NEW ZEALAND LAW SOCIETY

NZLS EST 1869

New Zealand Intelligence and Security Bill

11/10/2016

Submission on the New Zealand Intelligence and Security Bill

1 Introduction

1.1 The New Zealand Law Society (**Law Society**) welcomes the opportunity to comment on the New Zealand Intelligence and Security Bill (**Bill**).

1.2 The Law Society's submissions are set out below and address the Bill part by part.

1.3 In summary, the Law Society recommends that:

(a) The current definition of "national security" in clause 5 of the Bill should be retained. However, if the alternative definition proposed by officials is adopted, further public consultation should be undertaken on the text of a revised Bill implementing the alternative definition (paragraphs [2.11] – [2.12]).

(b) The reference in clause 11 to the agencies' "principal" objectives should be deleted (paragraph [3.3]).

(c) The Bill should be redrafted to clearly define the terms "well-being" and "economic well-being" in clause 11 or to restrict what intelligence agencies are allowed to do in pursuit of those objectives (paragraph [3.5]). The same recommendation applies also in relation to the intelligence agencies' ability under Part 5 of the Bill to access information held by other agencies (paragraphs [5.2] – [5.6]).

(d) A definition of "public authority" should be inserted in clause 4, to provide certainty about the scope of the clause 13 – 15 assistance functions (paragraph [3.8]).

(e) Clause 16 as currently drafted creates a significant gap in the protections provided in the Bill and should be redrafted to ensure that the co-operation function (i) is consistent with the intelligence agencies' clause 11 objectives and (ii) requires authorisation under Part 4 of the Bill (paragraphs [3.9] – [3.21]).

(f) The new function (clause 17) of the agencies' co-operation with other entities to respond to imminent threats is far-reaching and its scope will need careful consideration; in particular, its application to "any entity" is too broad, and there is potential for clause 17 to be used to circumvent the authorisation process under Part 4 (paragraphs [3.24], [3.27], [3.32]).

(g) A general principle should be inserted in the Bill, requiring the least intrusive collection of intelligence (paragraph [3.33]).

(h) The Committee should consider whether GCSB's operational requirements justify the conferment of broadly expressed powers (clause 66(1)(e) and (f)) in relation to intelligence warrants (paragraphs [4.2] – [4.8]).

(i) Clause 55 (relating to the issue of Type 1 warrants) and clause 63 (authorised activities) are drafted too broadly and should be narrowed in their application (paragraphs [4.9] – [4.12]).

(j) The Committee should consider whether the protections applicable to Type 1 warrants (New Zealand citizens and permanent residents) should also apply to Type 2 warrants (non-New Zealanders) (paragraphs [4.13] – [4.26]). At a minimum, the Committee should inquire further as to the justification for the current distinction based on nationality (paragraph [4.27]).

(k) The Bill should expressly require that applications for intelligence warrants are in writing, particularise the scope of the proposed activities, and address all matters relevant to the statutory criteria for warranting (paragraphs [4.39] – [4.41]).

(l) The issuing of urgent warrants should require "significant" or "serious" (rather than merely "material") prejudice, as a threshold allowing the relaxation of controls over the authorisation of unlawful activity (paragraphs [4.47] – [4.48]).

(m) "Very urgent" authorisations should be revoked either upon the expiration of 24 hours or the determination of any subsequent application for a warrant, regardless of whether a warrant actually issues (paragraph [4.54]).

(n) Clause 77(1) should be redrafted to make clear that the Director-General must be "satisfied" of the requisite urgency (paragraph [4.55]), and to impose a more stringent test for very urgent authorisations (paragraphs [4.56] – [4.58]).

(o) Clause 91, relating to the retention of incidentally obtained information, should be amended to ensure disclosure is made only to appropriate agencies and in relation to a higher threshold of "serious crime" (paragraphs [4.62] – [4.64]).

(p) Direct access agreements should include a reporting requirement: it would enhance transparency and public confidence for the intelligence agencies to be required to publish an annual summary report under the direct access agreements, and for the Privacy Commissioner and Inspector-General to be able to seek further information if required (paragraph [5.8]).

(q) The proposed power in clause 109 to amend Schedule 2 (databases accessible to the intelligence agencies) by Order in Council is not warranted and clause 109 should be removed from the Bill (paragraphs [5.9] – [5.12]).

(r) Clauses 257 – 259 (closed proceedings under the Passports Act) raise significant concerns that proceedings will not be fairly heard, and the Committee should consider amendments to the Passports Act closed procedure to ensure appropriate safeguards are incorporated (paragraphs [6.6] – [6.7]).

(s) The privacy protections contained in the Bill would be enhanced if the new exception to principle 10 was made available only to the intelligence agencies themselves (rather than, as currently drafted, being more widely available to other agencies) (paragraphs [6.12] – [6.15]).

2 Part 1 of the Bill: Preliminary provisions

Clause 5 – definition of "national security"

2.1 The Law Society supports the approach taken in the Report of the First Independent Review of Intelligence and Security in New Zealand (**Review Report**) to:

- require that the intelligence and security agencies should only be able to obtain a warrant to target New Zealand citizens, permanent residents and organisations where it is necessary to protect national security; and
- define "national security", in order to make clear what circumstances must exist before such a warrant may be obtained.

2.2 The Law Society considers that the definition of "national security" contained in clause 5 of the Bill, which is almost identical to that recommended by the Review Report, is workable and strikes a proper balance between:

(a) being broad enough to reflect the wide-ranging and changing nature of threats to New Zealand's status as a free, open and democratic society; and

(b) ensuring the definition is restricted to *protecting* New Zealand's national security.

2.3 The Law Society does not support the alternative approach to the term "national security" advocated in DPMC Factsheet No 3 and Cabinet Paper No 4. Under that alternative approach, "national security" would not be fully defined, but would be determined by the Attorney-General and Commissioner of Intelligence Warrants on a case-by-case basis by reference to a list of qualifying activities.

2.4 The Review Report considered it to be important to define "national security" because of the distinction between protecting national security and the agencies' other objectives, for the purposes of collecting information about New Zealanders. The Law Society agrees that this distinction means that the definition of "national security" needs to be transparent. The Bill makes it clear that New Zealanders can be targeted, but only if doing so is necessary to protect national security. It is important that this distinguishing feature is carefully defined in the legislation so that the legal criteria applicable are clear and so that the lawful application of those criteria can be tested in particular cases.

