NEW ZEALAND COUNCIL OF TRADE UNIONS
Te Kauae Kaimahi

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

on the

New Zealand Security Intelligence Service
Amendment Bill

P O Box 6645
Wellington

February 2011

Contents

1. Summary of recommendations

Recommendation 1: There should be a higher standard of evidence required to justify warrants where a person is not precisely identified.

Recommendation 2: There should be requirements to cease tracking and to destroy all relevant records immediately it is realised that a mistake has been made in identifying a targeted individual.

Recommendation 3: An independent report be commissioned to identify to the public the issues of privacy, civil liberties and technical matters that are raised by these proposals.

Recommendation 4: The proposed changes in Clauses 6, 8, 9, 13 and elsewhere relating to the recruitment of persons to assist the SIS not proceed.

Recommendation 5: That the SIS not be permitted to request employees to assist it.

Recommendation 6: Without prejudice to our position in Recommendation 5, that if enlisting of employees is persisted with, employment protection be given to such employees similar to that in s.104 of the Employment Relations Act.

Recommendation 7: Without prejudice to our position in Recommendation 5, if enlisting of employees is persisted with, there should unambiguously, in reality as well as in law, be a free choice by the individual employee, with no adverse consequences should they refuse.

2. Introduction

2.1. This submission is made on behalf of the 39 unions affiliated to the New Zealand Council of Trade Unions Te Kauae Kaimahi (CTU). With 350,000 members, the CTU is the largest democratic organisation in New Zealand.

2.2. 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.

2.3. The CTU has consistently expressed a high degree of concern regarding the increase in powers and intrusiveness of surveillance in New Zealand society including not only the SIS but also increased powers and wide definitions regarding "terrorism", the widening of authority to install and use surveillance equipment such as through the Search and Surveillance Bill, the widening of the definition of "security" to include "the making of a contribution to New Zealand's inter-national well-being or economic well-being", the increased use of private investigators by companies to watch people it considers are working against its interests, and other developments that could be used against people considered opponents of the government of the day.

2.4. Unionists have long been targets for surveillance and accusations by security forces, despite having a firm basis of legitimacy in domestic and international law.

2.5. The widening of the definition of "security" to include "the making of a contribution to New Zealand's inter-national well-being or economic well-being" in 1996 meant that any actions or viewpoints with potential economic consequences could be subject to SIS activities. Most union activity is deliberately concerned with economic wellbeing, as is much political activity in the community. The reach of the SIS is therefore already much too broad, which increases concerns at extensions of its powers, and heightens the need for improved transparency, accountability and oversight.

2.6. We are concerned that this bill sets up structures that will enable random surveillance without sufficient authorisation, at an extreme leading to a situation where there could be a wide network of informants throughout society. While this may not be the intent, we should not set up structures that would allow such outcomes.

2.7. This submission therefore reluctantly accepts the proposed extension of powers to electronic surveillance, but cautions against some provisions and asks for independent expert scrutiny of the proposals.

2.8. However it strongly opposes the proposals to weaken the controls on enlistment of informants (persons “requested to assist” the SIS), both as individuals and as organisations.

3. Background

3.1. Unionists have long been targets for surveillance and accusations by security forces, despite having a firm basis of legitimacy in domestic and international law.

3.2. The role of unions and the rights of union members are described in New Zealand legislation, and protected by international agreements and conventions through the International Labour Organisation, part of the United Nations system. Yet governments have at numerous times in recent and more distant history tried to demonise union activists, union leaders, and unions themselves as communists, saboteurs, or agents of foreign powers.

3.3. Internationally, unions and their leaders and members are constantly under attack in many countries. An extreme case is Colombia, the most dangerous place in the world for trade unionists. On 7 February 2011, the International Trade Union Confederation (ITUC) reported the murder, on 30 January, of Humberto de Jesús Espinoza Díaz, a member of the education trade union of Risaralda, SER. The trade unionist worked as a head teacher at an agricultural school in Mistrato, Instituto Agrícola Mistrato, in the department of Risaralda. According to the latest figures received by the ITUC, 25 out of the 46 trade unionists assassinated in 2010 were teachers. This rate of almost

one trade unionist killed a week has continued over many years in Colombia. It is calculated that over 60 percent of all trade unionists killed world-wide are Colombian.

