Human Rights Commission
Te Kāhui Tika Tangata

Human Rights Commission: Submission on the Independent Review of Intelligence and Security Services

---

To: Sir Michael Cullen and Dame Patsy Reddy - The Reviewers, Independent Review of Intelligence and Security Services

And to: Ministry of Justice

Date: 14 August 2015

Submission of Human Rights Commission

Independent Review of Intelligence and Security Services

14 August 2015

Introduction

1. The Human Rights Commission welcomes the opportunity to provide this submission to the Independent Review of Intelligence and Security Services ('the Review'). The Commission's position can be summarised as follows:

   1.1 The Commission considers that there is a strong case for substantial reform of New Zealand's intelligence and security regime. Such reform should be guided by a principled yet pragmatic methodology that maximises public trust and confidence in the operations of our intelligence and securities agencies. The Commission endorses the principles designed by David Anderson QC[1] and the Independent Surveillance Review Panel[2] in their recent reviews of UK intelligence and security system as being instructive for this purpose.

   1.2 Accordingly, the Commission considers that the societal challenges brought about by contemporary (and future) electronic surveillance and data interception technology requires that consideration be given to incorporating the right to privacy into New Zealand law through inclusion in the rights and freedoms protected under the New Zealand Bill of Rights Act 1990.

2. The Commission's specific recommendations for the Reviewers to consider can be found at paragraph 19 below.

3. Human rights are of central importance when considering intelligence and security policy, practice and legislation. The Commission appreciates the

[1] David Anderson QC, *A Question of Trust, Report of the Investigatory Powers Review,* June 2015, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf

[2] Independent Surveillance Review, *A Democratic License to Operate, Report of the Independent Surveillance Review*, Royal United Services Institute for Defence and Security Studies, July 2015, https://www.rusi.org/downloads/assets/ISR-Report-press.pdf

interest the Reviewers have taken in this matter to date and welcomes any opportunity for ongoing dialogue.

Initial Observations

4. Over the last two years, the role and functions of New Zealand's intelligence and security services have been subject to an unprecedented degree of public interest, judicial scrutiny and legislative reform. This occurred against a backdrop of domestic and international events that shone a public spotlight on intelligence services, in particular their extensive mass surveillance and data interception capabilities. The Commission has taken a close interest in these developments and their implications for human rights in New Zealand[3].

5. The legal and operational functions of these essential services give rise to human rights considerations that are fundamental to the functions of a modern democratic state. With this in mind, the Commission recommended in its 2013 report to the Prime Minister that an independent review of New Zealand's intelligence and security regime take place[4]. The Government has referred to the Commission's recommendation, and the subsequent legislative action it took to establish the periodic review process, in its sixth periodic report to the UN Human Rights Committee under the International Covenant on Civil and Political Rights[5].

6. The activities of intelligence and security agencies can be described as having a two-fold effect on human rights. Firstly, these activities may limit the human rights of people in New Zealand, an obvious example being the impact of surveillance operations on the privacy rights of affected persons. Conversely, the role and functions of intelligence and security services enhance the government's capability of meeting its human rights related duty to protect its people from harm.

[3] For further detail, please refer to the bundle of Commission reports and related international materials dated 27 July 2015 provided to the Reviewers
[4] Human Rights Commission, *Report to the Prime Minister: Government Communications Security Bureau and Related Legislation Amendment Bill; Telecommunications (Interception Capability and Security) Bill, and associated wider issues relating to surveillance and the human rights of people in New Zealand*, 9 July 2013, para 49, p 12
[5] New Zealand Government, *New Zealand's sixth periodic report under the International Covenant on Civil and Political Rights*, 2015, p 13, paras 83-88

7. This has led to a complex, polarised public debate, both in New Zealand and internationally. In his review of the UK's intelligence and security legislation, David Anderson QC described this debate as "double-jointed", dominated by the arguments of law enforcement officials and "securocrats" for more operational capability and fewer restraints on the one hand; and arguments by civil liberties advocates for more safeguards and less capabilities on the other. Anderson comments that "the silent majority" (the general public) sit in between these positions "in a state of some confusion."[6]

8. At heart of this debate lies a perception that a trade-off is required between privacy rights and rights related to personal security[7] in order to enable the operations of the intelligence and security services. The Commission submits that such a characterisation is too narrow. Instead, a balanced position can be found within the human rights concepts and principles that underpin the modern democratic state[8].

9. This balance has been explored in detail in the recent reports issued by David Anderson QC and the Independent Surveillance Review Panel (the ISR Panel)[9]. The approaches taken in those reports are instructive and of invaluable application to the New Zealand context.

10. Anderson's approach in balancing the complex and competing sets of interests is to place the notion of trust at the heart of the matter, noting that *"if one thing is for certain it is that the road to a better system must be paved with trust."* The Commission considers that, in order to earn the trust of the public, the "trustworthiness" of laws, institutions and practices is a matter of paramount importance in this respect.

11. In order to achieve a more balanced, accessible system that more effectively reflects and responds to the public interest, Anderson recommends that the

[6] *A Question of Trust*, p 245, 13.1. 13.2
[7] Such as the right to life and the right to personal security (Article 3 of the Universal Declaration on Human Rights and Articles 6 and 9.1 of the ICCPR)
[8] For the historical context informing the Commission's position, refer to speech by David Rutherford, Chief Commissioner, *Protecting the balance: trust, confidence, privacy and intelligence, NZIP Annual Conference*, 15 July 2015, https://www.hrc.co.nz/news/protecting-balance-trust-confidence-privacy-and-intelligence/
[9] The ISR Panel consisted of senior stakeholder representatives from across government, industry, civil society and Parliament – see *A Democratic License to Operate*, para 0.3

design and operation of intelligence and security legislation, policy and practices reflect the following five inter-related principles[10]:

- Minimise no-go areas
- Limited powers
- Rights compliance
- Clarity and transparency
- A unified approach

12. The ISR Panel frames the relationship between the public and the government security and intelligence services within concept of the eponymous "democratic license to operate", whereby the mandate of the intelligence and security services is derived from the consent of the people through the democratic process.

