NEW ZEALAND COUNCIL OF TRADE UNIONS
Te Kauae Kaimahi

Submission of the New Zealand Council of Trade Unions Te Kauae Kaimahi

to the

Foreign Affairs, Defence and Trade Committee

on the

New Zealand Intelligence and Security Bill

P O Box 6645
Wellington
October 2016

Table of Contents

1. Introduction

1.1. This submission is made on behalf of the 31 unions affiliated to the New Zealand Council of Trade Unions Te Kauae Kaimahi (CTU). With 320,000 members, the CTU is one of the largest democratic organisations in New Zealand.

1.2. The CTU acknowledges Te Tiriti o Waitangi as the founding document of Aotearoa New Zealand and formally acknowledges this through Te Rūnanga o Ngā Kaimahi Māori o Aotearoa (Te Rūnanga) the Māori arm of Te Kauae Kaimahi (CTU) which represents approximately 60,000 Māori workers.

1.3. The CTU and the New Zealand union movement have a strong interest in the activities of the intelligence agencies due to the chequered and inglorious history of the New Zealand Security Intelligence Service ('the SIS') particularly as it relates to union and progressive groups.

1.4. Nicky Hager gave a useful short history of the SIS in a public lecture in 2011.[1] He notes that:

> The SIS was established in 1956, the midst of the early Cold War, at the instigation and with the assistance of the British intelligence services…
>
> [Other than monitoring communist countries, the] SIS's other main target was local communist and socialist groups, as part of world-wide monitoring of these groups by their US and British allies. This spying was done under the security category of 'subversion'. Although, of course, New Zealand has no history of people trying to overthrow the government by force, but subversion was used as the pretext for spying on all sorts of progressive groups: unions, students, iwi, the nuclear free and environment movements and so on. The SIS has released some of the personal files it kept on progressive people during this era and they reveal an astonishing scale of intrusive and completely unnecessary surveillance. …
>
> In many ways this was just silly and irrelevant to New Zealand. But there was harm caused to the individuals and groups targeted. Some people's careers were unfairly and seriously harmed; and many people had fear about their groups being infiltrated and monitored (fears which were often correct). It had a negative effect on all sorts of political activity. One very large SIS case was that against the well-known New Zealander Bill Sutch: senior public servant, author, public intellectual. At 8.40pm on 26 September 1974 he was arrested near the top of Aro Street in Wellington (the remains of a concrete public toilet mark the spot, near the corner of Holloway Road). The SIS accused him of passing information to a Soviet embassy officer. It appears that Sutch had met with a Soviet embassy person. But he was very far from being a traitor. He was one of the great New Zealanders of his time, but of intense interest to the SIS because of his left-wing beliefs. There was a five-day trial, where he was acquitted, but the stress was so great that he had died within a year of the arrest.
>
> It is important to note that a lot of the SIS monitoring of progressive groups and people stopped at the end of the Cold War. Today a lot of people still fear they might be monitored by the SIS but, as far as I know, relatively little of the subversion monitoring continues. This is unnecessary fear, which needlessly chills political activity, so it is worth people knowing that it is mostly in the past (although police intelligence monitoring of political groups in New Zealand continues).

1.5. Many unions and progressive groups had embedded spies and informants watching and reporting on their activities. This certainly included the CTU and its predecessor organisations. Many unionists, including current CTU staff members and their families, were subject to intrusive surveillance.[2]

1.6. The SIS's history of suppressing political activism and dissent along with the attendant enormous waste of public monies chasing 'reds under the bed' does not instil confidence.

1.7. Since the end of the Cold War, the SIS has embarked on further misadventures such as the monitoring of sitting Member of Parliament, Keith Locke, their involvement in the legally-dubious Operation Eight and the persecution of Ahmed Zaoui that lead us to doubt whether they have justified the enormous public trust placed in them.