3.4. Yet unions are among the leaders of the popular movements that have overthrown dictatorial governments recently in Tunisia and Egypt, and in the past in South Africa, the Philippines, Argentina, Brazil, Chile and many other countries. They are a force for progress, and are unpopular among forces defending the status quo as a result.

3.5. The release of personal files of New Zealanders who were under surveillance by the NZSIS and its predecessors has revealed a pattern of suspicion and use of their information and powers against unionists, often connected to their activity in a workplace.

3.6. For example in the 1950s, a university lecturer was put under constant surveillance for some days by the New Zealand Security Service, the predecessor of the SIS. Noted among his movements was an address to the Public Services Association and the file included a report on it. His file also included extracts from the Public Service Journal which included "contributions by subject on various aspects of 'WAGES' with statistics".

3.7. The file of a well known trade unionist records that in 1980, a person from Railways telephoned the SIS "to enquire about certain individuals who are all employed in the Traffic Branch of Christchurch railways who belong to the National Union of Railwaymen (NUR). These individuals were described as causing trouble to the Christchurch railways management." The four individuals were then named. The SIS record continued: "I told LAWRENCE that some of these people were known to us in the context of CAFCINZ but that none of them were members of or associated directly with the SUPNZ."

3.8. So the SIS was used by employers to check on active union members in their employment, and the SIS was forthcoming with information which potentially could have affected their employment. Judging by files released to now numerous people, neither the accuracy nor the interpretation of any information passed to employers can be assured. Employees could be

adversely affected by information provided by the SIS without knowing it was being passed to their employer, let alone having the opportunity to correct it.

3.9. MP Keith Locke's files show that in the late 1970s, sources in vehicle assembly plants and freezing works he was employed in were reporting on him and others to the SIS, including their union and political activities. There was evidence of communication between the source and company management.

3.10. A *Sunday Star-Times* report[1] on the release of his files states:

> Another report says: "Locke has been trying to obtain employment in the Wellington area, but he has been given such bad references by Gear that he no longer asks for them." This suggests to Locke that the SIS and his employers were "conspiring with employers to reduce the influence of what they saw as strong trade unionists". After all, Gear had not complained about his work at the plant – quite the opposite. He had been promoted. Did they prevent him getting work? Locke is not sure. "It's not something I can prove. When I didn't get a job at Dulux Paints, how was I to know whether it was because of 'bad references'".

3.11. Other evidence of SIS sources or direct activity in the workplace include examples at Radio New Zealand, the *Truth* newspaper and universities.

3.12. Social historian, former PSA President and current advisor to Jim Anderton MP, Tony Simpson, found that his SIS files showed that in the 1980s, someone at Radio New Zealand passed scripts by him to the SIS[2].

3.13. Redmer Yska, author of a recently published history of the weekly newspaper *Truth*, "Truth: The Rise and Fall of the People's Paper", told *Sunday Star-Times* reporter Anthony Hubbard ("Spooky Business", 14 November 2010, p.C6) of evidence of the SIS being a source of stories, of the SIS trying to direct journalists to "keep an eye on" subjects of SIS surveillance, and of regular informal meetings between *Truth* staff and SIS

[1] "Locke, stock but no smoking barrel", by Anthony Hubbard, *Sunday Star-Times*, 8 February 2009, p.C3.
[2] "SIS file includes journo's radio talks", by Vernon Small, *Dominion Post*, 27 February 2010, p.A7.

employees. Yska said that there was a pattern of close cooperation between *Truth* and the intelligence services. This not only risks compromising journalists' careers and reputation, but undermines the credibility of the news media.

3.14. In universities, there has been concern over a long period, with evidence of SIS activity and sources going back to the 1960s. Despite a protocol that agents would not study at the same time as conducting surveillance, concern has continued. On 24 March 1994, the *Dominion* on its front page quoted two SIS agents as saying that "they, like all new agents, spent most of their time watching diplomats in Wellington, union leaders, university lecturers and suspected communists."

3.15. In November 2009, a request from the SIS to Vice-Chancellors to alert the SIS to any illicit science relating to the proliferation of weapons of mass destruction raised concerns that university staff were being asked to spy on students and each other. It could also "lead to some academics being targeted because of their religion, nationality or ethnicity" according to then Tertiary Education Union President Dr Tom Ryan. It would "undermine the legislated autonomy of institutions, including the guarantee of academic freedom"[3].