13. The ISR Panel based the notion of a "democratic license to operate" upon three distinct "deals".[11] The first deal exists between citizen and state and must be reflected in a clear, transparent legal framework and a coherent, visible and effective oversight regime. The second deal regards an improved "shared understanding" between the government and private sector as to the role internet and telecommunications companies have to play in sustaining the essential principles that govern an open society. The third deal concerns the importance of international harmonisation. This concept is particularly important when considering New Zealand's role in the Five Eyes Alliance and its obligations under international human rights treaties.

14. This approach provided the foundation for the ISR Panel's development of the following ten 'tests' with which to measure the potential intrusive impact of new legislation or regulations governing intelligence and security powers. These tests are:

- Rule of law
- Proportionality
- Necessity

[10] *A Question of Trust* pp 246-255
[11] *A Democratic License to Operate*, para 5.30-5.34

- Restraint
- Effective oversight
- Recognition of necessary secrecy
- Minimal secrecy
- Transparency
- Legislative clarity
- Multilateral collaboration

15. The Commission also wishes to emphasise the value of the recent work of UN entities in defining the role of intelligence and security services within the terms of the international human rights framework. In particular, the reports of UN Special Rapporteur Martin Sheinin to UN Human Rights Council that set out best practice guidelines [12] are particularly useful points of reference against which intelligence and security policy and legislation can be assessed.

Related issues outside the scope of the Review

16. The Commission notes that the 2013 and 2014 legislative reforms to intelligence and security law have avoided the issue of countering radicalism, nor has the use of ethnic or racial profiling in surveillance operations been directly addressed. The Commission considers that both civic education initiatives and community development approaches that avoid stigmatisation of particular communities are essential components of any security framework. These activities should have the ongoing resource and support required for them to flourish [13]. These measures are also an important component of Pillar 1 of the UN Global Counter-Terrorism Strategy, which calls upon States to[14]:

[12] Human Rights Council, Reports of Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism – *Ten areas of best practice in countering terrorism* A/HRC/16/51, 22 December 2010; *Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, A/HRC/14/46, 17 May 2010

[13] Speech by David Rutherford, Chief Commissioner, *Protecting the balance: trust, confidence, privacy and intelligence, NZIP Annual Conference*, 15 July 2015, https://www.hrc.co.nz/news/protecting-balance-trust-confidence-privacy-and-intelligence/

[14] United Nations Global Counter-Terrorism Strategy, A/RES/60/288, 2006, Pillar 1, para 3

"promote a culture of peace, justice and human development, ethnic, national and religious tolerance and respect for all religions, religious values, beliefs or cultures by establishing and encouraging, as appropriate, education and public awareness programmes involving all sectors of society."

17. The Commission also notes the ongoing challenge posed by the exponential growth in the collection and use of personal data by private sector entities. The ISR Panel has noted that the public is as equally, if not more, concerned about the use of personal data by private companies as they are in respect of government agencies[15]. The ISR Panel goes on to express its concern that mass data collection and surveillance by private sector organisations are "largely overlooked in discussions of transparency"[16]. While this concern falls outside the scope of this Review, the Commission considers that the Review's findings may have the potential to model best practice approaches that are of application across the public and private sectors.

Summary of the Commission's recommendations

18. The Commission has focused its submission at high-level issues arising from the Review rather than statutory detail. A summary of the Commission's positions on the various amendments to intelligence and security legislation that have taken place since 2013 can be found in the annexure to this submission.

19. The Commission has accordingly formulated the following recommendations for the Reviewers to consider:

    a. **That the Reviewers undertake a comprehensive review of New Zealand's intelligence and security legislation for consistency with international human rights law and norms.**

    b. **That the Reviewers consider ways in which the clarity, accessibility and structure of New Zealand's intelligence and security legislation can be improved.**

[15] *A Democratic License to Operate* p 35, para 2.24
[16] ibid p 44, para 2.53

c. **The Commission recommends that the Reviewers consider the implications that inclusion of the right to privacy in the New Zealand Bill of Rights Act would have for intelligence and security law, policy and operations.**

d. **That the Reviewers investigate the implications of consolidating the NZ legislative framework into a unified structure.**

e. **That the Reviewers investigate the implications of developing a statutory Code of Practice for ensuring human rights compliance by intelligence and security agencies.**

f. **The Commission recommends that the Reviewers consider statutory mechanisms (such as a statutory Code of Practice) for requiring human rights training for intelligence and security officials**

g. **That that the Reviewers investigate current and potential measures which enable oversight mechanisms to assess intelligence and security practices against New Zealand's domestic and international human rights obligations.**

h. **That the Reviewers investigate the implications of consolidating current oversight roles and functions into an independent centralised judicial entity such as an Intelligence and Security Commission.**

20. The Commission's position is set out in more detail below under the following sections, based on the terms of reference of the Review:

- **Part A:** Concerning the adequacy of the current legislative framework to protect NZ's current and future national security, while protecting individual rights.