---

[1] Nicky Hager (2011) A short history of the New Zealand Security Intelligence Service (NZSIS) available at http://www.nickyhager.info/a-short-history-of-the-new-zealand-security-intelligence-service-nzsis/

[2] An article that sets out the scope (and at times tragicomic nature) of this surveillance is Murray Horton (1999) SIS spied on CAFCA for quarter of a century. Foreign Control Watchdog 20(6). Retrieved from: http://www.converge.org.nz/watchdog/20/06.htm

1.8. The Government Communication Security Bureau ('the GCSB') has also failed to cover itself in glory through unlawful surveillance of Kim Dotcom and their participation in other morally dubious activities such as the alleged surveillance of the Leaders of Pacific Nations and other countries in support of the Hon Tim Groser's failed bid to head the World Trade Organisation. This is compounded by the exposure of the massive surveillance programme undertaken by the Five Eyes Alliance.

1.9. The activities of the intelligence agencies require the utmost public trust that the agencies will act in the public good. As Rebecca Kitteridge noted in her 2013 *Review of Compliance of the Government Communications Security Bureau* at [38]:

> [The GCSB's] 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 external reporting and oversight, should provide considerable assurance to the public.

1.10. The history of these agencies (almost from inception) does little to instil that trust. While we recognise that the framework in which these agencies operate precludes them from advertising their successes, the agencies have a mountain to climb in terms of building their credibility and moral mandate for the intrusive actions they undertake.

1.11. We acknowledge efforts of Ms Kitteridge, the Inspectors-General of Intelligence and Security and the authors of the first Independent Review of Intelligence and Security in New Zealand ('the Independent Review') to provide more robust scrutiny of our intelligence services. Their efforts are welcome.

1.12. The CTU supports the aspects of the Intelligence and Security Bill ('the Bill') which provide greater transparency and clarity to the operation of the SIS and GCSB. The Bill also provides an opportunity to clear up some longstanding issues of ambiguity in the application of the predecessor legislation.

1.13. However, the rather dismal legacy of these agencies means we do not support expansion of their powers without a very compelling case to do so. This case has not been made out by the Government.

1.14. Our submission begins with a general discussion of the human right to privacy at international law followed by a comment on the generally applicability of these rights

(including to New Zealand's actions overseas and to persons who are not New Zealand citizens or residents). We then move to the provisions of the Bill itself.

2. The right to privacy

2.1. The right to privacy is one of the most fundamental human rights. As Thomas J commented in *Brooker v Police* [2007] 3 NZLR 91 at [182]:

> Probably [no human right] is more basic to human dignity than privacy. It is within a person's sphere of privacy that the person nurtures his or her autonomy and shapes his or her individual identity. The nexus between human dignity and privacy is particularly close

2.2. The importance of privacy is well-recognised in the corpus of international human rights but poorly in our domestic laws. Article 12 of the Universal Declaration of Human Rights ('the UDHR'') states that:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

2.3. As a declaration, the UDHR is not binding on member states of the United Nations. Binding obligations come from the International Covenant on Civil and Political Rights ('ICPPR') and the International Covenant on Economic, Social and Cultural Rights ('ICESCR'). The UDHR, ICCPR and ICESCR together make up what is sometimes called the International Bill of Rights.

2.4. New Zealand played a strong role in the development of both ICCPR and ICESCR. We also ratified both Covenants in 1978.

2.5. Article 2 of ICCPR requires that:

> 1. Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.
>
> 2. Where not already provided for by existing legislative or other measures, each State Party to the present Covenant undertakes to take the necessary steps, in accordance with its constitutional processes and with the provisions of the present Covenant, to adopt such laws or other measures as may be necessary to give effect to the rights recognized in the present Covenant.

2.6. Article 17 of ICCPR mirrors the language of art 12 of the UDHR:

> 1. 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.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

2.7. Despite express reference to compliance with the ICCPR in its long title, the New Zealand Bill of Rights Act 1990 does not contain a standalone right to privacy. The Human Rights Commission comments in its submission to the Independent Review at [28] and [29] that:

> 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 person's right to privacy.… The Commission considers that the inclusion of a right to privacy in the NZBORA is entirely appropriate in the contemporary context.

2.8. We agree. *We recommend that the New Zealand Bill of Rights Act 1990 is amended to recognise a right to privacy.*

2.9. Failure to expressly include the right to privacy in the New Zealand Bill of Rights Act 1990 does not render the right to privacy nugatory however. Section 28 of that Act states that:

> An existing right or freedom shall not be held to be abrogated or restricted by reason only that the right or freedom is not included in this Bill of Rights or is included only in part.

