a question of how balance is to be built into the checks and controls that accompany the exercise of intrusive powers.

2.2.3 In a 2013 report commissioned by the US President, the review group recommended that security must be protected in both the national security and personal privacy contexts:[4]

> In the American tradition, the word "security" has had multiple meanings. In contemporary parlance, it often refers to *national security* or *homeland security*. One of the government's most fundamental responsibilities is to protect this form of security, broadly understood. At the same time, the idea of security refers to a quite different and equally fundamental value, captured in the Fourth Amendment to the United States Constitution: "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated…."[5] **Both forms of security must be protected**.

2.2.4 As noted by the Director of the NZSIS in her speech to the Identity Conference in May this year, we need both individual privacy and national security.[6] Describing her motivation for leading the Service, she said:

> "I want to protect [the New Zealand] way of life so we can continue to enjoy the things that are so wonderful about New Zealand, including the integrity of our institutions, the privacy of our citizens, and our democratic rights and freedoms."

2.2.5 I endorse the Director's articulation of the domestic context in which the intelligence agencies operate. We have long enjoyed national security, prosperity and democratic freedoms such as freedom of speech and individual privacy. We must be vigilant in protecting New Zealand's national security from serious threats and equally we must work hard to ensure that this is not at a cost to our democratic traditions and freedoms.[7]

---

[4] *Liberty and Security in a Changing World*, report and recommendations of the President's review group on Intelligence and Communications Technologies, 12 December 2013. https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

[5] For the comparable New Zealand provision, see the New Zealand Bill of Rights Act 1993, s 21.

[6] Rebecca Kitteridge, Director of Security, New Zealand Security Intelligence Service "Is the NZSIS interested in you? Privacy in the security world" (18 May 2015) http://www.nzsis.govt.nz/publications/news-items/Speaking_Notes_for_Identity_Conference.pdf

[7] In relation to rights compliance, see the Anderson report at pp 251-252.

2.2.6 It is worth remembering that these democratic freedoms have evolved over centuries of political struggle, revolution and upheaval. International instruments such as the Universal Declaration of Human Rights and International Covenant on Civil and Political Rights have framed these rights and freedoms in modern times and have helped to shape our own laws and conventions including the New Zealand Bill of Rights Act, the Human Rights Act and the Privacy Act. The right to privacy does not exist in isolation, but in the context of these international human rights instruments. Privacy is valuable in its own right; it also plays a pivotal role in supporting other significant rights such as freedom of expression, thought, conscience and religion.[8] It also plays a vital role in ensuring internet freedoms.[9]

Good process standards and safeguards

2.2.7 The opportunity to strengthen protections for democratic rights and freedoms such as privacy in the legislative framework would produce potential benefits for:

- New Zealanders' public trust and confidence in the intelligence agencies;
- New Zealand's international alliances and reputation; and
- New Zealand's economic interests in the developing tech sector.[10]

2.2.8 In terms of democratic rights, I am concerned in particular with ensuring adequate protection for **communications privacy**, which I address later in this submission.

2.2.9 Current international threats, from which New Zealand is by no means immune, are significant and concerning. The intelligence agencies must be suitably equipped to identify these threats so that all practicable steps can be taken to avert them. This may require the intelligence agencies to have recourse to unusual and special powers that override civil rights and intrude on personal privacy. However, the legislative framework under which the intelligence agencies operate must be carefully and deliberately developed on a "business as usual" basis. Any intrusive powers justified for serious threat situations must be strictly reserved and subject to strenuous oversight.

2.2.10 I am not proposing that in respecting democratic and human rights the intelligence agencies should be thwarted or handicapped in their operational activities. The thrust of my submission is that it is the quality of the process that is of central importance. There will be occasions where privacy intrusions through surveillance are a necessary and proportionate response to a particular issue. However, the seriousness of the privacy intrusion needs to be recognised through good process standards, including legal thresholds and warrant requirements. Civil rights and freedoms can be duly respected by paying careful attention to the process and

---

8 On privacy as a support for other fundamental rights, see the Anderson report at p25, 27-28.

9 See statement by the Global Commission on Internet Governance "Towards a Social Compact for Digital Privacy and Security" (2015) http://www.chathamhouse.org/publication/toward-social-compact-digital-privacy-and-security

10 See Juha Saarinen "The chilling effect of tech law" (The New Zealand Herald, 27 February 2015) http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11409067 "Routing around TICSA (The New Zealand Herald, 4 March 2015) http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11411053

warrant requirements under which special powers are exercised and the checks and balances that apply to them.

Risk to EU adequacy

2.2.11 I must also draw your attention to the potential consequences of New Zealand's legislative framework failing to adequately protect privacy interests. Our privacy framework has been assessed (after a protracted process) as being adequate under EU law. This removed the barrier to EU entities transacting business with New Zealand that involves the personal data of EU citizens. Findings of adequacy are rare and hard-won. Only 5 countries outside Europe have obtained this advantage.[11] Following international attention on the activities of the Five Eyes nations, Europeans' perception of New Zealand's role as a member of that alliance risks a revisiting of our adequacy status.

2.2.12 Any structural changes to the legislative framework that gives rise to a dilution of privacy rights may further jeopardise this status. I therefore suggest that it is in New Zealand's broader interests to maintain and protect privacy in the legislative framework.

Principles of a new framework

2.3 A principled approach to the legislative framework

Aligning the legislative framework with public sector governance and accountability

2.3.1 Historically, intelligence agencies have argued for special powers and special legislative treatment due to the nature of their work. Factors used to support that include:

- the intelligence gathering nature of the work of the agencies
- the reliance on human sources
- the seriousness of the activity and the threats to New Zealand being monitored
- the confidentiality of information to protect international sources and channels of information.

2.3.2 It is timely for these assumptions to be tested to assess whether the legislative framework should continue in force on an exceptional basis or to what extent the framework can be normalised.

2.3.3 My assertion is that these aspects of the work of the intelligence agencies are not unique. Other public sector agencies engage in intelligence gathering (the Police, Customs), rely on human sources (the Police), are concerned with activity that carries the potential for serious harm to the nation (Biosecurity, NZDF, Customs,

---

[11] Argentina, Canada, Israel, New Zealand and Uruguay.