- **Part B:** Concerning the current oversight arrangements and whether these provide sufficient safeguards at an operational, judicial and

political level to ensure that NZSIS and GCSB act lawfully and maintain public confidence.

21. As regards the Review's matters of particular focus, the Commission has previously stated its position on the Countering Foreign Terrorist Fighters legislation sunset clause and the definition of "private communications" under the GCSB Act in its submissions on those pieces of legislation. These positions are referenced in the annexure to the submission. The Commission does not intend to expand on those positions further in this submission.

PART A: The legislative framework

22. The legislative framework governing New Zealand's intelligence and security sector is complex and spread over a number of relatively obscure legislative instruments. The statutory structures and terminology used are, for the most part, highly technical and lack unifying guidelines or a code of practice. As a result, the legislative framework is relatively impenetrable and inaccessible to members of the public.

23. This is perhaps reflective of the ad hoc way in which the legislature has responded to the intelligence and security sector's evolving policy and operational objectives over the years. While this is not unique to New Zealand, this is not a desirable situation. In his analysis of the UK legislative framework, Anderson notes:

"Obscure laws – and there are few more impenetrable than RIPA and its satellites [the UK equivalents] *corrode democracy because neither the public…nor the legislators…truly understand what they mean*."[17]

24. The Commission considers Anderson's five inter-related principles – minimising no-go areas, limiting powers, rights compliance, clarity and transparency and a unified approach - provide invaluable guidance when approaching the complex and competing sets of interests that must be taken into account when contemplating the design and utility of intelligence and security legislation.

[17] *A Question of Trust* p 253

Minimising no-go areas and limiting powers

25. Anderson characterises the above two principles as follows:

    - In order for a system to be trusted, it must be fair and effective. No-go areas should be minimised as much as possible, whether in the physical or digital world.

    - That intelligence and security powers are limited in the interests of privacy

26. The operation of intelligence and security legislation has inherent implications for the privacy of individuals. This, in turn, gives rise to democratic concerns. As the ISR has noted, the individual's right to privacy, while not an absolute right, is a pre-requisite in a functioning modern democracy and provides the basis for freedom, personal autonomy and personal expression[18].

27. While a free-standing right to privacy is not expressly contained in the New Zealand Bill of Rights Act 1990, the right is guaranteed under international human rights law by way of Article 17 of the ICCPR, which provides that:

    No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

    Everyone has the right to the protection of the law against such interference or attacks

28. Rapid advancements in electronic mass surveillance and data interception are highlighting the difficulties New Zealand's domestic human rights law has in responding to emerging challenges brought about by 21st century information technology. The absence in the New Zealand Bill of Rights Act of a right to privacy, analogous to that guaranteed under Article 17 of the ICCPR, inhibits the current statutory compliance and oversight provisions from taking into account the impact of intelligence and security powers on a

[18] *A Democratic License to Operate*, p 31, para 2.10,

person's right to privacy (see paragraph 49 below). While the Privacy Act 1993 regulates the collection and use of personal information, it is not underpinned (or empowered) by a presumptive statutory right to privacy.

29. Accordingly, the Commission would encourage the Reviewers to give some consideration to this issue. The Commission considers that the inclusion of a right to privacy in the NZBORA is entirely appropriate in the contemporary context and would render it more consistent with the objectives stated in its long title, which are:

    (a)to affirm, protect, and promote human rights and fundamental freedoms in New Zealand; and
    (b)to affirm New Zealand's commitment to the International Covenant on Civil and Political Rights

30. In its 2014 report to the UN General Assembly, *The Right to Privacy in the Digital Age*[19], the Office of the UN High Commissioner (OHCHR) has noted that any legal limitations to the right to privacy under Article 17 of the ICCPR must be:

    …sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances. The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available.[20]

31. The principles of necessity and proportionality are therefore crucial human rights concepts[21] when considering the powers and jurisdictional scope of our intelligence and securities agencies.

[19] Office of the High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, June 2014, A/HRC/27/37
[20] ibid para 23, p 8
[21] And are not only limited to the right to privacy under Article 17. For example, Article 12.3 of the ICCPR provides for a restriction on the right to freedom of movement on the grounds of national security; an issue of direct relevance to the amendments to the Passport Act 1992 made under the Countering Foreign Terrorist Fighters legislation. In its General Comment No 27 on the right to freedom of movement under Article 12, the UN Human Rights Committee has found that in order to comply with Art 12.3 any such restrictions must be necessary to protect their aim and adhere to the principle of proportionality. See CCPR/C/21/Rev 1/Add 9 paras 11-18

32. The OHCHR suggests that the onus is upon governments to demonstrate that powers that interfere with individual privacy are both necessary and proportionate to address the specific risk. Without these precepts, the activities of government intelligence agencies, such as mass surveillance programmes risk arbitrariness, even if they serve a legitimate aim and are vested under an accessible legal regime[22].

33. Further to this point, both the ISR Panel and Anderson reinforce "the articulation of enduring principles" as a key component of any intelligence and security regime. The ISR Panel goes on to recommend the development of statutory Codes of Practice, written in plain accessible language, that include details of the technical implementation and application of governing legislation[23].

34. The Commission endorses this approach. New Zealand's disparate legislative framework lacks a coherent set of principles that guide consistent practices or set appropriate parameters of implementation.