2.10. The right to privacy must therefore be protected and not abrogated by the Bill or the exercise of State power. We consider that while the Bill is a step in the right direction it does not adequately respect the right to privacy.

3. The general applicability of human rights

3.1. The Electronic Frontier Foundation and Article 19 have published an excellent legal research brief in 2014 entitled 'Background and supporting international legal analysis for the international principles on the application of human rights to communications surveillance' ('the EFF brief').[3] With regard to the differential treatment of the citizens of other countries the EFF brief notes at 22 that:

> [T]he domestic legal framework of most countries typically gives much greater protection to the privacy rights of citizens as opposed to non-citizens and non-residents. As a result, many governments routinely engage in bulk surveillance of international communications with very little regard for the privacy of those communications, possibly in the mistaken belief that their legal obligations only extend as far as their own citizens or residents. Even more problematically, it appears that countries seek intelligence-sharing arrangements with other countries in order to obtain surveillance material concerning their own citizens that they could not obtain under their domestic legal framework.

[3] The EFF legal brief is well worth reviewing and available here: https://necessaryandproportionate.org/files/2016/03/29/background_and_supporting_legal_analysis_en.pdf

> However …the enjoyment of fundamental rights is not limited to citizens of particular states but includes all individuals, regardless of nationality or statelessness, such as asylum seekers, refugees, migrant workers, and other persons who may find themselves in a territory or subject to the jurisdiction of a State. In addition, all persons are also equal before the law and consequently, they are entitled, without discrimination, to equal protection of the law.

3.2. The EFF brief provides substantial international jurisprudence backing up this point. New Zealand cannot and should not draw a sharp line between the protections available to New Zealand citizens, residents and persons within our territorial boundaries and lesser or no protections available to others.

3.3. This is one of the most fundamental problems with New Zealand's intelligence-gathering framework. We recommend that the Committee seeks a specific briefing on New Zealand's international legal obligations regarding privacy, freedom of expression, freedom of association and other rights.

3.4. *We submit that the distinctions that the Bill draws between territorial and extra-territorial powers and that between New Zealand citizens and residents versus other persons are not justified in international law and must be removed*. New Zealand should behave in a rights-consistent manner regardless of the persons involved or their location.

3.5. This requires a reconsideration of the distinction in the Bill between New Zealand persons and foreign persons and organisations such as the lower thresholds for intelligence warrants relating to foreign persons (type 2 as opposed to type 1 for New Zealand citizens and permanent residents) and the restriction on who can complain to the Inspector-General. It also requires the removal of different standards of conduct for the intelligence and security agencies depending on the location of intelligence gathering or activities of interest (such as the safe harbour protection for lawful advocacy, protest or dissent in cl 22 only applying to those activities in New Zealand).

4. The purpose of the Bill (cl 3) and the objectives of intelligence and security agencies (cl 11)

4.1. In general, we support the purpose section of the Bill. In particular, we support the protection of New Zealand as a free, open and democratic society.

4.2. We strongly oppose the wording of cl 3(a) regarding "establishing intelligence and security agencies that will effectively contribute to… the international relations and well-being of New Zealand; and… the economic well-being of New Zealand."

4.3. The terms “international relations and well-being of New Zealand” and “economic well-being of New Zealand” together constitute such a broad and inchoate mandate as to be nearly meaningless.

4.4. This wording is based on the objective of the GCSB in s 7 of the Government Communication and Security Bureau Act 2003. This formulation came under significant criticism by submitters on the Government Communication Security Bureau and Related Legislation Amendment Bill 2013. Officials’ response in the Departmental Report on that Bill was that:

> All three matters [national security, international relations and economic wellbeing] that are listed need to be specified as the intelligence gathered by the Bureau is used to inform decisions-makers who are responsible for those matters. Intelligence about trade is important to our trade policies and matters relevant to international relations contribute to diplomatic engagements with other nations. Intelligence contributes to these activities and helps those responsible for those matters discharge their functions more effectively.