3.16. We have emphasised the effect on unionists and workers because that is who the CTU directly represents, but all of these cases also include wider considerations of people having the right to exercise free expression and to participate in political activities without fear of unjustified or disproportionate consequences that would disadvantage them. Those consequences could come from the State or from those with a degree of power over them, such as employers.

3.17. The personal files and public records show that the SIS has in the past taken interest in a wide range of groups and philosophies, many of which would now be considered mainstream and which have led to changes in society

[3] "SIS seeks varsity help in weapon watch", by Tina Law, *The Press*, 18 November 2009, available at http://www.stuff.co.nz/the-press/news/3072825/SIS-seeks-varsity-help-in-weapon-watch, accessed 13 February 2011.

which are widely welcomed and accepted. They include not only left political parties and discussion groups but organisations pursuing peace, civil liberties, advancement of women, international solidarity with groups opposing oppressive regimes overseas, and many more.

3.18. The examples span several decades. That does not mean concerns regarding security intelligence activities are out of date. It only reflects the fact that more recent information is less available. It does show that abuses and unjustified negative consequences for people exercising their rights as citizens can happen in New Zealand. Under different governments, the risks of abuse of enabling legislation could be higher or lower. We cannot simply assume high-risk legislation will not be abused.

4. The proposed amendments

4.1. The amendments cover two main areas. Firstly, the bill wishes to formalise the right of the NZSIS to undertake surveillance of people by electronic means. Secondly, it proposes changes regarding people assisting the SIS, on the basis of "improving efficiency".

5. Electronic surveillance

5.1. On the first, we see the extension of its powers regarding electronic surveillance as unfortunately inevitable. We have no doubt it is already occurring. It would be illogical to oppose it on principle given the widespread use of electronic devices, but acceptance does not signal any less concern about the rules governing the SIS, its behaviour and competence.

5.2. Its competence has most recently been brought into doubt by its failure to properly vet Stephen Wilce who (in the words of *Dominion Post* journalist John Hartevelt) "bluffed his way in to the job as Chief Defence Scientist and Director of the Defence Technology Agency through a series of elaborate and sometimes extravagant lies"[4]. That it failed on the most fundamental of its tasks does not speak well for its general competence. For a more extensive

[4] "Stephen Wilce inquiry finds SIS failure", by John Hartevelt, *Dominion Post*, 28 January 2011. Available at http://www.stuff.co.nz/dominion-post/news/politics/4593819/Wilce-inquiry-finds-SIS-failure, accessed 13 February 2011.

analysis of its record and its search for a new purpose following the end of the Cold War, see "The Curious Case of Mr. Tucker", by Paul G. Buchanan"[5].

5.3. We are not experts in the issues involved in electronic surveillance, but ask that these issues receive independent expert scrutiny both in technical terms and with regard to their effect on privacy and civil liberties, and the expert advice be made public.

5.4. For example, specifying warrants in terms of the "identity" of the person to be tracked (Clause 7(2)) where the "identity" could be simply a computer alias or username opens considerable risk of unconnected people being tracked as a result of mistaken "identity". There needs to be a high standard of justification for a warrant in these circumstances, and a requirement to cease tracking and destroy all records immediately it is realised that a mistake has been made.

Recommendation 1: There should be a higher standard of evidence required to justify warrants where a person is not precisely identified.

Recommendation 2: There should be requirements to cease tracking and to destroy all relevant records immediately it is realised that a mistake has been made in identifying a targeted individual.

Recommendation 3: An independent report be commissioned to identify to the public the issues of privacy, civil liberties and technical matters that are raised by these proposals.

6. Informants

6.1. We have a high level of concern regarding the proposals to make it easier to "request persons to assist" the SIS. We reject the rationale given for the change – to "improve efficiency and enable the NZSIS to respond more quickly to changes in circumstances". These amendments set up conditions whose possible use and effect mean that the need for close control far outweigh considerations of making the life of the SIS easier.

[5] "Paul G. Buchanan: The Curious Case of Mr. Tucker", 11 February 2009, http://www.scoop.co.nz/stories/HL0902/S00209.htm, accessed 13 February 2011.

6.2. In any case, the improvements in "efficiency" will be minimal. The efficiency is apparently in reducing their requirement to amend warrants. We have surveyed the SIS's annual reports from 2002 to 2010. No amendments to warrants were reported from 2002 to 2007. In 2008 they made 3 amendments, 4 in 2009 and 5 in 2010. Less than 20 percent of their warrants have required amendment over those last three years. That is hardly a major burden on the organisation, especially after taking into account that the warrants represent only a portion of their work (the public is not allowed to know how much). It certainly does not justify additional risks to civil liberties.