35. Rebecca Kitteridge indirectly identified this concern in her March 2013 report *Review of Compliance of the Government Communications Security Bureau*. Ms Kitteridge recommended the development of a "comprehensive compliance framework" for the GCSB. In coming to this recommendation, Ms Kitteridge observed:

    "I would argue that GCSB [is at the] *high-risk end of the compliance spectrum. Its powerful capabilities and intrusive statutory powers may only be utilised for certain purposes. The necessarily secret nature of its capabilities and activities prevents the sort of transparency that would usually apply to a public sector organisation. It is therefore imperative that the public be able to trust that those exercising the powers are doing so only in the way authorised by Parliament. A robust compliance regime, including visibly demanding*

[22] A/HRC/27/37 para 25, p 9
[23] *A Democratic License to Operate*, Recommendation 2

external reporting and oversight, should provide considerable assurance to the public." [24]

36. A statutory Code of Practice that applies across the intelligence and security sector has the potential to provide a stronger protective mechanism against intrusive practices or "jurisdiction creep" than a policy-level compliance framework.

37. In addition, the Commission agrees with Anderson's position that arbitrary distinctions should not be drawn between content data and communications data (meta-data). Instead, what is important is that such data may only be accessed pursuant to properly authorised requests, based on clear laws that are subject to independent judicial oversight.[25]

Rights compliance

38. In recent submissions, the Commission has identified a number of concerns about the potential impact on human rights of the recent tranche of reforms to New Zealand's intelligence and security laws[26].

39. The Commission has accordingly proposed that intelligence and security legislation includes both explicit reference to human rights principles and places an onus on officials to respect human rights in the course of implementing their statutory duties.[27]

40. This approach reflects international human rights standards articulated in a number of recent UN reports and General Assembly resolutions[28]. The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, for example, has proposed a number of practice standards that include:

[24] Rebecca Kitteridge, *Review of Compliance of the Government Communications Security Bureau* para 38, p 20, http://www.gcsb.govt.nz/assets/GCSB-Compliance-Review/Review-of-Compliance.pdf
[25] *A Question of Trust* para 13.12-13.14
[26] See Human Rights Commission, Reports and related materials on intelligence and security policy, 27 July 2015
[27] Human Rights Commission, Briefing to DPMC, para 2.4
[28] Such as General Assembly Resolution 68/178 on the Protection of human rights and fundamental freedoms while countering terrorism and Resolution 67/167 concerning.the right to privacy in the digital age

- That all intelligence services are constituted through publicly available laws that comply with international human rights law[29].
- That intelligence services are prohibited from undertaking any action that contravenes international human rights law[30].
- That intelligence services and their oversight institutions take steps to foster an institutional culture based on respect for human rights, including training members on the relevant provisions of international human rights law.[31]

41. Furthermore, the OHCHR has observed a disconnect between the "clear and universal" framework for the promotion and protection of privacy under international human rights law and the inadequacy of the legislative frameworks of many States in providing safeguards and accountability for privacy violations[32].

42. The OHCHR has also identified a "clear and pressing need for vigilance" in ensuring that surveillance policies and practices comply with international human rights law. Accordingly, the OHCHR has recommended that States review their national laws, policies and practices to ensure full conformity with international human rights law, and address any shortcomings through the adoption of a clear, precise, accessible, comprehensive and non-discriminatory legislative framework[33].

43. This Review provides an important opportunity for this type of human rights stock-take to take place. This should also include consideration of whether a specific statutory mechanism is required to ensure human rights compliant policy and practice. With this in mind, the Commission considers that a statutory Code of Practice could provide a basis for incorporating into legislation a set of human rights-complaint principles and related values that underpin national security policy and practice.

44. Further to this point, the UN Special Rapporteur Scheinin has observed that:

[29] A/HRC/14/46, Practice 4, p 7
[30] ibid, Practice 5
[31] A/HRC/14/46, ibid, Practice 19, p 17
[32] A/HRC/27/37, para 47
[33] ibid para 50

"…it is good practice for national security and its constituent values to be clearly defined in legislation adopted by parliament. This is important for ensuring that intelligence services confine their activities to helping safeguard values that are enshrined in a public definition of national security…In many areas, safeguarding national security necessarily includes the protection of the population and its human rights; indeed a number of States explicitly include the protection of human rights as one of the core functions of their intelligence services."[34]

Clarity and transparency

45. The recent reviews of the UK's intelligence and security apparatus have emphasised the importance of having a clear, consistent legislative framework that is coherent, transparent and accessible. As Anderson notes:

"The fact that the subject matter is technical is no excuse for obscurity. It should be possible to set out a series of limited powers, safeguards and review mechanisms with a high degree of clarity and… without technical jargon".[35]

46. Similarly, the ISR Panel lists "legislative clarity" as one of its ten tenets for testing legislation for intrusions against privacy, noting that while such legislation is not likely to be simple, it must be:

"clearly explained in Codes of Practice that have Parliamentary approval, are kept up-to-date and are accessible to citizens, the private sector, foreign governments and practitioners alike".[36]

47. UN reports also emphasise the importance of clear, accessible legislative language. UN Special Rapporteur Frank La Rue has recommended that legal frameworks governing communications surveillance measures meet *"a*

[34] A/HRC/14/46 p 5, 6 (such as Switzerland, Croatia and Brazil)
[35] *A Question of Trust*, para 13.33
[36] *A Democratic License to Operate*, p xiv

standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can forsee their application."[37]

48. The Commission is of the view that the statutory language in New Zealand's intelligence and security legislation is often less than clear or precise. In particular, the Commission has noted its concern that important terminology, such as the definition of "private communications" under s 4 of the GCSB Act, is vague and risks undermining reasonable expectations of privacy[38].

