Countering Terrorist Fighters Legislation Bill

Submission by the Privacy Commissioner

to the Foreign Affairs, Defence and Trade Committee

---

27 November 2014

Privacy Commissioner
Te Mana Matapono Matatapu

Introduction

The Bill has been introduced on an urgent basis to address particular issues with respect to the emerging risks posed by foreign terrorist fighters.

As well as addressing the counter-terrorism functions of agencies such as the SIS and the Police, I note the opportunity is also taken to enhance measures by which the SIS can carry out its general security functions. For example the SIS will gain visual surveillance powers and emergency powers that may be exercised without a warrant. It is a significant step to confer these powers on the security intelligence service.

It is vital in my view to ensure that appropriate process safeguards are included for these expanded powers.

The following submission focuses on necessary improvements to process and safeguards. It is important to note that in the time available, I have not received a detailed briefing from the SIS on the operational case for the expanded powers. My comments therefore are based in general principle.

I welcome the broader intelligence review of the security legislation that will take place in 2015. The Bill's provisions however deserve proper scrutiny as they will remain in place for over three years until April 2018.

My three key areas of concern relate to:

- The duration of visual surveillance warrants;
- The controls around warrantless surveillance powers;
- Clarifying the continuation of controls around access to Passenger Name Record (PNR) data under the Customs and Excise Act.

Visual surveillance powers – new section 4IA of the NZSIS Act

Period of warrant

Recommendation

> **The maximum period of a visual surveillance warrant should be 3 months, rather than 12 months, subject to renewal.**

Discussion

The Bill proposes new visual surveillance powers for the SIS under a warrant procedure. Continuous visual surveillance (particularly where a visual surveillance device such as a hidden camera is used) is qualitatively different from other forms of surveillance as to the level of intrusiveness on individual privacy rights.

Under the Bill, the time limit for a visual surveillance warrant would depend on whether the granter of the warrant imposes a condition to this effect, and would otherwise be subject to expiry after 12 months (subject to renewal).

Given the potential intrusiveness of continuous surveillance of an individual in a private place, and others who incidentally live at or visit the place under surveillance, there should be stronger checks and balances on the period of surveillance.

My submission is that the maximum period of a visual surveillance warrant should be 3 months, rather than 12 months. Renewals would be available where there is a case for ongoing surveillance operations. Where surveillance is carried out over a prolonged period, this allows the grantors of the warrant to verify the ongoing necessity for the surveillance.

Warrantless powers – new section 4IC of the NZSIS Act

Process safeguards

Recommendations

1. **The warrant application to regularise the exercise of warrantless powers should be made within 12 hours (rather than 48 hours).**

2. **A threshold for the exercise of warrantless powers should be introduced to better reflect the emergency circumstances in which they arise, either:**

    - **by limiting the use of warrantless powers to counter-terrorism activities; or**
    - **by adopting the formulation used as the threshold for refusing to issue a passport "where there is a danger to the security of New Zealand from a terrorist act, the proliferation of weapons of mass destruction or unlawful activity designed or likely to cause devastating or serious economic damage".**

Discussion

As noted in the introductory comments, it is a significant step to confer warrantless powers on the security intelligence service. In my view, the warrant process is the primary and critical mechanism for ensuring appropriate oversight of the use of surveillance powers in the security intelligence context. Departure from the warrant process should be justified, limited and proportionate.

The Bill proposes that the SIS would be authorised to exercise interception, search, visual surveillance and tracking powers for counter-terrorism purposes as well as for general security purposes, for a period of up to 48 hours without a warrant.

Following my office's initial engagement with officials, the proposed process safeguards around the use of warrantless powers have been strengthened and now include the following:

- The Director has to advise the Minister, the Commissioner of Security Warrants and the Inspector General within 12 hours of the authorisation;
- The Minister or the Commissioner may direct the Service to discontinue the warrantless activity or to destroy the information collected;

- The Director must ensure that a direction to cease or destroy given by the Minister or the Commissioner is carried out without delay;
- The Minister must ensure all non relevant records are destroyed;
- Failure to destroy non relevant records is an offence;
- Once the warrantless power has expired, it cannot be used again in relation to the same subject matter;
- If a warrant is not subsequently sought, the Director must report to the Minister and the Commissioner on why the authorisation was given, why no warrant was sought and the nature of the information collected;
- The Minister and the Commissioner then decide if the authorisation was appropriate – if not it is referred to the Inspector General for investigation; and
- Annual reporting is to include the number of authorisations given, the number that were subsequently followed by a warrant application and the number that were subsequently considered not appropriate.

However, there is room for further improvement. Although the heading for the new power is "situations of emergency or urgency", the substance of the provision essentially permits warrantless surveillance (subject to the authorisation of the Director) on grounds of impracticability and delay.