Police) or have a strong interest in protecting sensitive channels of information from international sources (MFAT, Customs, NZDF, Police).

2.3.4 These other public sector agencies carry out their work within the general legislative framework and the systems of governance and accountability that apply to the public sector as a whole with such particular, rather than general, exceptions as are necessary. This suggests that it should be possible to normalise the legislative framework that applies to the intelligence agencies, to a comparable extent. Where there is a case to be made for a special or exceptional approach, powers or process, this needs to be clearly and demonstrably explained and justified, including the particular interests that require a special approach. Where those interests are extra-national, such as a condition of partnership with other countries, that condition should also be clearly and publicly stated and understood.

2.3.5 The Law Commission has noted that not all risks to national security need the same level of protection.[12] In my submission to that review, I noted that a generalised approach to defining "national security" can make it difficult to robustly verify that displacing the normal rights and assumptions is justified. I also supported a more granular approach to defining "national security" and articulating the public policy reasons for treating the information as sensitive.

2.3.6 The concept of 'national security' comprises a bundle of interests. Identifying each of the strands that make up that bundle can help make clear which roles or functions of the intelligence agencies require a bespoke approach.

The legislative framework should reflect key principles of democratic governance

2.3.7 The legislative framework also needs to firmly embed foundational concepts of New Zealand's legal framework. I suggest the following key elements that should form the foundation of a new legislative framework:[13]

Rule of law

2.3.8 The rule of law requires that the powers of the State that have the potential to intrude on the rights of citizens, and the lawful purposes for which they can be used, must be expressly set out in statute.

2.3.9 It is worth reflecting on the historic and influential case of *Entick v Carrington* (1765), involving the search of a house for "seditious papers" under a warrant signed by the Secretary of State. The warrant was successfully challenged on the basis it had been granted arbitrarily with no legal authority.

2.3.10 The case reflects an important element of the rule of law that State powers must be properly exercised. While citizens are free to do anything that is not expressly prohibited under law, governmental agents are prohibited from doing anything that it is not expressly allowed by case law or statute.

---

12 Law Commission *"National Security Information in Proceedings"* (IP 38, 2015) at [6.97].

13 See the ISR report's 10 tests for privacy intrusion including rule of law, necessity, proportionality, restraint, effective oversight, recognition of necessary secrecy, minimisation of secrecy, transparency, legislative clarity and multilateral collaboration.

Clarity and certainty

2.3.11 The scope of the powers of the intelligence agencies and the circumstances in which they can be used should be clearly and plainly set out in statute, in a way that is accessible and understandable for the general public. [14] The statutes should explicitly set out the range of intrusive powers available to the intelligence agencies, the purposes for which they may use them and the authorisation required before they can be used.

Necessity and Proportionality

2.3.12 An intrusion on human rights such as privacy must be both necessary for a lawful purpose, and proportionate to that purpose. This means asking:

- Is the action taken and the level of intrusion justified for the purpose for which it is being taken?
- Does the action taken appropriately limit unnecessary intrusion on the rights of third parties in whom the agency has no legitimate interest?

2.3.13 The elements of necessity and proportionality should therefore underpin the safeguards and controls on the exercise of State powers. They should also influence legislative definitions that underpin the scope of the legislation (such as the definition of "security") and the legislative thresholds such as "national security".

Explicit limits on powers

2.3.14 Each power should be explicitly limited and subject to appropriate safeguards: "firm limits must be written into law: not merely safeguards, but red lines that may not be crossed."[15]

2.3.15 Consideration should also be given to establishing clear purpose limits on the use of personal information held by the intelligence agencies from their different functions. For example vetting information should not be cross-shared for the purposes of intelligence gathering except in accordance with proper process and controls. Similarly, information that is produced through the information assurance and cybersecurity function should not be cross-shared for other purposes without due process measures.

Reasonableness

2.3.16 The reasonableness of the exercise of coercive State powers is a necessary corollary of section 21 of the New Zealand Bill of Rights Act 1990 - everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise.

---

[14] On the need for clarity, see the Anderson report at pp 252-253, the ISC report at p 83-86 and the ISR report, recommendation 2.

[15] Anderson report at [13.18].

Transparency

2.3.17 Sunlight of course is the best disinfectant, where it can safely be applied. Enhancements to transparency are necessary and desirable to improve public trust and confidence, oversight and accountability. This requires attention to be given to improving reporting and the removal or reduction of any unnecessary barriers to transparency.

Communications privacy

> *"The citizen's right to privacy online as offline – and what constitutes a 'justifiable' level of intrusion by the state – has become a central topic of debate. As traditional notions of national security and public safety compete with the realities of digital society, it is necessary to periodically renew the licence of the … security and intelligence agencies to operate."*
>
> Panel of the Independent Surveillance Review (London, July 2015)

2.4 **Enhancing communications privacy, subject to "authorised intrusion" by judicial warrant.**

Key points:

- **Surveillance is not well regulated** –The Law Commission's 2010 report on surveillance and privacy invasions highlights that surveillance law requires attention to ensure it is fit for purpose. This is the substantive area of the law that provides the context for and scope of the powers of the intelligence agencies and so it is critical to address the identified need for reform.
- **Data surveillance** – As recommended by the Law Commission, data surveillance merits an expert review. The rate of change over the 5 years since the Law Commission's report has strengthened the need for this topic to be examined.
- **Private communications** – Citizens' routine communications, whether telecommunications, email or internet, should be presumptively private, and require independent judicial authorisation before being intercepted by the intelligence agencies. This should be expressly clarified.
- **Metadata** –The distinction between content and metadata has blurred and the collection and interception of metadata should be subject to appropriate safeguards proportional to the potential privacy intrusion.
- **New Zealanders versus non-New Zealanders** – the differentiation in protection levels for private communications between citizens/permanent residents and others is questionable in human rights terms, is increasingly unworkable and should be discarded.
- **Private sector collection practices are not a basis for wider access by the intelligence agencies** – Comparing private sector information practices to those of the intelligence agencies is a false equivalence and should not form the basis for justifying reduced controls on privacy intrusions.