49. Another related example is the requirement under s 8D(1)(a) of the GCSB Act that the GCSB deliver its functions in a "human rights standards recognized by New Zealand law", which is ambiguous as to whether this includes ratified international human rights treaties. This is a crucial issue when considering the obligations that the GCSB has with regards to the right to privacy, a right that is guaranteed in international human rights law under Article 17 of the ICCPR, but conspicuously absent from the NZBORA.

A unified approach

50. Consideration could also be given to consolidation of the disparate collection of statutes that currently make up New Zealand's intelligence and security framework.

51. Anderson has notably recommended the consolidation of the UK's similarly disparate legislative framework into a single body of law with a single system of oversight that applies across the investigatory and intelligence agencies[39].

52. This approach has been largely endorsed by the other contemporaneous UK reviews. The ISR Panel, for example, has endorsed Anderson's conclusions and recommended the development of a comprehensive new law that consolidates existing statutes. The Intelligence and Security Committee of the UK Parliament also proposed, at an earlier stage, a similar unified approach.

---

[37] Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression Frank La Rue*, A/HRC/23/40, 17 April 2013, para 83, p 21

[38] Human Rights Commission, *Report to Prime Minister*, paras 27-28

[39] *A Question of Trust*, para 13.44

53. The Commission also endorses the consideration of a similar unified approach for New Zealand's legislative framework. An exhaustive, transparent, rights-compliant unified statutory regime of the kind envisaged by Anderson[40] would constitute a significant improvement on the structure and accessibility of the current regime and would adhere more closely to international human rights practice standards.[41]

PART A - RECOMMENDATIONS: The legislative framework

a. The Commission recommends that the Reviewers undertake a comprehensive review of New Zealand's intelligence and security legislation for consistency with international human rights law and norms.

b. The Commission recommends that the Reviewers consider ways in which the clarity, accessibility and structure of New Zealand's intelligence and security legislation can be improved.

c. The Commission recommends that the Reviewers consider the implications that inclusion of the right to privacy in the New Zealand Bill of Rights Act would have for intelligence and security law, policy and operations.

d. The Commission recommends that the Reviewers investigate the implications of consolidating the NZ legislative framework into a unified structure.

e. The Commission recommends that the Reviewers investigate the implications of developing a statutory Code of Practice for ensuring human rights compliance by intelligence and security agencies.

f. The Commission recommends that the Reviewers consider statutory mechanisms (such as a statutory Code of Practice) for requiring human rights training for intelligence and security officials.

[40] *A Question of Trust*, para 12.45
[41] A/HRC/14/46, p 6, Practice 2

Part B: Oversight mechanisms

54. Oversight mechanisms are crucial components of a human rights compliant intelligence and security system. They have a critical safeguarding role in ensuring that powers are applied lawfully and in conformity with the State's human rights obligations.

55. In most jurisdictions, oversight of the intelligence and security services is carried out in a multi-lateral way by a combination of institutions located within the executive, judicial and legislative branches of government. While there is no single model for intelligence oversight, effective systems will include the following features[42]:

    - Specialised oversight institutions with mandates and powers based on publicly available law.
    - At least one civilian institution that is independent of both the intelligence services and the executive.
    - A combined remit of oversight that covers all aspects of the work of intelligence agencies, including compliance with the law, including human rights, as well as administrative, financial and operative performance.
    - Power, resources and expertise to initiate and conduct investigations
    - Measures necessary to protect classified information and data accessed as a result of oversight work.

56. Among these functions, the independent scrutiny of compliance with laws and human rights obligations is a particularly important aspect of the intelligence and security system's public mandate. As UN Special Rapporteur Sheinin has noted[43]:

    Intelligence oversight institutions serve to foster public trust and confidence in the work of intelligence services by ensuring they perform their statutory functions in accordance with respect for the rule of law and human rights.

[42] A/HRC/14/46 , Practices 6-8 p 8-10
[43] ibid p 9

57. In New Zealand, these oversight institutions and their functions are spread over a number of statutes and are relatively disjointed, in reflection of the current nature of the legislative framework. The Inspector-General of Intelligence and Security primarily has the role of providing independent review of the compliance of intelligence and security agencies with their legal functions, and can receive complaints regarding individual cases. The Commissioner of Security Warrants, a retired High Court judge, is charged with authorising applications for warrants[44] under the New Zealand Security Intelligence Service Act 1969 and interception warrants (in conjunction with the Minister) under the GCSB Act[45]. Parliamentary oversight is provided by the Intelligence and Security Committee[46].

58. It is notable that none of these institutions are expressly required to have any consideration of New Zealand's international human rights obligations, which serves to highlight the absence of the ICCPR Article 17 right to privacy from the NZBORA. The Inspector-General, the oversight mechanism responsible for compliance, is not explicitly required to regularly review operational policy and practice against human rights obligations or consider human rights impact[47], although they may consult with a Human Rights Commissioner when carrying out any of their inquiry, complaint and review functions[48]. The Inspector-General is also required to review the 'legal compliance" of intelligence and securities agencies, however the statutory language indicates that this review function is limited to domestic law.[49]

59. Furthermore, the Inspector-General's complaints inquiry functions are reasonably limited. The Inspector-General does not appear to have any authority to inquire into complaints regarding groups of people or systemic practices (such as racial or ethnic profiling for example), nor do they have jurisdiction to issue remedies to individual complainants. Redress is limited to the issue of a report that is furnished to the Minister and the agency chief

[44] And providing authorisation for warrantless surveillance under s 41E(2)
[45] Section 15B
[46] The Commission supports the establishment of a Parliamentary Select Committee with cross-party political membership, see Human Rights Commission, Report to Prime Minister, p 13, para 55(a)
[47] Section 11(1) Inspector-General of Intelligence and Security Act
[48] Section 12 Inspector-General of Intelligence and Security Act
[49] Section 11(1) Inspector-General of Intelligence and Security Act

executive.[50] Complainants have no right of access to that report. Instead, the Inspector-General is merely obliged to notify the complainant of their conclusions in limited terms[51].