2.5 Adopting the alternative approach set out in DPMC Factsheet No 3 and Cabinet Paper No 4 would carry an unacceptably high risk that warrants to target New Zealanders would be issued without a genuine need to protect national security.

2.6 The Law Society's concerns are partly driven, for example, by Cabinet Paper No 4, which states that:[1]

> The New Zealand Intelligence Community has shifted to a customer-driven model … The agencies' primary purpose is to collect intelligence to support the work of other agencies … [including] the criminal investigation and law-enforcement functions of the Police (which is the basis for including certain serious criminal activities in the list of activities).

2.7 There is a danger that the agencies may, in a desire to provide good service to other agencies, become overly focussed on the more concrete activity-based elements of the second limb of the proposed alternative definition, for example "serious crime" involving "use or transfer of intellectual property", to the detriment or even exclusion of the proposed national security limb.

2.8 Defining "national security" in concrete terms, as clause 5 of the Bill would do, is more likely to ensure national security is afforded its proper status as the principal prerequisite for the issue of a warrant targeting a New Zealander.

2.9 The Law Society also has concerns that the activities listed in the second limb of the proposed alternative definition are outside the definition of "national security" in clause 5. They seem instead to be matters of more general concern to law enforcement agencies such as the Police, including "activities which may be relevant to serious crime", involving "the movement of money, goods or people" or "use or transfer of intellectual property" or "threats to New

[1] At [62].

Zealand government operations". These activities are potentially outside the realm of national security.

2.10 The alternative definition also lacks the qualifiers used in the clause 5 definition. For example, the alternative definition merely refers to "threats to, or interference with, information (including communications) or information infrastructure of importance to the Government of New Zealand". By contrast, the definition in clause 5 refers to "threats, or potential threats, to the integrity of information or infrastructure of *critical* importance to New Zealand."

2.11 Accordingly, the Law Society recommends that the Bill's definition of "national security" in clause 5 be retained.

2.12 Given the importance of the concept of "national security" to the Bill as currently drafted, if this recommendation is not adopted the Law Society submits that the Committee should:

(a) release the text of a revised Bill implementing the alternative approach; and

(b) allow for a further round of public submissions on the proposed amendments to the Bill giving effect to the alternative approach.

3 Part 2: Intelligence and security agencies

Clause 11 – objectives

3.1 Clause 11 closely follows the language of existing section 7 of the Government Communications Security Bureau Act 2003 (**GCSB Act**), with two amendments: the qualification of the objectives as "*principal* objectives"; and the specification that the agencies are to contribute to "*the protection of* national security".

3.2 The Law Society supports the inclusion of the words "the protection of" in clause 11(a).

3.3 The Law Society does not support the reference to "*principal* objectives" in clause 11. The description of the objectives as "principal" objectives creates uncertainty by implying that the agencies may have other, unstated, secondary objectives. Given the nature of the agencies, their objectives should be clearly and exhaustively defined in their governing statute. The Law Society recommends that the word "principal" is deleted.

3.4 Clause 11 will be critical in establishing the boundaries within which the Government Communications Security Bureau (**GCSB**) and New Zealand Security Intelligence Service (**SIS**) may exercise the functions and powers given to them under the Bill. As a general principle of administrative law, an agency may only exercise its functions and powers to achieve the objectives for which it has been established. This is reflected, for example, in the requirements for Type 1 and 2 intelligence warrants in clauses 55 and 56.

3.5 It is therefore important that there is no uncertainty about the meaning of the terms in clause 11. The Law Society accordingly supports the inclusion of a definition of the term "national security" in the Bill, as submitted above at [2.1] – [2.12]. As discussed in more detail below at [5.2] – [5.6], the Law Society also recommends that the Bill define the terms "well-being" and "economic well-being" or restrict what intelligence agencies are allowed to do in pursuit of those objectives.

Clauses 13, 14 and 15 – assistance to "public authorities"

3.6 Clauses 13(2)(a), 14(1)(a) and 15(1)(a)(i) provide that the functions of the GCSB and SIS include the provision of assistance to "*any public authority* (whether in New Zealand or overseas)".

3.7 "Public authority" is not defined. This creates uncertainty about the scope of these assistance functions. The uncertainty is compounded by the use of the expression "government agency" elsewhere in the Bill (see, for example, clause 25 where "government agency" is listed as a type of "agency" in the definition of that term). This implies that a "public authority" is something different to a "government agency". But the nature of the difference is not clear.

3.8 The Law Society recommends that a definition of "public authority" be inserted in clause 4.

Clause 16 – co-operation with other entities to facilitate their functions

3.9 Clause 16 provides that it is a function of the GCSB and SIS to provide co-operation, advice and assistance to the New Zealand Police (**NZ Police**) and the New Zealand Defence Force (**NZDF**).

3.10 Clause 16 closely follows the existing function of the GCSB, contained in section 8C of the GCSB Act. The SIS, however, has no equivalent existing statutory function. Clause 16 therefore expands on the existing functions of the SIS.

3.11 The Law Society raised a number of concerns about the extent of the co-operation function in section 8C of the GCSB Act prior to its adoption.[2]

3.12 Those concerns also apply to clause 16. In particular:

(a) Clauses 16(1)(a) and (b) authorise both the GCSB and the SIS to "co-operate with" and to provide "advice and assistance to" the NZ Police and the NZDF. The open-ended nature of that language is broadly empowering of the whole range of activities that these agencies may engage in.

(b) Such advice and assistance must be "for the purpose of facilitating the performance or exercise of the [NZ Police's or NZDF's] functions, duties or powers" (clause 16(1)(b)). There is no express requirement that the advice or assistance must also achieve the clause 11 objectives of the GCSB and SIS. It seems likely that a court interpreting these provisions would say that the agencies must act consistently with their objectives. However, the Law Society submits that in the interests of clarity the Bill should make it an express requirement that any assistance provided under clause 16 must also achieve the *clause 11 objectives*. Reference to the *clause 11 objectives* is appropriate, particularly if that clause continues to refer to the agencies' "*principal* objectives" (see [3.3] above).