- **Encryption** – Citizens should not be prevented from taking up encryption technology to protect their communications.

Surveillance is not well regulated

2.4.1 As part of its comprehensive review of privacy law, the Law Commission released a 2010 report on surveillance and other privacy intrusions (outside of the Privacy Act).[16]

> We found that surveillance is not well regulated by the current law. Technology is developing rapidly and continually creating new ways of invading our privacy. There are legal controls on some kinds of surveillance but not all. The law is patchy and unsatisfactory, and contains some surprising gaps. We recommend in this report that the law should be rationalised and brought up to date…
>
> The report also discusses data surveillance. The existing law is capable of handling most kinds of invasive conduct of this kind, but it is complicated and contains logical anomalies and overlaps.

2.4.2 Law enforcement surveillance powers have been modernised to a large extent with the passing of the Search and Surveillance Act 2012. However, that Act does not generally apply to the intelligence agencies (unless assisting another agency) and does not address substantive issues such as the scope of lawful interception. One possibility is to more closely align intelligence agency powers with law enforcement powers.

2.4.3 Under the status quo however, the patchy and outdated state of our surveillance laws has direct implications for the powers of our intelligence agencies. To carry out any form of prohibited surveillance, the agencies require an authorisation process. But the risk is that any surveillance that is not expressly prohibited as a matter of policy is treated as permissible on the basis it is "not unlawful". Civil law protections that usually fill some of the gaps such as privacy tort claims, Privacy Act complaints or Bill of Rights Act proceedings are ineffective to control over-reaching privacy intrusions by the intelligence agencies. Updating surveillance laws should therefore be a priority, so that the powers and limits on the intelligence agencies are based on current societal norms and expectations.

2.4.4 I also support the Law Commission's recommended expert review of covert data surveillance given the rate of change since the computer misuse offences were introduced in 2003.

Disruption in the communications landscape and the privacy impact

2.4.5 Online communication and personal information deserve improved privacy protection in the intelligence and security context. While the communications

---

[16] Law Commission "Invasion of Privacy: Penalties and Remedies – review of the law of privacy Stage 3" (2010). The Law Commission's report still awaits a full government response.

landscape has fundamentally changed over the last 25 years with major advances in information and communications platforms and technologies and the rise of the internet, the legal controls that protect people's communications were developed for an earlier era and are no longer fit for purpose.

2.4.6 Traditionally there have been strong levels of protection for telephone communications and for mail. The parameters for protection depend on whether a person has a basis for suspecting the communication could be intercepted. That made sense in an era when communication was either in person, by telephone or in non-digital form. But in today's world, these parameters have become uncertain and largely meaningless.[17]

2.4.7 The issue we face is the disruptive nature of digital technology and its consequential impacts. Traditionally, our private papers and diaries are protected, both through property rights and because they are kept in private physical places. The same protections need to be adapted for our online lives. The challenge therefore is to develop privacy safeguards for our online presence that meaningfully equate to the traditional privacy protections we enjoy in private physical spaces such as our homes.

2.4.8 Information we consider to be personal, sensitive or confidential is no longer kept hidden under lock and key, but now exists in virtual form under varying levels of security, along with our photographs, networks of friends and contacts, daily messages and a myriad of other personal information, opinions, online searches and communications. The modern dispersed data model means expectations of privacy must now accompany data, as well as the devices by which it is transmitted and the locations in which it resides.

Restoring a presumption of privacy

2.4.9 In 2013, the statutory term "private communication" (used in other New Zealand statutes such as the Crimes Act since 1978) was added to the GCSB Act as a gatekeeper provision for protecting New Zealanders' communications from interception. In my view this was a backward step for communications privacy, and has raised public uncertainty about when personal communications are regarded as private and therefore safe from interception. The previous provision in the GCSB Act protected any "communication", broadly defined (other than the communications of a foreign person or organisation).[18]

---

[17] The issues with the definition of "private communication" are outlined in the Law Commission's report *"Invasion of Privacy: Penalties and Remedies – review of the law of privacy Stage 3"* (2010), pp 40-46. See also the submission of the Chair of the Legislation Advisory Committee to the Intelligence and Security Committee in relation to the 2013 amendments to the GCSB Act. http://www.parliament.nz/resource/en-nz/50DPMCISC_SUB_00DBHOH_BILL12122_1_LAC1/ae2cd10e7ad8f8cecff786ecae49200e29e8110d

[18] A "communication" includes "signs, signals, impulses, writing, images, sounds, or data that a person or machine produces, sends, receives, processes, or holds in any medium".

2.4.10 I recommend that this amendment should be reversed. The presumption should be that communications are private, but may be intercepted under appropriate authority where necessary and proportionate.[19]

2.4.11 Common communication methods such as telecommunications, email and internet communications need to be secure, trusted and relied on by the public. As noted above, the potential for surveillance, even if not often used, introduces a chilling effect, that is unwelcome in a vibrant democracy. Communications privacy forms a protective barrier beneath which individuality can be expressed and discovered and is a space that allows individuals to assert control over their identity. Privacy also serves a critical role in creating space for freedom of expression and the holding of opinions. It is a prerequisite for democracy[20] and part of the broader human rights infrastructure that needs to be embedded in the legislative framework.

2.4.12 The 2013 Kitteridge review of the GCSB noted some issues with the old provision such as the GCSB being able to test new equipment or assist with cybersecurity issues without breaching the GCSB Act.[21] In my view, appropriate specific provision can be made for such necessary activities in a manner that does not raise unnecessary doubt about the expected privacy of routine communications.

2.4.13 One of the questions the review is seeking to resolve is where to draw the line between protected private communications and communications made in public which do not warrant the same level of protection. In my experience, based on the Privacy Act model, this is not a difficult distinction to draw in practice. The Privacy Act has a definition of a "publicly available publication", which provides that personal information contained in a magazine, book newspaper or other publication that is generally available to members of the public, receives less protection than personal information in other contexts unless it would be unfair or unreasonable to use or disclose the information. The "reasonable expectation of privacy" test is another formulation used in contexts outside of the Privacy Act such as in privacy tort or in Bill of Rights Act section 21 cases, for which there is a growing body of case law.