60. New Zealand's oversight mechanisms therefore have limitations when it comes to monitoring human rights compliance. The Commission has previously raised concern that the 2013 amendments did not establish an oversight regime sufficient to assure the public that appropriate scrutiny and supervision will occur.[52]

61. In the UK, the Anderson report has recommended the consolidation of three independent oversight entities into one centralized Commission, entitled the Independent Surveillance and Intelligence Commission (ISIC). The ISIC model proposed by Anderson merges a number of judicial and bureaucratic functions together under the same roof, including:

    - Warrant oversight and authorisation (to be undertaken by Judicial Commissioners)
    - Capacity to carry out own-motion inquiries
    - Review and monitoring
    - Audit and inspection of intelligence and security services

62. Anderson proposes that the strong, centralized ISIC model brings a number of advantages due to its greater size and unified nature. This includes having much broader monitoring and investigation capabilities and a greater public profile.[53]

63. The IRS Panel has similarly recommended that a consolidated approach is taken through the creation of a National Intelligence and Surveillance Office (NISO). However, unlike Anderson's proposal, the Judicial Commissioners who authorise and oversee that warrant process remain independent from the NISO[54].

[50] ibid s 25
[51] ibid
[52] Human Rights Commission, *Report to Prime Minister*, para 42, p 11
[53] *A Question of Trust*, para 14.97
[54] *A Democratic License to Operate*, Recommendations 17-19, p xviii

64. The ISR Panel notes that a clear oversight regime is an essential aspect of maintaining public trust and confidence in intelligence and security services. Complex, obscure legal frameworks and institutions do not tend to serve the public well as they are difficult for the public to identify and access.[55]

65. The Commission considers that the strong, centralised institutional models envisaged in the ISIC and NISO models ought to be considered for adaptation in New Zealand. The Commission considers that the current "sole office-holder" approach taken in New Zealand risks having insufficient capacity to undertake a suitably broad range of oversight functions[56].

66. New Zealand is a small country and lacks the necessary level of resources, infrastructure and service demand to justify an entity on the scale of Anderson's ISIC model. Our current oversight regime is far more minimal in terms of personnel and institutional scope than the UK's incumbent model. Notwithstanding these inherent limitations, the notion of an independent Intelligence and Security Commission consisting of judicial commissioners that places the current Inspector-General and Commissioner for Security Warrants functions under one roof has some merit.

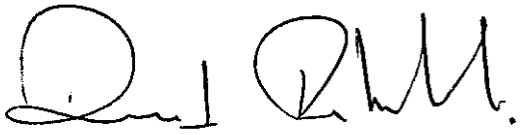
67. Such an approach may work to improve the institutional strength, scope and independence of New Zealand's oversight regime. This approach would also complement a more integrated or unified legislative framework and the development of a statutory Code of Practice.

Part B: RECOMMENDATIONS – Oversight mechanisms

g. The Commission recommends that the Reviewers investigate current and potential measures which enable oversight mechanisms to assess intelligence and security practices against New Zealand's domestic and international rights obligations.

[55] ibid para 4.42-4.43
[56] see also Human Rights Commission, *Report to Prime Minister*, p 7, para 29

h. The Reviewers investigate the implications of consolidating current oversight roles and functions into an independent centralised judicial entity such as an Intelligence and Security Commission



David Rutherford
Chief Commissioner

Contact Persons: John Hancock, Senior Legal and Policy Analyst
JohnH@hrc.co.nz

Janet Anderson-Bidois, Legal, Research and Monitoring Manager
JanetAB@hrc.co.nz

ANNEXURE: Human Rights Commission – Submission on the Independent Review of Intelligence and Security Services

Table: Comparison of recent reforms to legislative framework of intelligence and security services with domestic and international human rights obligations and principles

Legislation	Domestic human rights laws engaged	International human rights treaties engaged	UN Principles/commentary	Comments of HRC
Passports Act **Effect of reforms**:[1] Enables the Minister of Internal Affairs to cancel or refuse to issue a passport on grounds of national security if there are reasonable grounds to believe the person poses a danger to the security of another country	New Zealand Bill of Rights Act 1990 (NZBORA) Section 18(3) – right to freedom of movement Section 27 – right to natural justice (as regards ability to challenge Minister's decision)	International Covenant on Civil and Political Rights (ICCPR) Article 12.2 – freedom to leave any country including one's own Article 12.3 – no restriction on right to freedom of	UN Human Rights Council, 2010, A/HRC/16/51[2]: • Best practice in countering terrorism is ensuring that a person whose rights are breached in the exercise of counter-terrorism powers have access to an effective and enforceable remedy. UN General Assembly Resolution 68/178[3]:	The situation of NZ passport holders who have had their passports cancelled while out of NZ is not clear.[5] A solution may be establishing criteria for the provision of emergency travel documents.[6] Time limitations for lodging an appeal may create problems for persons out of the country to activate the appeal process.[7]