(c) Clause 16(2)(c) authorises the GCSB or SIS to provide such advice and assistance even though it may involve activities that could not otherwise be authorised under the Bill.

3.13 The Bill and supporting material are not clear as to whether the GCSB and SIS would need to obtain authorisation under Part 4 of the Bill when exercising the co-operation and assistance function under clause 16, or whether they would be able to rely solely on any warrant or other authorisation obtained by the NZ Police or NZDF.

---

[2] Law Society submission on the Government Communications Security Bureau and Related Legislation Amendment Bill 2013 (14 June 2013) at [27] to [29].

3.14 In particular, it is not clear whether an activity carried out by the GCSB or SIS under clause 16 to assist the NZ Police or NZDF in executing a warrant obtained under other legislation would be a "lawful" or an "unlawful" activity for the purposes of clauses 48 and 49.

3.15 This ambiguity needs to be resolved. Otherwise there is potential for clause 16 to be used to expand the activities that may be conducted by the GCSB or the SIS without having to meet the requirements for a Type 1 or Type 2 intelligence warrant under the Bill.

3.16 For example, clause 16 would permit the NZ Police to draw on the sophisticated electronic interception capabilities of the GCSB to execute a surveillance device warrant issued against a New Zealand citizen under section 53 of the Search and Surveillance Act 2012. It is arguable that, because a warrant has already been issued to the NZ Police, the GCSB would be carrying out a "lawful activity" and authorisation would therefore not be required under clause 48.

3.17 The conditions under which the NZ Police could obtain a surveillance device warrant are set out in section 51 of the Search and Surveillance Act. They fall significantly short of the conditions under which the GCSB could obtain a Type 1 intelligence warrant for the same activity under clauses 55 and 57. In particular:

(a) The NZ Police would not be required to establish that:

(i) the interception is necessary and proportionate and the purpose of the warrant cannot be achieved by a less intrusive means (as required by clause 57(a) to (c)), and

(ii) there are arrangements in place to ensure that the information collected under the warrant will not be misused (as required by clause 57(d) and (e)).

(b) The protections provided by the Type 1 "triple lock" requirements[3] would not apply. Warrants under the Search and Surveillance Act are issued by a single judge. They are not reported to the Inspector-General of Intelligence and Security (**Inspector-General**). It is not clear whether the judge issuing the warrant would be aware of the fact that the GCSB would be used to assist the NZ Police in its execution.

3.18 This creates a double standard. Activities carried out by the GCSB and SIS on their own initiative must meet the authorisation requirements of Part 4 of the Bill. However, the same activities carried out by the GCSB and SIS at the request of the NZ Police do not.

3.19 The Law Society therefore considers that, as drafted, clause 16 creates a significant gap in the protections provided in the Bill. It does not consider that the implications of clause 16 have been fully explained or justified in the Regulatory Impact Statement (**RIS**) and other material accompanying the Bill.

3.20 The Law Society recommends that the Bill should be amended to clearly require that any activities performed under clause 16:

(a) must be consistent with the objectives contained in clause 11; and

(b) also require authorisation under Part 4 of the Bill.

---

[3] Regulatory Impact Statement at [115]: "Tier one warrants (targeting a New Zealander) would be authorised by the Attorney-General, approved by a judicial commissioner, and subject to the review and audit of the Inspector-General (a "triple-lock")."

3.21 If, contrary to this submission, officials consider that activities performed under clause 16 should not have to meet these requirements, the Committee will need to satisfy itself that the double standard identified above has been adequately explained and justified.

Clause 17 – co-operation with other entities to respond to imminent threat

3.22 Clause 17 contains a new function to co-operate with and provide assistance and advice to "any entity that is responding to an imminent threat to the life and safety" of persons in certain circumstances.

3.23 This is a far-reaching provision. The creation of such a function was recommended by the Review Report. The Law Society notes, however, that there was little discussion of the need for, and implications of, this new function in the Review Report. The addition of this function and its scope should therefore be considered carefully by the Committee.

3.24 The Law Society has two primary concerns about clause 17:

(a) its application to "*any entity* that is responding to an imminent threat" is too broad; and

(b) there is potential for the provision to be used to circumvent the authorisation process under Part 4.

Application to "any entity"

3.25 The Law Society is concerned by the extension of the clause 17 co-operation function to "*any entity*". "Entity" is defined in clauses 4 and 36 to mean: an unincorporated body; a body corporate; a corporation sole; or a trust. However, that definition in clause 36 is expressed as applying only to Part 3, subpart 2. No separate definition is provided in the context of Part 2. It is unclear whether a different meaning of "entity" is intended in relation to Part 2. The Law Society recommends that this is clarified.

3.26 The Law Society considers that the definition of "entity" in clause 36 is significantly broader than the problem that clause 17 is intended to address. The Addendum to the RIS provides the following examples of the type of organisations that clause 17 is intended to cover: the NZ Police, Maritime New Zealand, or overseas search and rescue authorities.[4] This is a much narrower class of organisation than those that fall under the definition of "entity" in clause 36.

3.27 The Law Society accordingly recommends that the expression "any entity" be revisited to ensure that clause 17 is no wider than necessary to achieve its stated purpose.

Clauses 17(2)(b) and (d) – circumvention of authorisation process

3.28 There is also the potential for the function in clause 17 to be used to circumvent the usual authorisation process under Part 4.

3.29 This risk was identified by officials preparing the Bill.[5] In order to address that risk, officials recommended the inclusion of what is clause 17(2)(b). This is intended to prevent the GCSB or SIS from relying on the assistance function when carrying out activities that more properly fall within their intelligence gathering or protective security functions.

---

4 At [26] to [28].

5 Addendum to the Regulatory Impact Statement, at [31].

3.30 However, the Law Society is concerned that, when read together with clause 17(2)(d), clause 17(2)(b) could be interpreted as meaning that other activities carried out under clause 17 do not require authorisation under Part 4.

3.31 The Law Society does not consider that this is necessary or appropriate. Part 4 provides for "very urgent authorisations" in the case of situations of urgency. The definition of "situation of urgency" in clause 47 encompasses all of the situations set out in clause 17(1). It should therefore be possible to obtain a very urgent authorisation to carry out any of the activities necessary to discharge the function provided for in clause 17.