4.5. This fails to balance the basic rights of all people (including non-New Zealand citizens) to privacy, freedom of expression, freedom of association and so on with the convenience of New Zealand’s trade emissaries and diplomats. The convenience of our foreign affairs corps should not outweigh basic human rights except where clearly defined national security interests are under threat. Potentially serious damage to New Zealand’s economic security or international relations are covered within the definition of national security in cl 5(d).

4.6. This comment applies to the identical framing used in the principal objectives of the intelligence and security agencies in cl 11.

4.7. *We submit that cl 3(a)(ii)-(iii) and cl 11(b)- (c) should be deleted.*

4.8. The second problem with cl 3 is the ambiguity of cl 3(c)(i) “ensuring that the functions of the intelligence and security agencies are performed… in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.”

4.9. The ambiguity here is what is meant by “New Zealand law.” We discuss the problem of the ‘missing’ right to privacy in the New Zealand Bill of Rights Act 1990 in part two of our submission above. If the intelligence and security agencies look solely to the statute books, they will mislead themselves as to the scope of their obligations.

4.10. Our courts take a different approach to New Zealand’s international obligations than a simple scan of the statute books. As Richardson P observed in *Tranz Rail Ltd v Rail & Maritime Transport Union (Inc)* [1999] 1 ERNZ 460 (CA) at [40].

> The well settled approach of the Courts of New Zealand [is that [s]ubject to any New Zealand legislation and consideration of any special local circumstances, the Courts of New Zealand will always seek to develop and interpret our laws in accordance with generally accepted international rules and to accord with New Zealand's international obligations.'

4.11. New Zealand has entered into binding international obligations (including the right to privacy) and the Courts will read legislation consistent with these rights (the so-called presumption of consistency). The Bill should reflect this approach and also honour our binding commitments.

4.12. *We submit that greater clarity will be achieved by amending s 3(c)(i) to state "in accordance with New Zealand law and New Zealand's human rights obligations".*

5. The meaning of national security (cl 5)

5.1. *We support the introduction of a legislative definition of national security.*

5.2. The potential for confusion and abuse generated by leaving this term undefined was one of our key submissions on the Government Communication Security Bureau and Related Legislation Amendment Bill 2013. Bringing exactly what is meant by national security into the light is an important step.

5.3. The UN Special Rapporteur on Freedom of Expression, Frank LaRue, has expressed concern that "vague and unspecified" notions of "national security" had been unduly used to justify interception and access to communications without adequate safeguards.[4] He noted that:

> The use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern. The concept is broadly defined and is thus vulnerable to manipulation by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists, or activists. It also acts to warrant often-unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability.

5.4. So the introduction of a definition of national security is a very good idea. However, the balance has not been struck as well as it should be. We have three issues with the proposed definition in cl 5.

5.5. First, a "potential threat" is tautological and worryingly broad. A threat is defined by the Oxford Dictionary of English (2 Ed) as "a person or thing likely to cause damage or danger." The same dictionary defines potential as "having or showing the capacity to develop into something in the future."

[4] A/HRC/23/40, report of 17 April 2013, at para. 58, available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

5.6. "Threat" already contains the concept of likelihood of occurrence and adding "potential" simply makes the necessary likelihood considerably lower. Combining the two definitions together, a potential threat is "a person or thing with the capacity to become likely to cause damage or danger in the future." This is an extraordinarily wide definition that, again, acts as nearly *a carte blanche* for action by the intelligence services.

5.7. *We submit that it would be clearer, more practical and consistent with a rights-based approach to remove "potential threats" and only refer to "threats" in the definition of national security.*

5.8. Second, the term "serious harm… to the quality of life of the New Zealand population" in cl 5(c) is too vague and subjective. Terms like "quality of life" are frequently the subject of political debate and there are valid disputes as to what it means. For example many would have the view that the growth of a wealthy elite threatens our quality of life because of their ability to excessively influence the democratic process and the media, while others would claim that such a group demonstrates that people are rewarded for effort, skill or innovation and that that is essential to our quality of life. The security agencies should not take a position in such debates, but history shows (as outlined above) that they have a strong proclivity to do so. The bounds of the definition need to be clear and sufficiently defined to allow the intelligence agencies (and others) to rule threats in or out.