In my submission, the obligation to notify the Minister and Commissioner of Security Warrants within 12 hours of the authorisation should be strengthened to require a warrant application to made within 12 hours. Under this approach, the surveillance would be positively authorised by the Minister and Commissioner, rather than being subject to discontinuance.

In addition, the use of warrantless powers should be reserved for the most significant and serious investigations and monitoring. I suggest either limiting warrantless surveillance powers to counter-terrorism activities, or alternatively, adopting the formulation used as the threshold for refusing to issue a passport "where there is a danger to the security of New Zealand from a terrorist act, the proliferation of weapons of mass destruction or unlawful activity designed or likely to cause devastating or serious economic damage."

The case for more generic warrantless powers could be revisited in the broader 2015 intelligence review of the security legislation.

Public reporting should be more frequent

Recommendation

> **The frequency of reporting should be increased from annually to either monthly or at least quarterly – new section 4IE (9)**

Discussion

The proposed annual reporting is not sufficiently frequent to provide the appropriate transparency and public confidence that the powers contained in the Bill will not be used excessively.

Direct access to Customs databases

The Bill is unclear about whether established controls for accessing Passenger Name Record (PNR) data would apply

Recommendations

1. **The Bill should clarify that sections 38G to 38K of the Customs and Excise Act apply to direct access for counter-terrorism purposes:**

    a) **Change new section 280M(5) definition of "information" (b)(ii) to "information the Customs is entitled to view under any of sections 38G to 38K"**
    b) **Add new sub-section 280M(5) definition of "information": (c) "does not include information which the Customs is not entitled to view under sections 38G to 38K".**

2. **The Bill should require the Chief Executive of Customs to consult the Inspector-General of Intelligence and Security and the Privacy Commissioner prior to concluding the access agreement with the Director of Security and the Commissioner of Police.**

Discussion

The Bill should not expand SIS's or Police's lawful access to passenger name record (PNR) information

New section 280M of the Customs and Excise Act grants SIS and Police "direct access" to a range of Customs data, including information collected under Part 3A of the Customs and Excise Act. This includes information on the travel details of every person crossing the border provided in advance by airlines, more commonly known as "passenger name record" or PNR data.

I understand that the intent of this new section is to clarify that SIS and Police can lawfully be provided direct access to Customs systems for the purpose of accessing relevant information, and to allay concerns that there may be a distinction between "direct access" and "disclosure" as is currently provided for under section 282A of the Customs and Excise Act.

Access to PNR data is carefully restricted by sections 38G-38K of the Customs and Excise Act. Under these criteria Customs may only view PNR data without warrant:

- within 28 days of the travel (section 38H);
- where an individual has undertaken travel within the 28 day period (section 38I); and
- in emergencies where a warrant would otherwise be granted (section 38K).

Section 282A of the Customs and Excise Act makes clear that Customs may only disclose information to other agencies for other purposes where it meets the criteria set out in 38G to 38K of the Act, including where it has been viewed under warrant (warrant requirements are set out in section 38J).

The 28 day window is intended to prevent PNR data being used for ongoing surveillance of individuals' travel. PNR data covers all travelling individuals, whether or not they raise law enforcement, immigration or security concerns. Its collection and use has been the subject of significant debate internationally, and it is covered by IATA guidelines which emphasise the need to preserve passenger privacy.

New section 280M does not expressly preserve the restrictions that currently exist in section 282A of the Customs and Excise Act, and would therefore expand NZSIS and Police's rights to access PNR data. This could be corrected by changing the reference to "part 3A" in the definition of "information" in new section 280M to "information the Customs is entitled to view under any of sections 38G to 38K", and by adding a new subclause (c) "does not include information which the Customs is not entitled to view under sections 38G to 38K". This language mirrors the existing language used in section 282A of the Customs and Excise Act.

Access agreement should be subject to consultation

New section 280M make clear that direct access to Customs systems must be subject to a written agreement. This is an important requirement that ensures that Customs' legal obligations with regard to the disclosure of information are maintained by providing direct access, and that appropriate safeguards are put in place. To this end I recommend that the Chief Executive of Customs be required to consult myself and the Inspector General of Intelligence and Security on the agreement. Consultation of this sort is usual in other information sharing contexts.

Passports Act amendments

I do not make any recommendation on this aspect of the Bill.

A passport is a significant identity document and therefore expanding the power to cancel or to deny the issue of a passport or travel document potentially raises privacy concerns. However I have taken account of the current suspension powers in the Passports Act that will continue to operate subject to certain extensions proposed by the Bill, the serious grounds that must exist before the powers may be exercised, the notification requirement and appeal rights.

I have also conferred with the Human Rights Commission and defer to the Commission's conclusion that the Bill's proposals are generally consistent with international law.