3.32 The Law Society accordingly recommends that clause 17(2) should be amended to provide that an intelligence and security agency may perform the function under clause 17(1) only to the extent that it involves the exercise of powers or the conduct of activities which are otherwise lawful or have been authorised under Part 4.

General principle of least intrusive collection of intelligence

3.33 The Review Report concluded that, as a general principle, intelligence should be collected using the least intrusive means possible in the circumstances. Where information can be collected through open sources, that should always be the preferred option.[6] The Law Society supports this finding. A general principle should be inserted into the Bill (potentially after clause 22) stating that intelligence must be collected using the least intrusive means possible in the circumstances and that collection of information though open sources should be preferred.

4 Part 4: Authorisations

The move to a single framework

4.1 The Bill enables the GCSB and the SIS to continue to seek warrants to undertake activities that would otherwise be unlawful, but changes the authorisation process. The Bill provides a single authorisation framework under which both agencies must operate. The Law Society considers a single framework is logical, given:

(a) the warranted activities of each agency have common privacy and other implications; and

(b) the current, bifurcated approach gives rise to the operational difficulties identified in the Review Report.

Expansion of activities capable of authorisation and attendant powers

4.2 Under current legislation:

(a) the Director of GCSB must obtain authorisation to intercept communications or to access information infrastructures; and

(b) the Director of Security must seek authorisation to either (i) intercept or seize any communication, document, or thing not otherwise lawfully obtainable or (ii) undertake electronic tracking.

[6] Review Report at [2.8] and p 146.

4.3 Under the proposed single framework, a broader scope of activities may be warranted. Warrantable activities could include:

(a) requesting the government of another jurisdiction to undertake an activity that, if undertaken by NZSIS or GCSB, would be an unlawful activity (clause 63(1)(e)); and

(b) "human intelligence gathering activities", which are broadly defined as activities involving the use of any person to gather intelligence but not activities involving violence, threats of violence or attempts to pervert the course of justice (clause 63(1)(g)).

4.4 Although either agency may seek authorisation to undertake such activities, the powers available to the personnel of each differ. SIS warrants will confer powers allowing entry to and searching of places and the placement of visual surveillance devices and tracking devices. GCSB warrants will not allow entry, search or (unless for the purpose of maintaining operational security of the authorised activity) the use of visual surveillance devices.

4.5 However, under clauses 65(1)(l) and 66(1)(f) warrants issued to either agency would confer powers to "do any other act that is reasonable in the circumstances and reasonably required to achieve the purposes for which the warrant was issued". Such broadly expressed powers are in addition to other broadly expressed powers to "do any act that is reasonable in the circumstances and reasonably required to conceal the fact that anything has been done under the warrant and to keep the activities of the intelligence agency covert" (clauses 65(1)(k) and 66(1)(e)).

4.6 Employees of SIS are already empowered to do "any other act that is reasonable in the circumstances and reasonably required to achieve the purposes for which the warrant was issued". The Bill seeks to extend that general power to GCSB personnel.

4.7 The Law Society questions whether:

(a) GCSB's operational requirements justify the general conferment of such broadly expressed powers; and

(b) any such requirements might not be met by a "joint warrant", under which employees of either agency may access the powers of both.

4.8 These questions arise because the Bill does not seek to change the fundamental character of the agencies. Under clause 9(1) the SIS continues as an agency "that specialises in human intelligence activities" and, under clause 10(1), GCSB continues as a department "that specialises in signals intelligence and information assurance and cybersecurity activities". Currently employees of GCSB undertake those activities simply through authorised interception and access activity.

Breadth of clause 55(2)(b) and 55(2)(c)

4.9 The Review Report considered that the intelligence and security agencies should only be able to target New Zealand citizens, permanent residents and organisations where it is necessary to protect national security.[7] The Law Society agrees with that approach. By contrast, clauses 55(2)(b) and (c) would allow New Zealanders to be targeted for the broader objectives of "the international relations and well-being of New Zealand" or "the economic well-being of New Zealand" if:

[7] Review Report at [21] and [30].

(a) there is a reasonable suspicion they are acting or purporting to act for or on behalf of a foreign person, a foreign organisation or a designated terrorist entity; or

(b) there is a reasonable suspicion they are part of a class of persons employed by or members of a foreign government or are members of a foreign government or a designated terrorist entity.

4.10 The Law Society considers that clause 55(2)(b) and (c) are drafted too broadly. Clause 55(2)(b), for example, would allow a New Zealand lawyer to be targeted for the objective of the "well-being of New Zealand" merely on the basis of a reasonable suspicion the lawyer is acting for an Australian person. The Australian person for whom the lawyer is acting need not even have any relevance to the intelligence sought to be gathered under the warrant.

4.11 In the Law Society's view, the reference to "designated terrorist entities" in clauses 55(2)(b)(ii)(C) and 55(2)(c)(ii)(B) does not justify clauses 55(2)(b) and (c). New Zealanders who are acting for, employed by, or members of a designated terrorist entity are likely to be caught in any event by clause 55(2)(a) because the protection of national security is likely to be activated in that scenario.

Breadth of clause 63(1)(e)

4.12 The Law Society also questions whether clause 63(1)(e) achieves its intended purpose. This sets out one of the categories of activity capable of authorisation under warrant. It would allow a Director-General to seek authorisation to request other Governments "to undertake an activity that, if undertaken by an intelligence and security agency, would be an unlawful activity". Such authorisations could enable a Director-General to request a foreign intelligence agency to undertake intelligence gathering in New Zealand that would be contrary to New Zealand law.

Discriminatory effects of the authorisation process

4.13 Currently:

(a) SIS has powers to seek not only "foreign" but also "domestic" interception warrants whereas, under section 14 of the GCSB Act, GCSB may not gather intelligence by intercepting private communications of New Zealand citizens and permanent residents; and

(b) SIS and GCSB warrants receive increased scrutiny if sought in relation to New Zealand citizens or permanent residents.

4.14 The Bill does not continue the GCSB Act's injunction against domestic spying. However, as discussed below, the proposed single framework would continue to discriminate between New Zealand citizens/permanent residents and others, by differentiating two kinds of intelligence warrants (Type 1 and Type 2 warrants) and then discriminating between those warrants in terms of authorisation requirements and process.