5.9. *Officials should be asked to state what threats may fall under this part of the definition which would not otherwise be captured by other limbs of the test. If they can provide valid examples then these should be more tightly captured.*

5.10. Third, the definition of "threats, or potential threats, to international security" in cl 5(g) is broad and ambiguous. It allows a wide latitude to intelligence agencies to justify interception without even the weak safeguards applied to the other limbs of the test.

5.11. The inclusion of "international security" in the concept of national security is conceptually incoherent. It is difficult to see how threats or potential to international security are threats to national security (sufficient to justify inclusion in its definition) unless they also pose a threat to New Zealand's interests sufficient to engage one of the other limbs of the test of "national security."

5.12. The concept of "threats or potential threats to international security" is unclear and problematic. Are security threats to one other country "international security threats?"

Two or more countries? To any countries or just ones deemed by some process to be friendly or important to New Zealand (in which case, what is that process)? Threats to international organisations such as the United Nations? More clarity is needed.

5.13. What is the threshold for determining when a threat or potential threat warrants the involvement of a New Zealand intelligence agency? There is not specification of what sort of threats might engage this definition (and with it permission to spy on New Zealanders if necessary). This is not good enough.

5.14. *Clause 5(g) should be deleted. If the intelligence agencies are to have a function of protecting international security then this term should be defined and properly bounded in the legislation (and the case for spying on New Zealanders will be weaker). The definition of international security could logically also include the protection of other countries from New Zealanders (under cl 5(f))*.

6. Bringing the SIS into the State sector framework (cl 9)

6.1. *We strongly support the move to make the SIS a department of the State and to extend the provisions of the Employment Relations Act 2000 regarding freedom of association and collective bargaining to the SIS.*

6.2. The Government has committed to the promotion of collective bargaining through several international treaties, including most notably International Labour Organisation Convention 98 on the Right to Organise and Collective bargaining. Art 4 of C98 states that:

> Measures appropriate to national conditions shall be taken, where necessary, to encourage and promote the full development and utilisation of machinery for voluntary negotiation between employers or employers' organisations and workers' organisations, with a view to the regulation of terms and conditions of employment by means of collective agreements.

6.3. The mainstreaming of the SIS's employment relationships is a welcome recognition of the human rights of SIS employees. As the Regulatory Impact Statement: New Zealand Intelligence and Security Bill (5 April 2016) notes at [56] the GCSB is already unionised and "there is no compelling reason why this cannot also be the case for the SIS." We agree.

7. The principles underpinning the performance of the agencies' functions (cl 12)

7.1. We support the intention of cl 12(1) that an intelligence and security agency must act in accordance with the law, New Zealand's human rights obligations, independently, impartially, with integrity, professionalism and democratic oversight.

7.2. Our comment regarding the problem with the framing of "all human rights obligations recognised by New Zealand law" under cl 3 applies with equal force here. We recommend the same change to the wording.

7.3. *We submit that greater clarity will be achieved by amending cl 12(1)(a) to state "in accordance with New Zealand law and New Zealand's human rights obligations."*

7.4. The good words of cl 12(1) are almost immediately undone by cl 12(2) however which states that "subsection (1) does not impose particular duties on" an intelligence and security agency, its Director-General or employees.

7.5. This may be unintentionally ambiguous drafting but we would suggest that cl 12(1) should absolutely impose a number of particular duties on the agencies, their directors and employees. They should have to follow the law and due process, observe human rights and follow any applicable codes of conduct or other requirements placed on public servants and institutions. Subclause 12(2) continues to give the unfortunate impression that the intelligence agencies are above the law.

7.6. *We recommend that cl 12(2) is deleted from the Bill.*

8. Limitation on collecting intelligence within New Zealand (cl 22)

8.1. Clause 22 is supposed to provide a modicum of comfort for advocacy organisations (including unions) that taking a position counter to Government policy is not, in itself, sufficient grounds for being subject to intelligence gathering by the intelligence and security agencies.