[1] Passport Amendment Act 2014 - enacted 12 December 2014 (by way of Countering Foreign Terrorist Fighters Bill 2014)
[2] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism:Ten areas of best practice in countering terrorism, see Practice 5, section D, paras 22-23
[3] A/RES/68/178, Protection of human rights and fundamental freedoms while countering terrorism
[5] Submission of HRC, Countering Foreign Terrorist Fighters Bill 2014, para 5.2
[6] ibid para 6.4
[7] Submission of HRC, Countering Foreign Terrorist Fighters Bill 2014, para 6.2(i)

		movement, unless necessary on grounds of national security Article 12.4 – no one shall be arbitrarily denied the right to enter their own country Article 2.3 – right to effective remedies determined by competent authorities	• Ensure access to a fair procedure for seeking full, effective and enforceable remedies within a reasonable time. • Ensure due process guarantees consistent with international human rights treaties and protocols. UNHRC General Comment No.27: Freedom of Movement (Article 12)[4] • Recognises States right to restrict the Article 12 right in exceptional circumstances, including protection of national security UNHRC General Comment No 29 on States of Emergency • Measures that derogate from ICCPR rights should be in place for a limited time and	The power of the SIS to suspend travel documents for up to 10 days without conclusive evidence of a terrorist risk, without any realistic avenue for redress or review poses natural justice problems.[8] Classified information may be withheld from the review/appeal process. Suggestion that consideration is given to establishing an independent review process to address this.[9] Sunset clause should set a shorter operative time period – 'the absolute minimum' to enable the review, civil society engagement and the drafting of new resulting legislation.[10]

[4] CCPR/C/Rev.1/Add.9, November 1999
[8] Ibid para 6.2(ii)
[9] Ibid para 6.5
[10] Submission of HRC, Countering Foreign Terrorist Fighters Bill 2014, paras 7.1-7.2

			only for the duration of the emergency.	
Government Communications Security Bureau Act 2003 **Effect of reforms[11]:** To update and broaden surveillance capabilities of GCSB, including enabling foreign intelligence agencies to access data on NZ citizens	NZBORA: Section 21 - Right to protection from unreasonable search and seizure NZBORA Long title (b) - An act to affirm NZ's commitments to ICCPR	ICCPR: Article 17[12] – regarding the right of the individual to protection from arbitrary or unlawful interference to their privacy Article 9.1- the right to liberty and security of the person	UN Human Rights Council, 2010, A/HRC/14/46[13] • **Practice 21. Intelligence collection** - National law should prescribe: the types of collection services available to intelligence services, the categories of persons and activities subject to collection, the threshold of suspicion for activating surveillance, limitations on the duration of surveillance procedures and procedures for authorising, overseeing and reviewing and surveillance and collection powers UN General Assembly Resolution on the Right to Privacy in the Digital Age.[14]	The definition of "private communications" under s4 is unacceptably vague and has the potential to undermine reasonable expectations of privacy[15]. Concern at the very broad statutory remit of the GCSB objectives under s7 and the wide range of activities that it may undertake in co-operation with SIS, Police and the Defence Force under s8C.[16] Concern at a weak level of oversight by the legislature compared with other nations.[17] Stronger accountability and oversight mechanisms are required; including establishment of a

[11] By way of Government Communications Security Bureau Amendment Act 2013
[12] See also Article 12 of the Universal Declaration of Human Rights
[13] Report of the Special Rapporteur Martin Scheinin on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures etc 17 May 2010
[14] A/RES/68/167, January 2014
[15] HRC, *Report to Prime Minister: Government Communications Security Bureau and Related Legislation Amendment Bill, and associated wider issues relating to surveillance and the human rights of people in New Zealand, 9 July 2013*, paras 27-28
[16] HRC Report to Prime Minister, July 2013. Paras 24-25

			• Calls on States, inter alia, to review their procedures, practices and legislation regarding surveillance of communications, interception and collection of personal data (including meta-data from mass surveillance) with a view to upholding the right to privacy by ensuring full compliance with international human rights law • Establish or maintain independent, effective domestic oversight mechanisms capable of ensuring transparency	Parliamentary Select Committee.[18] Concern at the use of urgency in passing important amendments to security legislation[19]. Recommends that officials working in intelligence services have human rights training.[20] Legislation should include explicit reference to human rights principles and obligations of officials to respect/consider/apply human rights principles when carrying out functions.[21]
Telecommunications	NZBORA:	ICCPR:	UN Human Rights Council, 2010,	Notes that many of the

[17] Ibid para 42
[18] Ibid para 55a
[19] Ibid paras 46-48
[20] Ibid 55d and see also HRC, *Protection of Fundamental Freedoms in the Digital Age*, Paper for UN High Commissioner for Human Rights, 20 June 2014 p 6-7
[21] HRC Briefing Paper relating to human rights and the targeted review of foreign terrorist fighters, for Andrew Kibblewhite, CE DPMC, 3 November 2014 para 2.4