2.4.14 In the case of social media content for example, there is a spectrum of private to public communication depending on the particular settings used. Whether a communication is public or private will be a question of fact in any particular case. There is also a possibility that a private communication could be disseminated by a recipient to a wider audience (whether on social media or by email or text). However that risk of wider sharing should not diminish the privacy of the channel used for the original communication.

---

[19] See statement by the Global Commission on Internet Governance "Towards a Social Compact for Digital Privacy and Security", p 12.

[20] ISR report, p 31.

[21] Rebecca Kitteridge, *Review of Compliance at the Government Communications Security Bureau* (March 2013) http://www.gcsb.govt.nz/assets/GCSB-Compliance-Review/Review-of-Compliance.pdf, p15.

2.4.15 Even in the case of publicly available information, there is a case for controls where personal information is collected by the intelligence agencies. The Canadian Privacy Commissioner has recommended regulating access to open-source information and investigations exploiting publicly available personal information sources, to ensure that the collection and use of personal information is necessary and proportionate to a lawful purpose.[22]

2.4.16 Question 11 of the submission form asks members of the public to comment on their level of comfort with the intelligence agencies having access to certain types of information (a mixture of content and metadata) to assist them to identify threats to New Zealand's interests:

- Time and date of email, text message or phone call, locations for send/receive
- IP addresses
- Communications content
- Internet browsing history
- Social media posts

2.4.17 I suggest that the questions for New Zealanders should be more nuanced. All of this information can be accessed under a warrant. Any proposal to allow any wider access needs to ask New Zealanders:

- Are there types of information or circumstances where they are comfortable with this information being accessible by the intelligence agencies without a warrant?
- If so, would they expect retrospective oversight and by whom?
- How should the information be protected from access that is not for a lawful purpose?
- Would they support the prolonged retention of this data to enable ongoing or future access by the intelligence agencies?
- Would they expect to be able to request access to their own data from the intelligence agencies under principle 6 of the Privacy Act?
- Would they expect to eventually be told about the monitoring by the intelligence agencies?
- Would they expect the information to be discarded once it had served its purpose?
- Would they expect the information to be shared with other domestic or overseas agencies, and if so, under what circumstances?

2.4.18 As David Anderson notes in his report:[23]

> Recent changes in privacy norms are not without relevance: they may for example have a bearing on whether there is a reasonable expectation of privacy in a particular type of data at a particular time. They do not however amount to any sort of argument for dispensing with constraints on the government's collection or use of data. Indeed as more of our lives are lived online, and as

---

[22] Office of the Privacy Commissioner of Canada "Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance" (January 28, 2014) https://www.priv.gc.ca/information/sr-rs/201314/sr_cic_e.asp

[23] Anderson report at [2.44].

> more and more personal information can be deduced from our electronic footprint, the arguments for strict legal controls on the power of the state become if anything more compelling.

Metadata

2.4.19 There are currently no express statutory safeguards for metadata.[24] Old paradigms that protect communications *content* but not *metadata,* are also outdated and should be discarded. The relevant distinction is not whether information is metadata or content, rather the question is whether the meaning potentially derived from the information raises a reasonable expectation of privacy. If so, specific safeguards should apply.

2.4.20 The Privacy Act does this through its definitional threshold of "personal information". The Privacy Act applies to any information (broadly defined and including metadata) that is "about an identifiable individual." In other contexts beyond the Privacy Act, a reasonable expectation of privacy has also been extended to metadata.[25]

2.4.21 In 2013, Parliament's Privileges Committee inquiry into the use of intrusive powers within the Parliamentary precinct considered whether the collection and release of metadata should be treated differently from substantive content. OPC's submission to that inquiry noted the potential for metadata to reveal personal information, and challenged the treatment of metadata as a discrete type of information:[26]

> Increasingly, it is becoming clear that the micro-level, transactional data that is stored about us can paint a very personal picture of our movements, activities, purchasing, and social engagement. As technology is integrated into our daily lives, the extent of the data collected, and its descriptive power, grows.

2.4.22 The President of the Law Commission's submission also noted that the distinction between content and metadata is disintegrating in the age of Big Data.[27] For practical examples illustrating the sensitivity of metadata, see the recent Stanford MetaPhone research.[28] There has also been judicial comment in the United

---

[24] s57 of the Privacy Act allows the holders of metadata to provide it in response to any request from intelligence agencies, without breaching the privacy principles.

[25] See for example, the Canadian Supreme Court decision, *R v Spencer*, 2014 SCC 43, finding a police request to an ISP for subscriber information without a warrant to be contrary to Charter rights protecting a reasonable expectation of privacy in the context of search and surveillance powers.

[26] https://privacy.org.nz/news-and-publications/reports-to-parliament-and-government/submission-to-the-privileges-committee/

[27] Sir Grant Hammond, Submission to the Privileges Committee Inquiry into intrusive practices in the Parliamentary precinct (11 October 2013) http://www.parliament.nz/resource/en-nz/50SCPR_EVI_00DBSCH_PRIV_12317_1_A363399/f6035283ac83b90bc1d66e6446f49f46183609d5

[28] Cyrus Farivar "Volunteers in metadata study called gun stores, strip clubs, and more" (March 13, 2014) http://arstechnica.com/tech-policy/2014/03/volunteers-in-metadata-study-called-gun-stores-strip-clubs-and-more/ "Metaphone: the sensitivity of telephone metadata" http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/ See also the US

Kingdom and Europe[29] recognising the personal nature of metadata (also known as communications data).