8.2. The predecessor of this clause is the almost identically worded s 2(2) of the New Zealand Security Intelligence Service Act 1969 which was added to that Act in 1999 as late recognition of the massive overreaches of the "subversion" surveillance during the Cold War.

8.3. Along with the guarantees of political neutrality in cl 21 this constitutes an important safeguard against the intelligence agencies targeting lawful opponents of the Government.

8.4. *We support the extension of this protection to the work of the GCSB along with the SIS.*

8.5. However, the protections in cl 22 are less substantial than they appear and should be strengthened. Clause 22 does not place positive obligations on intelligence and security agencies to embed proper safeguards against the targeting of dissent.

8.6. *We recommend the addition of a new cl 22(3) based on cl 21 stating:*

> *The Director-General of an intelligence and security agency must take all reasonable steps to ensure that the agency does not take any action for the purpose of suppressing or harming persons who are engaging in lawful advocacy, protest or dissent in relation to any matter.*

8.7. The limitation in cl 22(2) applies only to information "on any person who is in New Zealand or any class of persons who are in New Zealand." As discussed in part 3 of our submission above, this raises a troubling question as to whether our intelligence and security agencies are collecting information about person involved in advocacy, protest or dissent activities in other countries. Our intelligence and security agencies should not be spying on those exercising rights to lawful advocacy, protest or dissent anywhere in the world. These are core freedom of expression rights. *Geographic constraints on this protection should be removed.*

8.8. The rights to lawful advocacy, protest and dissent are distinct from one another. However, this clause of the Bill and its predecessor section in the New Zealand Security Intelligence Service Act 1969 refers these rights as "the right." This should be fixed.

8.9. *We recommend that clause 22(2) is reworded to state:*

> *The exercise of the rights in subsection (1) do not, of themselves, justify an intelligence or security agency collecting intelligence on any person.*

9. Authorisations (part 4)

9.1. We support the introduction of a more robust warranting system for the intelligence agencies. However, the proposals in the Bill are not sufficiently robust, clear or protective of human rights.

9.2. First, as we note in section 4 above, international human rights law does not permit the distinction drawn between greater protections afforded to New Zealand citizens and residents (Type 1 warrants) against lesser protections for other persons (Type 2 warrants).

9.3. *We submit that all unlawful activities should be subject to the same warranting process. This process should be the Type 1 warranting process but subject to the changes we propose below.*

9.4. Second, we do not accept that the case has been made by the Independent Review or any other publically available document for the extension of visual surveillance. By its nature, visual surveillance is one of the most intrusive types and is likely to involve intrusion into the privacy of others apart from the target.

9.5. The intelligence and security agencies have a long road to build public trust (accepting that their activities were largely directed by their political masters at the time). Until that public trust is built, the intelligence and security agencies should not be given additional scope to gather intelligence.

9.6. *We submit that the SIS should not be given the power to install visual surveillance devices (under cl 65(1)(b)(i)). If the GCSB is using existing equipment such as cameras on computers or cellular phones to conduct visual surveillance this should also be prohibited.*

9.7. Third, the protections for privileged communications under cl 67 are too weak. These cover only the carrying out of any activity or the exercise of any power **for the purpose** of obtaining privileged communications of New Zealanders. *As we have noted above in part 3 of our submission above, these protections should apply to any person.* Failure to protect legal professional privilege may violate basic human rights to a fair trial in other jurisdictions.

9.8. Also, restricting the issuance of an intelligence warrant to activities with the purpose of obtaining privileged communications is too narrow. There is a real risk of collecting such information incidentally. *Privileged communications should specifically be included in the definition of "unauthorised intelligence" in cl 83 and subject to the same rules.*

9.9. Fourth, the Bill is silent on requirements for the intelligence and security agencies to only hold information gathered (under warrant and where this information is publically

available) for as long as necessary for the purposes gathered (Information Privacy Principle 9). Because of the nature of the information held by the intelligence and security agencies it is difficult to prescribe an exact timeframe for destruction and disposal of information records but due to the often extremely-sensitive nature of the information, this principle is paramount.