4.15 The New Zealand Bill of Rights Act 1990 (**NZBORA**) and the Human Rights Act 1993 (**HRA**) provide for the right to freedom from discrimination.[8] In particular, section 19 of NZBORA sets out:

[8] New Zealand Bill of Rights Act 1990, s 3(a); and Human Rights Act 1993, s 20J(1)(a).

> **19 Freedom from discrimination**
>
> (1) Everyone has the right to freedom from discrimination on the grounds of discrimination in the Human Rights Act 1993...

4.16 The prohibited grounds of discrimination listed in section 21 of the HRA include:[9]

> ethnic or national origins, which includes nationality or citizenship

4.17 On its face, the Bill proposes to discriminate within the warranting regime on the basis of nationality (clauses 51 and 52).

4.18 Part 4, subpart 1 of the Bill sets out a framework where a Type 1 intelligence warrant is reserved for persons who are New Zealand citizens or permanent residents of New Zealand while a Type 2 warrant is for all other persons. An application for a Type 1 warrant must be made to the Attorney-General and the Chief Commissioner of Intelligence warrants. An application for a Type 2 warrant needs only to be made to the Attorney-General (clause 53). While it can be expected the Attorney-General will exercise his/her functions on an independent basis, this framework applies less scrutiny to Type 2 warrants affecting persons who are not New Zealand citizens or permanent residents.

4.19 The Bill also discriminates between New Zealand citizens/permanent residents and others when it comes to the material that may be seized under an intelligence warrant. Clause 67 provides that an intelligence warrant may not authorise the carrying out of any activity or the exercise of any power for the purpose of obtaining privileged communications of a New Zealand citizen or a permanent resident. There is no equivalent provision in relation to the privileged communications of other persons.

4.20 The Ministry of Justice in its advice to the Attorney-General for the purposes of section 7 of the NZBORA did not address this issue nor whether the prima facie discrimination was considered to be justified. In the absence of detailed consideration by the Ministry of Justice, it is difficult to assess the reasons for, and the reasonableness of, the distinction.

4.21 The only (brief) discussion in the materials accompanying the Bill is in the RIS. It states:[10]

> Certain aspects of the Bill infringe upon the right of individuals to be free from discrimination. Non-discrimination is a core value in New Zealand society and the right to be free from unfair discrimination is protected by the Human Rights Act 1993 and the Bill of Rights Act 1990. This Bill will discriminate on the basis of nationality, in that New Zealand citizens and permanent residents are afforded added protections in the warranting and oversight regime compared to foreign nationals. Officials are confident that **national security and the national interest provide sufficient grounds for a limitation on the right, and that drawing such a distinction in this sphere reflects established practice in New Zealand and comparable jurisdictions.**
> (Emphasis added.)

4.22 The RIS appears to justify the distinction between New Zealanders and others on the basis of "national security" and "national interest", without further elaboration. It is therefore difficult to assess whether the discrimination is rationally connected to these aims.

4.23 The Law Society questions the statement in the RIS that it is "established practice" in New Zealand to discriminate in this way. The Law Society notes a similar type of nationality distinction was the subject of a recent section 7 report on the Land Transfer (Foreign

---

9 Human Rights Act, s 21(1)(g).

10 Regulatory Impact Statement at [302].

Ownership of Land Register) Amendment Bill 2016. In that report the Attorney-General expressed the view that the Land Transfer (Foreign Ownership of Land Register) Amendment Bill "prima facie" discriminates on the "grounds of national origin" due to the Bill's requirement that overseas persons must provide details of their nationality for the purposes of a land register. The Attorney-General could not find sufficient justification under section 5 of NZBORA for this discrimination.[11]

4.24 National security risk assessment is based on the type and scale of the threat. The nature of that threat, whether from a New Zealander or a non-New Zealander, is key. More rigorous analysis is needed as to whether the practice of discriminating between New Zealanders and non-New Zealanders is an anachronism.

4.25 Further, the Law Society notes that there is no nationality distinction for warrants under the Search and Surveillance Act. The Search and Surveillance Act and the Bill both have similar implications for the privacy rights of individuals. Creating a distinction in the proposed Bill would create an inconsistency across these two frameworks.

4.26 The Law Society suggests that the same protections applicable to the issue of a Type 1 warrant should also apply to a Type 2 warrant.

4.27 At a minimum, however, the Committee should seek advice from officials on what purpose the distinction serves, what perception as to unfair treatment it might create in immigrant/migrant communities in New Zealand, and whether on balance it is reasonable.

Additional criteria for the issue of intelligence warrants

Clause 57(a) – application of the criterion of "necessity"

4.28 Clause 57(a) sets out "additional" criteria for the issue of intelligence warrants. It provides that a warrant may issue only if the proposed activity is "necessary" to:

(a) perform an agency function;

(b) test, maintain or develop capability; or

(c) train employees to perform agency functions.

4.29 The threshold test of "necessity" is high. Doubtless this reflects the purpose of authorising otherwise unlawful activity.

4.30 Assessing "necessity" in terms of agency function is problematic.

4.31 The agencies' functions are to:

(a) collect, analyse and provide intelligence (clause 13);

(b) provide protective security services, advice and assistance (clause 14); and

(c) co-operate with and assist (a) each other, NZ Police and NZDF (clause 16) and (b) any other entity in response to threats to human life or safety (clause 17).

4.32 These broad functions must be exercised in furtherance of agency objectives to "contribute to" (i) the protection of national security, (ii) the international relations and well-being of New Zealand and (iii) the economic well-being of New Zealand.

[11] Report of the Attorney-General under the New Zealand Bill of Rights Act 1990 on the Transfer (Foreign Ownership of Land Register) Amendment Bill (4 September 2016) at [11].

4.33 Although seemingly a high threshold, it is difficult to see how the "necessity" test can be strictly applied. It is unlikely that any particular activity could be said to be truly "necessary" for the performance of an agency's intelligence gathering function. Rather, the test will likely be whether the activity is necessary to gather the intelligence in question. In other words, the test would stand to be met simply if the intelligence is not publicly available (or otherwise available through lawful means).

4.34 The Law Society considers the "necessity" criterion to be only a very limited check upon the authorisation of otherwise unlawful activity.