2.4.23 In a case involving Google and Safari users, the English Court of Appeal decided that internet browser generated information (made up of detailed browsing histories and information gleaned from double-click cookies that link the browsing history to an individual user or device) was capable of being personally identifiable information within the scope of the Data Protection Act (the UK equivalent of the Privacy Act).[30]

2.4.24 Another relevant case is the test case brought by Members of Parliament and others, where the UK High Court declared that the Data Retention and Investigatory Powers Act 2014 (DRIPA) was unlawful and the powers it contained in relation to telecommunications metadata were disproportionate, lacked clear rules restricting access to and use of the metadata to their particular purpose (namely, investigating and prosecuting serious criminal offending) and were not dependent on prior independent administrative or judicial review.[31]

2.4.25 The growing jurisprudence in this area suggests that it is no longer appropriate to maintain the traditional metadata/content distinction in developing frameworks that implicate privacy rights.[32] The United Kingdom reviews, while not discarding the distinction have suggested that certain categories of metadata should receive greater protection given their potential to reveal sensitive personal information.[33]

Privacy and Civil Liberties Oversight Board report on the telephone records program conducted under section 215 of the USA PATRIOT Act and on the operations of the Foreign Intelligence Surveillance Court (January 23, 2014) concluding the programme "lacked a viable legal foundation".

[29] *Digital Rights Ireland Ltd* v *Minister for Communications, Marine and Natural Resources and others*, CJEU (8 April 2014)

[30] Google v Vidal-Hall [2015] EWCA Civ 311. See also the Australian Privacy Commissioner's decision upholding a journalist's Privacy Act access request for his communications metadata. http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/privacy-determinations/2015-aicmr-35.pdf

[31] Davis & Ors, R (on the application of) v Secretary of State for the Home Department & Ors [2015] EWHC 2092 (Admin) http://www.bailii.org/ew/cases/EWHC/Admin/2015/2092.html

[32] See Electronic Frontier Foundation "Necessary and Proportionate - International Principles on the Application of Human Rights to Communications Surveillance – background and supporting international legal analysis", (May, 2014) http://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf "Protected Information" pp8-12. See also the Anderson report, recommendation 12 that would retain the distinction but recognises the potential intrusiveness of some data types may require particular authorisation.

[33] The Anderson report, recommendation 12 retains the metadata/content distinction but recognises the potential intrusiveness of some data types may require particular authorisation. See also the report of the United Kingdom's Parliamentary Intelligence and Security Committee *Privacy and Security: A Modern and Transparent Legal Framework* (London, 2015) (the ISC report) and the ISR report.

The communications privacy of non-New Zealanders

2.4.26 I am also concerned at the distinction that has been created between the privacy rights of New Zealanders and others, as protection for the communications privacy of non-New Zealanders is more limited under our current legislation. The differentiation in protections for private communications between citizens/ permanent residents and others is not justified on the basis of necessity or proportionality and should be discarded. The current approach is questionable on a human rights analysis and is increasingly difficult to justify or comply with in the current globalised communications environment.[34] Privacy protection under New Zealand law should apply regardless of status, unless there is a reasonable basis for departure, in the particular circumstances.[35]

2.4.27 Concerns about foreign espionage are understandable; however I suggest that a blanket presumption of lesser protection discriminates between people on the basis of nationality. The potential impact on visitors to New Zealand, as well as neighbouring countries, is not necessarily a proportionate response.[36] The default should be shifted so that the distinction applies only where there is a reasonable basis for applying it.

Private sector collection practices are not a basis for wider access by the intelligence agencies

2.4.28 Question 12 of the submission form asks people how comfortable they are with private companies such as Facebook and Google collecting personal data, and question 13 asks people if they are more comfortable with personal data being available to private companies or the GCSB.

2.4.29 The suggestion that a public willingness to disclose personal information on social media and to large corporate interests is equivalent to personal data being made accessible to the intelligence agencies is misguided.[37] The private sector, including Facebook and Google, are subject to the Privacy Act and its overseas equivalents. That means that I or my overseas counterparts can receive complaints from the public about private sector practices, I can initiate an enquiry into those practices

---

[34] Michael Geist "Why Better Oversight Won't Fix Internet Surveillance and the New Anti-Terrorism Bill" (3 February 2015) http://www.michaelgeist.ca/2015/02/better-oversight-wont-fix-internet-surveillance-new-anti-terrorism-bill/ ; Graham Smith "The tangled net of GCHQ's fishing warrant" (2 January 2015) http://cyberleagle.blogspot.co.uk/2015/01/the-tangled-net-of-gchqs-fishing-warrant.html

[35] See Report of the Office of the United Nations High Commissioner for Human Rights *"The right to privacy in the digital age"* (30 June 2014). http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

[36] See the 6 constraints on the surveillance of non-nationals including ensuring that surveillance of non-nationals is directed exclusively at protecting national security interests (not including commercial interests), and limiting disclosure of information about non-nationals if not relevant to protecting national security interests, recommended by the Presidential review group Liberty and .

[37] See the Anderson report at [2.43] noting the distinction between the activities of service providers and those of the State.

and make public comment about them, and I can co-ordinate with my overseas counterparts in relation to any enforcement action.

2.4.30 The intelligence agencies are exempt from much of the Privacy Act and so are not subject to these accountability and review measures. The nature of a citizen's relationship with a corporate entity compared to an agency of the State is also entirely different. The corporate entity collects information on the basis of its contractual terms of service and privacy policy disclosure which a citizen can accept in order to use the service, or the citizen can choose not to participate in the service. There is no citizen choice in any engagement with the intelligence agencies, and the intelligence agencies can use coercive state powers against citizens.

2.4.31 The third point of difference derives from the rule of law. Private actors including corporates are free to engage in lawful commercial practices that are not expressly forbidden. The intelligence gathering arm of the State however, in exercising intrusive powers, is limited to acting within its expressly stated mandate.[38]

2.4.32 This suggests that tighter and more explicit controls and limits on intrusive actions of the State are appropriate, compared to the controls on the private sector.

Encryption

2.4.33 Although not expressly raised in the submission form, encryption is a topical and critical issue in the relationship between the public and the intelligence agencies, and for communications privacy.[39] Encryption is a double-edged sword – it can protect communications privacy; however it can also raise a need for decryption where the intelligence agencies intercept encrypted communications.