6.3. These amendments make it easier for the SIS to "request persons to assist" it – in other words for the SIS to recruit informants, people to assist in planting or removing surveillance devices, or for other purposes. These people, who would presumably not be SIS staff (though the bill is silent on payments to them), would operate in the wider community such as in the workplace. We shall refer to them as "informants" for brevity.

6.4. The description understates the consequences of a person being engaged as an informant. Presumably the SIS has sources in the community who provide information without the need for warrants and who have no more powers than an ordinary citizen. However these informants have wide protection from the law in carrying out a warrant. This includes for example, accessing a computer system in ways they would otherwise be illegal, but it is much more than that. Clause 6(5) amends s.4A(6) to state that both the informant and his or her handler ("authorised person")

> is justified in exercising any powers conferred on the person by or under this Act for the purpose of giving effect to the warrant, and in taking, or attempting to take, any reasonable action necessarily involved in giving effect to the warrant, in accordance with the terms and conditions of the warrant; and
>
> (a) no civil or criminal proceedings shall lie against him by reason of his so doing; and

(b) the issue of the warrant shall not be subject to judicial review under Part 1 of the Judicature Amendment Act 1972 or otherwise.

6.5. The warrant does not need to be produced in Court in any proceedings requiring proof that a person was acting under a warrant, and these powers are in addition to "any other enactment relating to the execution of warrants". (ss. 4A(7), (8)).

6.6. This allows an informant (and authorised SIS employee) to, for example, break in to a house or office, fight with any occupants who either do not know who the person is or in what capacity (which is most likely) or do not want information removed or tracked, read personal correspondence or listen to private conversations, and take items, all without fear of criminal or civil proceedings.

6.7. How in these circumstances it would be possible to judge what is "reasonable" is highly problematic. Frequently (by the nature of such actions) the only witnesses will be the informant and sometimes the person being tracked. Given the secrecy of warrants, the SIS and its employees, legal proceedings would be very difficult for any person who suffered from such actions and considered that a warrant had been exceeded, abused or was not in existence. There appears to be no remedy for an innocent person who suffered from such actions but was a case of mistaken identity as long as the actions taken by the informant were "reasonable".

6.8. Similar provisions are already in the Act, but at least there is some constraint on the SIS as to who and how many people it takes on as informants. Currently informants must be identified in the warrant either individually or by "class of person" (s.4D(2) of the Act). That is weak enough, but at least it requires a degree of justification to the Minister, and provides a specified limit to the period of time those people are under the direction of the SIS. The Director of the SIS may apply for the warrant to be amended by substituting or adding further informants and must do so to change informants (or class of them). It is this minor inconvenience that the bill says it wishes to remove.

6.9. Clause 8 of the bill however amends s.4D to allow informants to be taken on by the SIS without requiring them to be identified to the Minister. Worse than that, the Director of the SIS may delegate this power to any SIS employee, who in turn may delegate that further (Clause 15, new s.5AA(4)). The only constraint will be that requests to informants must be recorded in writing (Clause 8, new s.4D(3)).

6.10. The danger in this is its vagueness and looseness. It could lead to the formation and steady growth of a permanent army of informants with considerable powers. While in theory informants must be taken on "for the purpose of giving effect to a warrant" (new s.4D(2)), it would not be difficult to swap them from warrant to warrant for as long as they were of use to the SIS. There appears to be little that would prevent this, and little accountability for the number or nature of informants being run by the SIS. No-one outside the SIS would know what was occurring, let alone be in a position to challenge it.

6.11. Not to put too fine a word on it, in unscrupulous hands, this allows growth of police state, where increasing numbers of New Zealanders will not know who of their friends or workmates is spying on them.

6.12. The weakness of Parliamentary control increases our concern at the dangers inherent in this proposed situation.

6.13. We consider this a dangerous move and far from minimising the risks to civil liberties, privacy and safety that the powers of the SIS represent, allows indefinite extension of them. We oppose this change.

6.14. We are concerned about a further proposed change in the use of informants, even under the status quo restrictions on enlisting them.

6.15. Under the proposed new s.4D(2) in Clause 8, organisations may be requested to assist the SIS in the same way as individuals. This is a concept that could be described as a "corporate informant".