Clause 57(b) – (e): The "additional" criteria more generally and the absence of application requirements

4.35 The remaining "additional" criteria are essential in terms of ensuring that authorised activity is appropriate. The remaining additional criteria would be met where the issuer is "satisfied" of the following:

(a) the proposed activity is proportionate to the purpose for which it is to be carried out (clause 57(b));

(b) the purpose of the warrant cannot be reasonably achieved by a less intrusive means (clause 57(c));

(c) there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the warrant beyond that essential to the proper performance of the requesting agency's function (clause 57(d)); and

(d) there are satisfactory arrangements in place to ensure that any information collected in reliance on the warrant will be retained, used, and disclosed only in accordance with this Act or any other enactment (clause 57(e)).

4.36 In order for these criteria to be properly considered, the activity for which authorisation is sought must be properly particularised. This is also important in supporting the Inspector-General's function of reviewing not only the issuing of authorisations but the carrying out of authorised activity (clause 121(1)(f)).

4.37 The Bill would require warrants to state "the particular activity or activities authorised to be carried out" (clause 61(f)). The application for authorisation should also be properly particularised. That would mean that particulars are recorded in cases where a warrant is not issued. In addition, as a practical matter the particulars included in warrants will likely be based on information provided in the application documents.

4.38 The Directors-General will be best-placed to particularise activities requiring to be authorised. Their representations on warrant applications ought to be readily reviewable by the Inspector-General whether a warrant issues or not.

4.39 The Bill does not propose any express requirements for warrant applications. Currently, by contrast:

(a) the Director of GCSB must apply "in writing" for authorisations (section 15A of the GCSB Act); and

(b) warrants authorising SIS activity may issue only if the Minister is satisfied "on evidence on oath given by the applicant for the warrant" that the relevant criteria are met (section 4A(2) of the New Zealand Security Intelligence Service Act 1969 (**NZSIS Act**)).

4.40 The absence of such requirements in the Bill probably reflects the Bill's accommodation of "urgent" warrants. Applicants for "urgent" warrants may be "excused" from "putting all or any part of the application in writing" (clauses 69 and 70). Arguably this implicitly requires applications otherwise to be in writing.

4.41 The Law Society recommends that the Bill should be amended to expressly require applications to:

(a) be in writing;

(b) particularise the scope of the proposed activities; and

(c) address all matters relevant to the statutory criteria for warranting.

4.42 This will both:

(a) support informed decision-making; and

(b) allow the Inspector-General to meaningfully exercise her review function, which may extend to reviewing the sufficiency of representations made in support of applications.

Urgent applications and warrants

4.43 The Bill allows for the issuing of warrants in "situations of urgency", defined in clause 47 as where:

(a) "there is an imminent threat to the life or safety of any person"; or

(b) delay in applying in the usual way "is likely to materially prejudice the protection of New Zealand's national security".

4.44 In such situations, the Attorney-General and a Commissioner of Intelligence Warrants (or, if the Attorney-General considers it "necessary", the Attorney-General alone) may allow an application for a Type 1 warrant to be made orally, such as over the phone or in person (clause 69). Urgent applications may also be made to the Attorney-General for Type 2 warrants (clause 70). Reasons for the urgent issue of a warrant must be recorded "as soon as possible" (clause 71).

4.45 Urgent Type 1 warrants are "revoked by operation of law" after 48 hours unless an ordinary application for issue has been made within that time, in which case the Attorney-General and a Commissioner of Intelligence Warrants may "confirm" an urgent warrant as a Type 1 warrant or revoke it (clause 72). Parallel provisions apply to urgent Type 2 warrants (clause 73).

4.46 The issuing of any urgent warrants must be referred to the Inspector-General for review as soon as practicable after issue (clause 75).

4.47 The Law Society appreciates that the capabilities of GCSB and SIS might be urgently required to preserve human life or to protect national security. The requirement of "material" prejudice to the protection of national security is likely intended to posit a suitably high threshold for urgent issue of warrants. However, effects upon national security are likely to sit along a continuum of "materiality". What is required is the identification of a point along that continuum, such as through the use of modifiers such as "significant" or "serious".

4.48 For this reason, the threshold of "material" prejudice is inadequate, particularly as a threshold allowing the relaxation of controls over the authorisation of unlawful activity.

4.49 The Law Society supports the requirement for mandatory reporting of urgent warrants to the Inspector-General. This will ensure real-time oversight.

"Very urgent" authorisations

4.50 Where clause 77(1) applies, a Director-General may "authorise" the carrying out of otherwise unlawful activity for which a warrant would be required.

4.51 Clause 77(1) applies if:

(a) an application for the urgent issue of an intelligence warrant would otherwise need to be made; but

(b) the delay in making that application would defeat the purpose of obtaining the warrant.

4.52 Under clauses 78 and 79, such authorisations must be reported immediately to, and may be revoked by either:

(a) the Attorney-General and the Chief Commissioner of Intelligence Warrants (Type 1 warrants); or

(b) the Attorney-General solely (Type 2 warrants).

4.53 Authorisations have the effect of warrants for 24 hours unless an application for a warrant has been made within that time, in which case they will be revoked if a warrant actually issues.

4.54 The Bill should provide that authorisations are revoked either upon the expiration of 24 hours or upon the determination of any subsequent application for a warrant, regardless of whether a warrant actually issues. If activity is not warrantable, it should not be authorised.

4.55 Clause 77(1) does not require a Director-General to be "satisfied" of the requisite urgency. Rather, it is expressed as applying only if such urgency actually exists. This has ramifications for persons acting under authorisations because immunities apply only to the carrying out of authorised activity (clause 88(1)(a) requires a reasonable belief that the act was necessary). It is unsatisfactory for the Bill to permit of uncertainty as to whether the clause 77(1) conditions are met.

4.56 The test itself is also unsatisfactory. As noted:

(a) warrants may issue only if particular "additional" criteria apply; and

(b) these criteria require consideration of issues of proportionality and sufficiency of controls over the proposed activity itself.

4.57 By contrast, the clause 77(1) condition that "delay in making that application would defeat the purpose of obtaining the warrant" requires nothing in terms of justification for the proposed activity. Such a "purpose" could be significant or insignificant. Under the Bill, the only question is whether a delay in seeking a warrant would defeat it.