2.4.34 It is my clear view however that any steps to limit the uptake of encryption technology by the general public would be counter-productive. The public and organisations that are stewards of personal and confidential information must be free to take steps to protect privacy and security, and encryption is a necessary and reasonable measure. It is also consistent with the information assurance and cybersecurity functions of the intelligence agencies to facilitate the use of encryption as a security measure. While decryption may create challenges for the agencies, other solutions must be sought, such as ancillary legal powers and technological solutions.

Bulk data collection & retention

2.5 Setting appropriate controls and process around the use of bulk data

2.5.1 In 2013, there was a flurry of debate about whether the GCSB is empowered to engage in "mass surveillance". The report of the House of Commons Intelligence and Security Committee details the capabilities of the GCHQ in this area.[40] Bulk

---

38 See *Entick v Carrington*, noted above.

39 See the discussion in the ISR report, pp 12-14, 106.

interception capability is used by the GCHQ to investigate the communications of individuals already known to pose a threat, or to generate new intelligence leads. Bulk interception is described in the ISC report as involving three stages of filtering, targeting and selection:

- Choosing which communications links to access;
- Selecting which communications to collect from those links; and
- Deciding which of the collected communications should be read, analysed or examined and stored for further analysis.

2.5.2 My assumption is that the GCSB interprets its own powers to enable the targeting of particular batches of communications (rather than individualised communications) in the search for intelligence.[41] If my assumption is correct, I support greater transparency in the legislative framework as to the powers of the GCSB in relation to bulk data. If that is not the case, then this capability should be expressly prohibited.

2.5.3 The isolating of communications in bulk, even if few are actually scrutinised, gives rise to concerns for communications privacy. The public has very little way to understand how their communications are protected in the event that they are processed in some way by the intelligence agencies.

2.5.4 The ISC report grapples with this topic in detail and discusses various measures and safeguards relating to proportionality including limits on "fishing expeditions", the use of selection rules that must be applied, filtering and triage, criteria for examination, the numbers of innocent communications incidentally collected, length of retention and security issues, oversight and audit. The Parliamentary Committee concluded that the capability should be retained, subject to being tightly controlled and subject to proper safeguards, recommending that a criminal offence should be introduced in the event that interception capabilities are misused. David Anderson QC also recommended specific limits on the use of bulk interception warrants.[42]

2.5.5 In the New Zealand context, the question that needs discussion is the nature of the safeguards, protections and controls that apply to these practices by our own agencies, if they are being used. This would ensure that current practices are scrutinised and improvements made where necessary. It would also greatly assist the public to understand that the powers of the intelligence agencies are not to be used indiscriminately or to conduct "mass surveillance", but are to be used appropriately as a reasonable and proportionate response, with suitable checks and balances.

2.5.6 The ISC report also highlights the reliance of the intelligence agencies on bulk personal datasets.[43] The Parliamentary Committee recommended that the capability for using large databases of personal information to identify individuals,

---

40 ISC report, chapter 4. See also the ISR report, recommendation 8.

41 Note the Anderson report at p 360: "Given the restrictive nature of [intelligence warrant] requirements, it is unlikely that NZSIS has any power to carry out bulk interception."

42 Anderson report, recommendations 40-49, 79-80.

43 ISC report, chapter 7. See also the ISR report.

establish links and verify information should be acknowledged in statute and tightly regulated. This is an issue that should also be examined and addressed in the New Zealand review of the adequacy of legislative settings.

Internal Controls – privacy and good process

2.6 Embedding privacy and good process measures in the legislative framework

2.6.1 This review represents an opportunity to ensure that privacy and other good process measures and safeguards are embedded in the legislative framework. In this section I comment specifically on privacy and related measures.

Privacy standards

2.6.2 The intelligence agencies are subject to privacy principle 6 (right of access to personal information), principle 7 (right to seek correction of personal information) and principle 12 (regulating the use of unique identifiers). They have an exemption from the other privacy principles by virtue of section 57 of the Privacy Act. In its review of the Privacy Act, the Law Commission recommended that more (but not all) of the privacy principles should apply to the intelligence agencies.[44]

2.6.3 The Privacy Commissioner can deal with complaints about breaches of principles 6, 7 and 12 by the intelligence agencies; however, these matters do not proceed to the Human Rights Review Tribunal as there is a special procedure by virtue of section 81 of the Privacy Act. Under this procedure, the Privacy Commissioner can report any interference with privacy to the agency concerned and make recommendations. If no action is taken, the Privacy Commission can raise the matter with the Prime Minister who must lay a report before Parliament.

2.6.4 In 2013, the Government Communications Security Bureau Act was amended to include a new requirement in section 25A for the GCSB to develop a personal information policy, in consultation with the Inspector General and the Privacy Commissioner. The policy is to apply equivalent principles to privacy principles 1, 5, 8 and 9 as set out in s 25B of the GCSB Act. Non-compliance with the policy as revealed by audits is to be reported to the Privacy Commissioner, who in turn can report to the Inspector General. However, there is no complaints jurisdiction in relation to non-compliance. While the GCSB amendments go some way towards remedying the gap in privacy standards, I am not persuaded that the measures set out in sections 25A and 25B of the GCSB Act are sufficient; indeed, I have significant reservations about the capacity of these provisions or any policy developed under it to materially add to privacy protections and public confidence.

2.6.5 Given developments since the Law Commission's 2011 Privacy Act review, I submit there is now a strong case for removing the section 57 exemption and moving to apply all of the principles to the intelligence agencies with specific exceptions on a

---

[44] Law Commission *"Review of the Privacy Act 1993"* (R123, 2011) recommendation 46. The Law Commission recommended that principles 1, 5, 8 and 9 should also apply to the intelligence agencies. The submissions of the intelligence agencies to the Law Commission's review indicated no objection to becoming subject to these principles.

case by case basis. This would put the intelligence agencies on a similar footing to the Defence Force, Police, Customs and MFAT, all of which carry out sensitive and important work while complying with the Privacy Act.