6.16. The status quo (s.4D(2)) does not allow requests to organisations, but only to individuals or a "class of persons". Under s.4D(3), if an employee is

requested to assist the SIS under a warrant then the warrant must also request “the employers or the employees, or any other persons in any way in control of the employees, to make the services of the employees available to the Security Intelligence Service.”

6.17. The position of an employee being requested to become an informant is highly problematic. If the employer does not know that the employee has accepted, then the employee, even in the best of situations, faces risks of grave misunderstandings of any actions taken as an informant, disciplinary actions, loss of job and possibly career. There may be times when telling the employer would defeat the purpose of the warrant under which the employee is recruited.

6.18. If the employer is told by the SIS that the employee is being requested to inform, there is a risk of pressure from the employer on the employee to take on this role against his or her own wishes and judgement. The employee may feel for example that their future career prospects are at risk should they refuse.

6.19. Informant behaviour is likely to cause deterioration in trust and respectful relationships in a workplace. If the employer is involved it could well constitute a breach of the good faith relationships required under the Employment Relations Act.

6.20. We therefore oppose the enlisting of employees as informants.

6.21. Without prejudice to this position, if enlisting of employees is persisted with, we consider that telling the employer is the lesser of two evils, but there should also be protections for an employee who is requested to inform, similar to those in s.104 of the Employment Relations Act. This would prevent the employer from taking any action that would disadvantage the employee as a result of the decision he or she took. It is still a highly problematic situation, out of keeping with the kinds of workplaces New Zealand should be trying to build.

6.22. If the employer cannot be informed (if for example, he or she is the target of surveillance), existing employees should not be asked to become informants.

6.23. We consider the new proposal to be even more problematic. The amendment says under the new s.4D(5):

> If an organisation is requested under subsection (2), any employee of the organisation whom the organisation nominates to assist the authorised person is taken to have been requested under that subsection.

6.24. An organisation's decision to accept, and its nomination of an individual employee, places even greater pressure on individual employees by increasing the expectation (whether perceived or real) that they should cooperate as part of the job. We reiterate our opposition to employees being enlisted as informants, but again without prejudice to this position, if enlisting of employees is persisted with there should unambiguously, in reality as well as in law, be a free choice by the individual employee, with no adverse consequences should they refuse.

6.25. The new s.4D also removes the requirement of the existing 4D(3) that if an employee is requested to inform, their employer should also be requested, as discussed above. Yet it leaves open the possibility of an individual employee being requested. We oppose this situation.

6.26. Finally, we wonder what the acceptance of a request to assist the SIS by a member-based organisation (such as a union or an incorporated society) means for the members of the organisation. Even the receipt of such a request would put the manager or executive of such an organisation in an extraordinary quandary. It would be an important enough issue that the members should be consulted, but one can assume that would be opposed by the SIS. Yet members would understandably be very angry if they found the organisation was acting as an informant without their knowledge, so the positions of managers, employees and executive would be at risk if the membership found out.

6.27. The acceptance of such a request by an organisation in which freedom of expression is essential, such as a university or news organisation, could also be highly destructive of its ethos, creating an atmosphere of suspicion and distrust if discovered.

6.28. For all these reasons, we strongly oppose this change.

Recommendation 4: The proposed changes in Clauses 6, 8, 9, 13 and elsewhere relating to the recruitment of persons to assist the SIS not proceed.

Recommendation 5: That the SIS not be permitted to request employees to assist it.

Recommendation 6: Without prejudice to our position in Recommendation 5, that if enlisting of employees is persisted with, employment protection be given to such employees similar to that in s.104 of the Employment Relations Act.

Recommendation 7: Without prejudice to our position in Recommendation 5, if enlisting of employees is persisted with, there should unambiguously, in reality as well as in law, be a free choice by the individual employee, with no adverse consequences should they refuse.

7. Conclusion

7.1. We have a high degree of concern about the breadth of scope, powers, functions, work and competency of the SIS, and its effect on trade unionists in particular and on free speech, political activities and privacy in general. Our reluctant acceptance of some of its powers should not be taken as indicating comfort.

7.2. With regard to this bill, we are particularly opposed to extensions and broadening of its powers to recruit informants, and in effect to maintain an army of informants in the workplace and elsewhere in the community. There are grave dangers in the proposals.

7.3. The SIS lacks sufficient public accountability, transparency and oversight. Remedying that should be the first priority in any changes to its status rather than extensions of powers.