9.10. This applies particularly to incidentally obtained information (cl 91) where it appears that the presumption is that the intelligence and security agencies may retain this information in case it becomes necessary. This is not good enough.

9.11. *We recommend that Part 4 should include a general requirement that, in accordance with Privacy Principle 9, the intelligence and security agencies must destroy information held when it is no longer necessary to hold that information. Failure to destroy such information should be subject to the penalties in cl 84.*

10. Oversight of intelligence and security agencies (Part 6)

10.1. We appreciate the greater scrutiny that the intelligence agencies have faced in the past three years. Given the evidence of previous overreach and the resulting gulf in public trust in the agencies however, more must be done.

10.2. Given the secrecy in which the intelligence and security agencies operate, Parliament is the most important democratic bulwarks against overreach by the intelligence agencies. It is disappointing therefore that the Bill rejects recommendations by the Independent Review with regard to the operation of the Intelligence and Security Committee including that that the Committee should elect its own chairperson.

10.3. We note comments by the Hon Phil Goff MP in the debate on the Government Communications Security Bureau and Related Legislation Amendment Bill. And the comments of Phil Goff: [5]

> You also need changes to be made to the Intelligence and Security Committee. I served on that committee for 3 years. It is a farce. It does not do the job, because John Key does not let it do the job. It hardly ever meets, it does not get briefed properly, and it does not give anywhere near adequate reports to this House. It is an absolute conflict of interest that the Minister in charge of the Security Intelligence Service should be the chair of the committee having oversight into the Intelligence and Security Committee. He is the person who should be held to account. This bill says: "Oh, put the Deputy Prime Minister in or the Attorney-General." That is not good enough. Maybe we should look at the Regulations Review Committee and, like that committee, have an Opposition member chairing the committee.

[5] (8 May 2013) 689 NZPD 9657

10.4. Official's justification for keeping the Prime Minister or his or her nominee in charge of the Committee are very weak. All they can muster (at [159] of the Regulatory Impact Statement) is "The Prime Minister has traditionally held a role leading the national security system." This conflict of interest with the oversight of the system is exactly why the Prime Minister (or whichever Minister is in charge of the intelligence agencies) should not chair the Intelligence and Security Committee.

10.5. *We recommend that the Bill is amended to ensure that the committee is not chaired by the Minister in charge of either of the intelligence agencies.*

11. Ministerial policy statements (cls 165-174) including regarding covert activities and co-operation with overseas public authorities

11.1. The Independent Review recommended an expansion and consolidation of the arrangements relating to the creation of false identities and cover arrangements. The Bill sets these out in Part 3.

11.2. We are concerned at the expansion of these powers (including to the GCSB) without adequate safeguards. As Gordon Campbell comments:[6]

> As for SIS and GCSB operatives, the way will be clear for them to seek and obtain fake birth certificates, IDs, utility bills, driving licences and passports, and to seek the collusion of ordinary citizens in obtaining such documentation. In Britain, similar latitude in this area has resulted in the use of the identities of dead children by Police. It has also seen undercover operatives enter into sexual relationships and even start families under fake identities. (Can sex be truly consensual when it is with someone whose allegiances are really the reverse of what they are claiming them to be?) Will NZ spies be now similarly "exempt from civil and criminal proceedings" as a result of being a party to such deceptions?
>
> In Britain, some of the Police undercover units – such as the Special Demonstration Squad – formerly vested with these sweeping powers have since been closed down, for violating ethical standards.
>
> The SDS is praised by police chiefs for vital undercover work that stopped serious crimes and violence. But it has been hit by a series of revelations about its officers sleeping with female campaigners, fathering children and using dead children's identities. The Met declines to say why the SDS was shut down when some of its activities were hailed as being so crucial. A senior source with close knowledge of the secret discussions that led to the closure in 2008 told the Guardian that concerns about the unit surfaced in the Met in 2006, leading to a review being ordered. The source said: "It was worse than out of control. It was actually a force within a force, operating to set of standards and ethics more suited to guerrilla warfare than modern policing. Quite simply, they lost their moral compass and as a result nothing was out of bounds. A quite shocking vacuum of any supervision and leadership allowed this to happen. "…Poor supervision [by] managers were responsible for the retention of intelligence which failed to comply with the law.