Privacy by Design

2.6.6 I was impressed on my visit to Washington DC earlier this year to hear about the use of Privacy Impact Assessments by the Department of Homeland Security (including publication on their website). A 2014 report highlights that the Department of Homeland Security (DHS), the intelligence community and the US Department of Defence are among the leaders in developing privacy-protective technologies and policies for handling personal data.[45] The report highlights practices such as data tagging to enforce usage limitations, controlled access policies and immutable auditing that can be integrated into databases and data practices to provide built-in protections for privacy and civil liberties.

2.6.7 Data tagging is a set of safeguards that tracks where information has come from, where it goes and under what authority. It enables access controls on a need to know basis and preserves links to source data and the purpose of its original collection, and can allow for specific use limitations or special cases governed by law or regulation. The DHS used privacy impact assessments as a tool in developing this model for data management.

2.6.8 I would like to see greater adoption of PIA processes by our own intelligence and security agencies as they develop their IT infrastructure, and a greater emphasis on Privacy by Design. This is an area that the intelligence and security agencies could be required to regularly report on, either to me, to the Inspector General or in their annual report.

Transparency requirements

2.6.9 Increasingly, the intelligence agencies both in New Zealand and overseas, are recognising that blanket secrecy can be counter-productive, and that steps can safely and productively be taken towards introducing transparency measures.[46]

2.6.10 I encourage greater reporting by the intelligence agencies on the use of their powers.[47] While the trade-off between transparency and national security remains complex, there are ways such as reporting aggregated intelligence requests figures that allow the public to have greater insight into the extent and use of intelligence powers without harming national security. I note with interest that other jurisdictions have taken steps to loosen laws that govern public reporting on requests for information made by the intelligence agencies to third parties (usually in the private sector). For example, Facebook in the United States can report on the number of

---

[45] Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* (The White House, May 2014) https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

[46] See discussion in the ISR report, pp 42-44.

[47] See also the recommendations of the Privacy Commissioner of Canada "Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance" (January 28, 2014)

intelligence requests they receive. National Security Letters and Foreign Intelligence Surveillance Act requests are to be reported in bands of 1000 in Facebook's government request reports.

2.6.11 My Office is currently exploring policy options for developing a role in the reporting of law enforcement requests for personal information, including the feasibility of providing a portal through which reporting statistics can be released by a range of organisations based on common metrics.

2.6.12 One option might be a platform for reporting on requests received from a range of public sector agencies, including the law enforcement and intelligence agencies. However, there are currently legislative restrictions that prevent the inclusion of requests data from the intelligence agencies.

2.6.13 In my view, it would be desirable to review this aspect of the legislation so that a form of reporting on compliance with intelligence agency requests can be facilitated. It should be possible to develop appropriate reporting bands to give the public a picture of the frequency with which requests are made by the intelligence agencies and where they are directed, without creating an undue operational risk. This serves public trust, confidence and accountability.

Information sharing

2.6.14 There is growing public awareness of the role of our intelligence agencies in alliances such as the Five Eyes, and the potential for intelligence to be shared with overseas counterparts. To an extent, it would seem that our intelligence agencies are assisting overseas allies as actors in a common enterprise that is broadly but indirectly in New Zealand's national interests. This places our agencies in a different position to the role they play where they act for a purpose that is directly in New Zealand's interests. And yet, the legislative framework does not acknowledge that difference or provide for how the sharing of personal information should take place or how it should be authorised.

2.6.15 There are a number of questions about the provision of mutual assistance by the intelligence agencies. For example:

- Is raw unexamined information shared with overseas counterparts, or only the results of targeted analysis (with extraneous information being discarded)?
- Is there appropriate authorisation for the sharing, both in New Zealand and for the request from the overseas jurisdiction?[48]
- How are fundamental concepts such as necessity, proportionality and reasonableness taken into account before the information is shared?
- Is New Zealand "obliged" to comply with overseas requests (as a price of membership) or are requests considered on a case by case basis?
- What is the nature of the privacy safeguards that apply to the information once it is shared overseas? Are there limits on further sharing of that information?

[48] The GCSB Act allows for intelligence to be shared with any overseas person on authorisation by the Minister, without specifying criteria for the granting of a ministerial authorisation.

- Is there adequate oversight of sharing arrangements within New Zealand and across jurisdictions?

2.6.16 The ISC report examines the topic of international information sharing and finds it unsatisfactory that sharing arrangements are implemented as a matter of practice and policy only. It proposes that future legislation should define this more explicitly including defining the powers, describing the circumstances in which intelligence may be shared and the constraints governing such exchanges.[49]

2.6.17 I believe this is an issue that should be addressed by this review and reformed in the legislative framework, given the significant potential impact on human rights. There is a strong case to be made for suitable safeguards to ensure that the sharing of intelligence information is proportionate and justified, limits adverse impacts on individuals, and complies with New Zealand law.[50]

Oversight

2.7 Addressing weaknesses and gaps in effective oversight

Oversight agencies

2.7.1 The **Inspector-General of Intelligence and Security** (IGIS) has the lead role in oversight of the intelligence agencies. A mix of other Parliamentary and executive agencies have oversight roles for aspects of the work of the work of the intelligence agencies:

- **The Ombudsman** – oversees compliance with the Official Information Act and can refer Ombudsman Act complaints to the IGIS
- **The Auditor-General** – has power under the Public Audit Act to examine the performance of any public entity and compliance with statutory obligations.
- **The Privacy Commissioner** – reviews complaints under principles 6, 7 and 12; can make recommendations to the intelligence agency and reports to the Prime Minister. Power to inquire into any matter if it appears the privacy of the individual may be infringed; can refer a complaint to the IGIS.[51]

2.7.2 Any potential overlaps between the different oversight bodies are dealt with by statutory consultation and referral provisions. This mechanism removes any unnecessary duplication. These multiple accountabilities may sometimes be

---

[49] ISC report pp 90-94; Anderson report, recommendations 8, 76-78; Council of Europe Commissioner for Human Rights *Democratic and effective oversight of national security services* (Issue paper, Strasbourg, May 2015), recommendation 5. See also Privacy Commissioner of Canada "Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance" (January 28, 2014) https://www.priv.gc.ca/information/sr-rs/201314/sr_cic_e.asp

[50] See also Electronic Frontier Foundation "Necessary and Proportionate - International Principles on the Application of Human Rights to Communications Surveillance" (May 2014).