4.58 The Law Society accepts that there may be situations in which the effects of a delay in seeking even an urgent warrant will be significant. However, the power of Directors-General to themselves authorise otherwise unlawful activity should be limited to such situations.

Clause 91 – retention of incidentally obtained information

4.59 Intelligence activities, by their nature, often involve incidental collection of information. For instance, the information may relate to third parties who are not associated with the reason for which an individual is under surveillance: they simply happen to be in a particular place at

a particular time. Interception of communications, and visual and audio surveillance raise particular issues in this regard.

4.60 It is therefore appropriate that the Bill should place limits on the retention and use of incidentally obtained information, to help to avoid unintended impacts, especially on third parties. Clause 91 is designed to offer this protection.

4.61 However, the clause is arguably broader than it needs to be in two respects.

4.62 First, clause 91 allows for retention and disclosure of incidentally obtained intelligence to a wide group of agencies, including "any public authority (whether in New Zealand or overseas) that the Director-General considers should receive the information." The term "public authority" is not defined. It provides scope for uncertainty.

4.63 This would be less problematic if the purposes for which the information can be retained and disclosed were more limited. However, "preventing and detecting serious crime in New Zealand or any other country" covers a very broad class of offences. "Serious crime" is defined in clause 47 as relating to offences that are "punishable by 2 or more years' imprisonment" (or that would attract that potential sentence if they were committed in New Zealand). The definition is taken from the GCSB Act. It includes offences such as a conversion of a vehicle or other conveyance (section 226 of the Crimes Act) and conspiring to prevent collection of rates or taxes (section 309 of the Crimes Act).

4.64 In light of the important privacy rights that are protected by clause 91, the Law Society submits that the threshold for serious crime is too low. The threshold for serious crime represented in the information sharing agreement between Inland Revenue and NZ Police of "an offence that is punishable by a term of imprisonment of 4 years or more" would be more appropriate. Covering offences at the higher end of the spectrum of seriousness would also be more in line with the other interests protected by clause 91(3)(b), (c) and (d) (preventing threats to life, the security or defence of New Zealand, etc).

5 Part 5: Accessing information held by other agencies

<u>Accessing information held by other agencies – should not be available in relation to "economic well-being"</u>

5.1 The provisions relating to accessing information held by other agencies in Part 5 are a welcome clarification of the law. In particular, the mechanism requiring the intelligence agencies to enter into direct access agreements – with appropriate protections for personal privacy and consultation with the Privacy Commissioner – appear to be a pragmatic and efficient, but also protective, way to fulfil legitimate intelligence functions.

5.2 However, the Law Society has a general concern in relation to the defined objective for the intelligence agencies in clause 11(b) and (c), and reflected elsewhere in the legislation: that is, that the intelligence agencies are to contribute to "the well-being of New Zealand" and "the economic well-being of New Zealand". The problems with having an objective expressed in such broad terms become particularly apparent when considering what personal information the intelligence agencies will be able to source from other agencies, either by request or by direct access.

5.3 The terms "well-being" and "economic well-being" are reflected in the existing legislation, but their meaning is unclear and the Bill does not provide clarification. Many actions can be

justified in the name of "well-being" or "economic well-being", not all of them necessarily serious or appropriate for the involvement of the intelligence agencies.

5.4 The key threats to New Zealand's economy are already recognised in the definition of "national security" in clause 5 (quality of life; unlawful acts or foreign interference that may cause serious damage to New Zealand's economic security; threats or potential threats to the integrity of information or infrastructure of critical importance to New Zealand). It is not plain that the sweeping powers in the Bill should apply to all lesser economic threats.

5.5 For example, many of the privacy-invasive activities of the intelligence agencies are permissible if they are acting in accordance with their functions or powers. It is questionable how meaningful some of the privacy protections in the Bill are (including the protections in Part 5) if the intelligence agencies are acting in pursuit of such potentially broad objectives as "well-being" or "economic well-being".

5.6 The Law Society therefore recommends that the Bill should either clearly define "well-being" and "economic well-being", or restrict the ambit of what the intelligence agencies are allowed to do in pursuit of those objectives. For instance, there may be arguments to allow the GCSB to provide cyber-security expertise for the purposes of that objective, but not to permit direct access to databases held by other agencies other than for the purposes of national security or international relations.

Direct access agreements – include a reporting requirement

5.7 The provisions relating to direct access agreements (clauses 102 – 109) largely reflect provisions and privacy protections that form part of approved information sharing agreements (**AISAs**) under Part 9A of the Privacy Act 1993. This level of clarity and consistency is helpful. The three-year review period in clause 108 is also an important backstop protection.

5.8 However, unlike AISAs, the direct access agreements do not include a reporting requirement (cf section 96S – 96U of the Privacy Act). It would enhance transparency and public confidence if the intelligence agencies were required to publish a summary report of their activities under the direct access agreements every year, and for the Privacy Commissioner and the Inspector-General to be able to seek further information if they require it. The Law Society recommends the Bill be amended accordingly.

Clause 109 – power to amend Schedule 2

5.9 The Law Society considers that the proposed power in clause 109 to amend Schedule 2 by Order in Council is not warranted. It is highly unusual for subordinate legislation to be used to amend primary legislation, as clause 109 would allow. The Bill's departmental disclosure statement does not establish adequate justification for clause 109, merely stating: "This allows for such matters as databases being reconfigured or the holder agency changing."[12]

5.10 What is proposed in clause 109 goes much further than allowing for "database reconfiguration or change in holder agency". Instead, it is broad enough to allow additional databases to be added to Schedule 2. This would have significant implications for individual privacy and is a matter that the Law Society considers is best left to Parliament.

[12] Departmental Disclosure Statement, at [12].

5.11 The Law Society notes that the LAC Guidelines relevantly state:[13]

> **Inconsistency with primary legislation**: Delegated legislation should rarely, if ever, override, suspend or amend primary legislation (empowering provisions that authorise delegated legislation of this nature are sometimes called Henry VIII clauses). … In the rare cases where power of this kind is needed, it must be drafted in the most limited terms possible, must be consistent with and support the provisions of the empowering Act, and must be subject to adequate safeguards. The empowering provision should usually also be limited in time (that is to say, a temporary law), as should any regulations made under the power.