[6] Gordon Campbell on the new legislation for the spy agencies (16 August 2016) http://werewolf.co.nz/2016/08/gordon-campbell-on-the-new-legislation-for-the-spy-agencies/

> In New Zealand, there is nothing about safeguards or boundaries in the covert operational powers being granted to our spy agencies.

11.3. The Independent Review recommended at [6.114] that:

> The use of these powers should be covered by a tier 3 authorisation (policy statement) to ensure they are exercised only where necessary and proportionate.

11.4. We agree with the sentiment. However, cl 165 regarding the issue of ministerial policy statements relating to covert activities falls significantly short of assurance that cover will be used only where necessary and proportionate to do so. The use of examples of what might be covered falls short of requiring actual content.

11.5. *We propose that cl 165 should include a subclause that states:*

> *The ministerial policy statement shall direct that the creation and use of assumed identities under subpart 1 of Part 3 and the creation and use of legal entities under subpart 2 of Part 3 shall only occur when and for as long as is necessary and appropriate*.

11.6. The Independent Review also includes a series of recommendations regarding sharing of intelligence between the intelligence and security agencies and foreign partner organisations. The most potentially important of these is the creation of a ministerial policy statement regarding co-operation with overseas public authorities.

11.7. This is an important step towards the public acknowledgement of the degree of co-operation between our intelligence and security agencies and others. We are concerned however, that that framework provided is insufficient to provide reassurance that the intelligence and security agencies will behave in a manner that is protective of human rights.

11.8. There is no requirement to consider or consult on the human rights impact or implications of intelligence sharing with overseas public authorities. This is a major failing given that in many instances the intelligence may be gathered in a manner which substantially impinges on human rights (such as the massive data-mining by the Five Eyes partner nations) or intelligence gathered may be used to stifle fundamental freedoms such as expression, assembly and movement (without the safeguards of the New Zealand legal system).

11.9. *We submit that the Minister responsible for an intelligence and security agency should be required to consider the human rights implications of the activities covered by a ministerial policy statement (including covert activities and co-operating, providing advice or intelligence sharing with overseas public authorities) and to place*

appropriate protections and restrictions on such activities to reasonably protect against human rights abuses by overseas Governments and organisations.

11.10. *Alongside this, the consultation requirements for issuing a ministerial policy statement in cl 169 should include mandatory consultation with the Human Rights Commissioner.*

11.11. We support the proposal that the Director-General make the ministerial policy statements public. However, the restrictions on publication are framed far too broadly and are likely to make the publication of ministerial policy statements almost meaningless due to the significant redactions needed.

11.12. There is a substantial public interest in the publication of these statements which should be balanced against operational considerations and international relations rather than an outright ban. The Government should not be prepared to countenance activities in the shadows that it would not support in the light.

11.13. *We propose that cl 173(2) should state that:*

> *There is a rebuttable presumption of the statement should be disclosed due to the high degree of public interest. A Director-General must balance the public interest with any likely risks that the disclosure would prejudice the carrying out of the activity to which the statement relates, the security and defence of New Zealand or the international relations of the Government of New Zealand.*

12. Intelligence agencies and privacy principles (cl 264)

12.1. *We strongly support the extension of Information Privacy Principles 1, 4(a), 5, 8, 9, 10 and 11 to the intelligence and security agencies[7] via cl 264 replacing s 57 of the Privacy Act 1993.*

12.2. However, we do not think it is appropriate to exempt the intelligence and security agencies from Information Privacy Principle 4(b) which states:

> Personal information shall not be collected by an agency—
>
> (b) by means that, in the circumstances of the case,—
>
> (i) are unfair; or
>
> (ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned.

12.3. Given the potentially intrusive and personal nature of the intelligence gathering by the intelligence and security agencies, this principle is particularly important to their work.

[7] The SIS and GCSB are defined as 'intelligence organisations' in s 2 of the Privacy Act 1993 (rather than intelligence and security agencies).

12.4. *We recommend that the intelligence and security agencies should also be subject to Information Privacy Principle 4(b).*