[51] Office of the Privacy Commissioner "Privacy Commissioner's role in oversight of GCSB" (17 September 2014) https://privacy.org.nz/blog/gcsb/ "American takeaways" (10 March 2015) https://privacy.org.nz/blog/american-takeaways/

regarded by the intelligence community as creating a compliance burden. But this arrangement ensures that the intelligence agencies are firmly linked to the public sector accountability structure, and benchmarks compliance performance against the rest of the public sector. In my view, oversight by a range of expert bodies helps to lift overall compliance by the intelligence agencies. The involvement of expert bodies also helps guard against any risk of regulatory "capture" that may exist if there is only one oversight agency.

2.7.3 It is critical that the intelligence agencies are appropriately funded for their compliance work and processes so that compliance is not simply an "add-on" to the central and pressing work the agencies engage in, but an integral component of their operations.

A proposed Oversight Board

2.7.4 A range of different oversight structures are used internationally. The United States President has created a Privacy and Civil Liberties Oversight Board.[52]

2.7.5 I believe there is potential for the current New Zealand oversight agencies to come together with other to form an Oversight Board. This would assist to formalise oversight co-operation between these bodies, raise the public profile of oversight functions, improve the focus on privacy and human rights impacts within the intelligence agencies and create a forum for developing policy issues in oversight.

The role of the Inspector-General

2.7.6 The Inspector-General's role was strengthened in 2013. Nevertheless the review is a timely opportunity to examine whether improvements can be made.[53]

2.7.7 <u>Independence</u>

Consideration could be given to steps to strengthen independence. For example, currently:

- the Minister approves the Inspector-General's workplan;
- there are limits on inquiries into matters that occurred prior to 1996;
- there are limits on material that can be disclosed to the Inspector-General should the Minister issue a national security certificate.

2.7.8 <u>Explicit oversight</u>

I also recommend that consideration be given to providing in statute that certain key areas attract explicit oversight, for example:

- Communications privacy and interception powers
- Information sharing

---

[52] Privacy and Civil Liberties Oversight Board, Washington D.C. https://www.pclob.gov/about-us.html

[53] See for example the recommendations of the Council of Europe Commissioner for Human Rights *Democratic and effective oversight of national security services* (Issue paper, Strasbourg, May 2015).

- Bulk data sets
- Information assurance and cyber security
- Vetting processes

2.7.9 Express recognition in the statute would confirm the importance of scrutiny of these areas, and assist to promote public trust and confidence that sensitive areas are actively monitored by an independent agency.

2.7.10 Whistleblowing

I also recommend that particular consideration be given to whistleblowing procedures. Every effort should be made to ensure that concerns can safely be raised with the Inspector-General (anonymously if necessary) so that the whistleblowing processes act as an effective safety valve. This helps to address the risk of significant harm to national security interests through any unauthorised leaking of information.

Expanding Privacy Commissioner oversight

2.7.11 As highlighted in the previous section, there is a strong case for reforming sections 57 of the Privacy Act and removing the current Privacy Act exemption that applies to the intelligence agencies.

Co-ordinating oversight

2.7.12 There is growing awareness among national oversight bodies that measures are needed to facilitate effective oversight of intelligence agency co-operation arrangements and the collecting and sharing of intelligence across national borders. The Dutch Review Committee on the Intelligence and Security Services described the problem in its 2014 Annual Report, coining the term "accountability deficit".[54]

> The Committee points out that more and more often the question is raised in international forums whether national oversight is still sufficient. The work of intelligence and security agencies extends beyond national borders; operations are carried out together with other services and exchanging information is a commonplace procedure. The mandate of national oversight bodies is limited to the information about such co-operation that is made available at the own national service. This makes it difficult to examine what foreign services do with data provided by a national service. Often, it is not possible for an oversight body to ascertain whether the data which the national service receives from abroad was collected lawfully. A national oversight body can only examine whether the national service provided or received information lawfully. This limit on what national oversight can do is also referred to as an 'accountability deficit'.

2.7.13 The opportunity for this review is to ensure that potential positive consultation and engagement between oversight bodies, both domestically and internationally, is

---

[54] This will be one of the themes of the International Conference of Data Protection and Privacy Commissioner in October this year.

enabled by the legislative framework and any unnecessary barriers are removed, subject to secrecy provisions to protect classified information.

Countering Terrorist Fighters legislation

2.8 Strengthening safeguards and oversight of agency powers acquired through the CTF legislation

2.8.1 The Countering Terrorist Fighters legislation that resulted in changes to the NZSIS Act and other statutes was enacted after a truncated policy development and parliamentary process. This review is an opportunity to reflect on the amendments that were made and to make any necessary adjustments.

2.8.2 In my submission to the Foreign Affairs, Defence and Trade Committee, I highlighted three areas of concern:

- The duration of visual surveillance warrants;
- The introduction of warrantless surveillance powers; and
- Controls on NZSIS access powers to Customs passenger name record data.

Visual surveillance warrants

2.8.3 I continue to support a reduction in the length of visual surveillance warrants (currently 12 months). I suggest a shorter period would be appropriate (3 months) with flexibility for a warrant to be renewed if ongoing surveillance is necessary.

Warrantless surveillance

2.8.4 I continue to support a reduction in the period of warrantless surveillance (currently 24 hours). It should be possible in my view for warrants to be arranged within a shorter timeframe, removing the need for warrantless surveillance except in the rarest of circumstances. Administrative arrangements need to be improved so that this objective is achievable.

Access to Customs databases

2.8.5 The system under which Customs collects passenger name record data is undergoing change. The safeguards in the CTF legislation were predicated on the prior model under which data was available to Customs only within a 28 day window, with any other access requiring a warrant. Changes to the way that Customs receives this data means that safeguards around NZSIS access will need to be reviewed.

14 August 2015