5.12 Accordingly, the Law Society recommends that clause 109 should be removed from the Bill.

6 Part 8: Repeals and amendments

Clauses 257–259 – closed proceedings under the Passports Act 1992

6.1 Clauses 257 – 259 amend sections 29AA and 29AB of the Passports Act 1992, concerning proceedings involving classified security information.

6.2 The Law Society notes that these provisions were criticised by the Law Commission in its recent report concerning national security information in proceedings.[14]

6.3 The Law Commission expressed concerns about the closed procedures where national security information is involved under the Passports Act 1992, in particular that:

(a) there is no procedure for the appointment of a special advocate as exists, for example, in the Telecommunications (Interception Capability and Security) Act 2013;[15] and

(b) the court appears to have little or no power to require further information to be disclosed in a summary to the affected person.[16]

6.4 The Law Commission concluded in relation to the Passports Act provisions that "… there is a real risk that the courts will be unable to ensure proceedings can be fairly heard."[17]

6.5 Section 27(3) of the NZBORA provides that there is a right to bring civil proceedings against the Crown and defend proceedings brought, and that these proceedings must be heard according to law in the same way as proceedings between any two ordinary parties. The default position should be that there must be equal access to both parties to all material placed before the judge. Any departure from this position must be reserved for cases where it is necessary.[18]

6.6 The Law Society does not consider that the limitations in sections 29AA and 29AB of the Passports Act are justified in terms of section 5 of the NZBORA.[19] The Law Society shares the Law Commission's view that these provisions create a risk that proceedings will not be fairly heard.

---

13 Legislation Advisory Committee Guidelines (2014 edition), at [13.5].

14 New Zealand Law Commission *The Crown in Court: A Review of the Crown Proceedings Act and National Security Information* NZLC R 135 (December 2015) [**NZLC R135**].

15 NZLC R135 at [7.9] and fn 118; Telecommunications (Interception Capability and Security) Act 2013, s 105.

16 Ibid.

17 NZLC R135 at [7.9].

18 NZLC R135 at [7.51].

19 Compare Ministry of Justice advice under section 7 to the Attorney-General at [96].

6.7 The Law Society recommends that the Committee take the opportunity afforded by the present Bill to review the Passports Act closed procedure in light of the Law Commission's recommendations. In particular, the Law Society recommends the Committee consider amendments to ensure that:

(a) the issue of withholding information from a party who would otherwise be entitled to receive it, is considered in advance of any substantive proceeding involving the use by the court of such information;

(b) the court is empowered to make the final decision on disclosure of any information that the Crown wishes to use in proceedings; and

(c) a special advocate is appointed in proceedings where information is to be withheld. The special advocate can receive the information and can also take instructions from the affected party and will be expected to vigorously represent the interests of the affected party.

Clauses 263–264 – amendments to the Privacy Act 1993

6.8 Intrusions into privacy are to some extent an inevitable consequence of the activities of intelligence organisations. However, the nature and scope of those intrusions should be strictly limited to what is proportionate in the circumstances. Intrusive activities should also be subject to strong oversight and review.

6.9 The Bill provides some additional protections for personal privacy which the Law Society welcomes. However, in some instances, it is practicable and desirable for the Bill to go further.

Restrict new principle 10 exception to intelligence agencies themselves

6.10 The new exception to principle 11[20] is arguably unnecessary since the existing exceptions to the principles are broad enough to cover disclosures to the intelligence agencies. However, if the exception will assist to remove doubt, the Law Society has no objection to it, particularly as it adds some privacy protection when compared with the existing section 57 of the Privacy Act. There is a greater degree of oversight. Also, it removes the blanket exception for disclosing information to an intelligence agency. Instead, the disclosing agency will need to be able to form a reasonable belief that the disclosure fits the exception. This will not be hard, in most instances, but it requires all agencies to turn their minds to making sure the transaction is justifiable.

6.11 Similarly, the new exception to principle 10[21] makes sense in relation to uses of information by the intelligence agencies themselves. It allows them to act but with a greater degree of oversight and accountability than the current exemption in section 57 allows for.

6.12 However, the Law Society has concerns about the new principle 10 exception as it applies to other agencies. Section 57 currently only allows other agencies to disclose information to

---

20 Explanatory Note to the Bill, at p 27: The exception will allow an agency holding personal information to disclose the information if the agency believes on reasonable grounds that the disclosure is necessary to enable an intelligence and security agency to perform a statutory function.

21 Ibid. This exception will allow an agency holding personal information to use that information for a different purpose from the purpose for which it was obtained if the agency believes on reasonable grounds that the different purpose is necessary to enable an intelligence and security agency to perform a statutory function.

intelligence agencies. It does not allow them to repurpose information to support the intelligence agency activities.

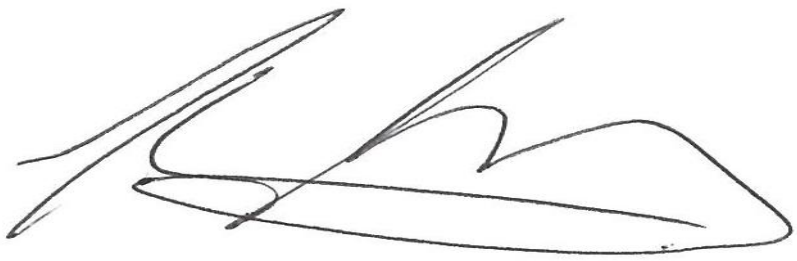
6.13 This is therefore a new and potentially very broad exception to the normal rule that agencies must only use information for the purpose for which they obtained it, or for directly related purposes. It has the capacity to circumvent some of the other protections in the Bill. It would allow for mass processing of information to support intelligence agency activities.

6.14 There is insufficient analysis in the background documentation to justify why the new exception is needed. For instance, it is unclear what other agencies are currently hindered from doing, when the intelligence agencies require their assistance.

6.15 In the absence of a stronger justification for the new exception, the Law Society recommends that other agencies should continue to have to rely on the existing exceptions for maintenance of the law, safety and so on. These exceptions are likely to cover most, if not all, circumstances in which repurposing of information to assist the intelligence agencies is justifiable and proportionate.

7 Conclusion

7.1 The Law Society wishes to be heard in support of its submission.



Kathryn Beck
President
11 October 2016