(Interception Capability and Security) Act 2013 **Effect of reforms:** Places obligations on telecommunications network operators to assist government on network security matters which raise a risk to NZ's security or economic wellbeing. Also prescribes the use of classified security information obtained by interception in court proceedings	Section 13 – the right to freedom of thought, conscience, religion without interference Section 14 – the right to freedom of expression Section 21 - Right to protection from unreasonable search and seizure Section 27(1) – right to the observance of natural justice by any tribunal or public authority Section 27(3) – the right to defend and be heard in civil	Article 17[22] – regarding the right of the individual to protection from arbitrary or unlawful interference to their privacy Article 14.1 All persons shall be equal before the court and tribunals	A/HRC/14/46 • **Practice 26**: Individuals have the right to request access of their personal data held by an intelligence agency, either through a relevant authority or by way of an independent institution. UN Human Rights Council 2013 A/HRC/23/40[23] • While use of communications technologies to address national security concerns and criminal activity may justify their use in exceptional circumstances, the potential interference with the rights to privacy and freedom of opinion/expression poses a risk to democratic foundations.	provisions are unclear and capable of broad interpretation .[24] Notes a wide Ministerial discretion under the Act (s38) to require, upon application of surveillance agencies, service operators to have the same interception capabilities as network providers.[25] Notes concern at the provisions contained in subpart 8 of the Act regarding use of classified security information in court proceedings. In particular, the restrictions on disclosure of that information to the suspect; and the court's ability to proceed to hearing in the absence of the suspect notwithstanding the power of the court to appoint a Special Advocate.[26]

[22] See also Article 12 of the Universal Declaration of Human Rights
[23] Report of Special Rapporteur, Frank La Rue, on the promotion and protection of the right to freedom of opinion and expression
[24] HRC, *Report to Prime Minister*, July 2013, para 32
[25] HRC, *Report to Prime Minister*, July 2013, para 32
[26] Ibid para 33

	proceedings brought by the Crown			
Inspector–General of Intelligence and Security Act 1996 **Effect of Reforms:**[27] Establishes Inspector-General of Intelligence and Security with a view to increasing level of independent oversight of NZ's intelligence and security services.	NZBORA: Does not directly engage NZBORA, but I-Gs functions include[28] inquiring into any complaint by a NZ citizen or intelligence official about any action, omission or practice by intel/security agencies that adversely affects a NZ person Includes discretion to consult with Human Rights Commissioner in exercise of s11 functions[29]	ICCPR: Article 2.3(a) – Places an obligation on the State to access an effective remedy in cases where their human rights and freedoms have been breached Article 2.3(b-c) – obligation to establish competent authorities to hear and determine such complaints and grant and enforce remedies	UN Human Rights Council, 2010, A/HRC/16/51 **Practice 6**: An effective system of oversight includes at least one civilian institution that is independent of the executive and the intelligence services. **Practice 7:** Oversight institutions have the power to initiate their own investigations **Practice 8**: Avenues to redress individual complaints are established. **Practice 9:** Recourse to effective remedies are provided, including reparation for harm caused.	The functions of the Inspector-General when carrying out a s11(d) review does not explicitly require assessment of operational policy, and practice against international human rights obligations or the human rights impact (instead referring to "legal compliance generally") Complaints inquiry function under s 11 is limited to complaints regarding a New Zealand person; there does not appear to be scope to inquire into complaints regarding groups of people or systematic practices The Inspector-General has no jurisdiction to issue remedies to individual complainants – redress is limited to the issue of a section 25 report

[27] By way of Inspector–General of Intelligence and Security Amendment Act 2013
[28] Section 11 Inspector–General of Intelligence and Security Act
[29] Ibid, Section 12

New Zealand Security Intelligence Act 1969 **Effect of Reform**[30] Amends s41 provision of the Act regarding visual surveillance warrants – in particular s 41D enables the Director to authorize 24 hour warrantless visual surveillance and/or intelligence interceptions, seizures of communications and electronic tracking, necessary for the detection, investigation of any actual, potential or suspected terrorist act or facilitation of a terrorist act	NZBORA: Section 21 - Right to protection from unreasonable search and seizure	Article 17[31] – regarding the right of the individual to protection from arbitrary or unlawful interference to their privacy Article 9.1- the right to liberty and security of the person	UN Human Rights Council, 2010, A/HRC/14/46 • Practice 22 – Intelligence collection measures that impose significant limitations on human rights are subject to a multi-level process of authorization that includes approval by the political executive and an institution independent of the intelligence services and the executive.	The s41D powers to proceed with warrantless surveillance and intelligence powers require the Minister, the Commissioner of Security Warrants and the Inspector-General to be notified. However, the s41D(1) process does not require any authorization by the Inspector-General. The Minister and the Commissioner of Security Warrants may direct the warrantless surveillance or intelligence processes to be discontinued and any material destroyed. After the expiry of a 24hour warrantless surveillance period any information obtained relevant to activities prejudicial to security (both nationally and relevant to the gathering of foreign intelligence) may be retained. All other information must be destroyed, unless a

[30] By way of New Zealand Security Intelligence Amendment Act 2014
[31] See also Article 12 of the Universal Declaration of Human Rights

				warrant has been duly obtained after the expiry of the 24 hour period.
Intelligence Security and Committee Act 1996 **Effect of Reform[32]:** To introduce period reviews of the intelligence and security services; and to establish a procedure for chairing Committee reviews of intelligence services to address potential conflict of interest in the event the PM is the responsible Minister.			UN Human Rights Council, 2010, A/HRC/14/46 • **Practice 6** – oversight of intelligence services includes parliamentary oversight, in combination with other oversight mechanism	Supports (and has recommended) full independent inquiry of NZ's intelligence and security services.[33] Supports establishment of enhanced Parliamentary oversight, preferably through the establishment of a Parliamentary Select Committee[34]. Terms of reference of inquiry should include reference to relevant human rights obligations and principles.[35]

[32] By way of Intelligence Security and Committee Amendment Act 2013
[33] HRC, *Report to Prime Minister*, July 2013, para 54
[34] Ibid para 55a
[35] HRC, *Protection of Fundamental Freedoms in the Digital Age*, Paper for UN High Commissioner for Human Rights, 20 June 2014 p 11