Privacy Foundation NZ

1 May 2020

Hon Andrew Little

Minister Responsible for the GCSB and the NZSIS

Attention: Lynda Byrne

By email: Lynda.Byrne@dpmc.govt.nz

Dear Minister,

Review of Ministerial Policy Statement on Intelligence Cooperation

Privacy Foundation New Zealand is grateful for the opportunity to comment on the Review of the Ministerial Policy Statement (MPS) on Cooperation of New Zealand Intelligence and Security Agencies (GCSB and NZSIS) with overseas public agencies. Our organisation advocates for the protection of the privacy rights of New Zealanders by providing independent, informed and fair public comment on privacy.

The Foundation notes that the Report of the Inspector General of Intelligence and Security, Cheryl Gwyn, into New Zealand intelligence agencies information sharing and engagement with the CIA in connection with the latter's detention and interrogation program from 2001 to 2009 (The Gwyn Report)[1] finds significant gaps in the existing MPS. These include the clarity of limitations concerning the obtaining or use of information tainted by torture. The Foundation also notes that the Gwyn Report[2] highlighted that the degree to which the agencies interacted with the CIA programme and the safeguards that existed against the agencies' complicity in acts of torture goes to the heart of whether New Zealanders can have confidence the intelligence agencies act lawfully and in accord with this country's international obligations.

The numbered questions on which consultation is sought are addressed by the Foundation in order below. They are, however, prefaced with an important general observation. This is that New Zealand, unlike many other jurisdictions, subjects its intelligence and security agencies

[1] Office of the Inspector-General of Intelligence and *Security Inquiry into possible New Zealand intelligence and security agencies' engagement with the CIA detention and interrogation programme 2001-2009* 31 July 2019.
[2] At [10].

for the most part to the full ambit of its privacy legislation. Thus, the principles contained in the Privacy Act apply to the agencies with only few exceptions.[3] The exceptions are principles 2, 3 and 4 (b).

Whilst information may therefore be obtained by intrusive or unfair methods, the application of principle 4 (a) still ensures that its collection through illegal means is proscribed. Accordingly, the use of information collected through torture would not be permissible as this would contravene New Zealand's domestic and international legal obligations as noted in the Gwyn Report. Although application of privacy legislation to the agencies is commendable, it nonetheless leads to an inevitable tension as the scope and purposes of the agencies is much broader than is contemplated by the privacy legislation. The examples discussed below, if anything, highlight these difficulties. Despite some suggestions being made below as to how such tensions may be attenuated the reality must also be confronted that in some areas, they are simply irreconcilable.

1. **Consistency of the Overseas Cooperation MPS with domestic and international legal obligations**

   The comments made here relate purely to legal obligations in relation to privacy. We note that the Privacy Act is in the process of being modernised with the new Act originally scheduled to be in force by the end of 2020. The enhanced legislation is designed to better align this country's regime with that contained in the European Data Protection Regulation (GDPR). The GDPR prohibits the export of personal information to jurisdictions not regarded as providing adequate protection for individuals in respect to its processing. New Zealand is fortunate to be amongst a handful of jurisdictions accorded adequacy under the GDPR's predecessor but there is no guarantee this will be replicated.

   It is salient to observe, in this context, that the principal reason for the striking down in 2015, by the European Court of Justice, of the scheme through which the export of personal data from the European Union had hitherto been permitted[4] was the revelations made by former United States intelligence operative Edward Snowden. These revealed surveillance of European citizens through the cooperation of companies such as Facebook that were beyond the reach of European data protection regulations.

   The application of New Zealand's updated legislation to such corporations[5] together with the requirement of the intelligence and security agencies to adhere to the legislation thus affords some degree of assurance. Accordingly, paragraphs 53 and 54 of the MPS are reassuring and must be retained. These prohibit the agencies from using the international networks to circumvent the protections contained in New

[3] Intelligence and Security Act 2017 and see Privacy Act 1993, s 57.
[4] The so-called Safe Harbor scheme.
[5] Privacy Bill 2018, cl 3A.

Zealand's regime through using back door conduits as well as requiring adherence to the information privacy principles and an adequacy assessment when information is sent overseas.

Adherence to the Privacy Act, however, consists of more than simply stating that it applies, particularly as it seeks to meet the expectations of enhanced accountability contained in the GDPR. The latter requires demonstrable adherence with assurances such as through documentation, audits and similar measures. This needs to be reflected more accurately in the MPS. For instance, paragraph 50 refers to the NZ agencies clearly articulating the purpose for which information is sought as well as their expectations that no human rights have been contravened in the obtaining of such information. The language of "expectations" ought, in our view, to be replaced with stronger language such as guarantees or certified undertakings.

Further guidance as to the steps that need to be outlined in the MPS to ensure accountability, as well as deficiencies in this regard that have been identified in the Gwyn Report, are set out in paragraph 2 below.

In terms of New Zealand's domestic and international legal obligations we also draw attention to a report issued in 2018, that examined the right to privacy in New Zealand, by Privacy International, a charitable organisation based in the United Kingdom.[6] The report found significant issues with the Intelligence and Security Act 2017 (ISA), which governs the intelligence and security agencies in New Zealand. The ISA sets a lower standard of rigour for approving intelligence warrants targeting foreign persons. Several portions of the MPS emphasise the paramount importance of New Zealand's obligations which are not to be subservient to the intelligence cooperation relationship.[7] However, information shared with partners that has been gathered by targeting foreign persons may lead to non-compliance with New Zealand's international obligations.

2. Whether the Overseas Cooperation MPS, together with operative legislation, provides sufficient clarity as to the guidance, safeguards and restrictions needed for cooperation to occur

As is pointed out in the Gwyn Report the current MPS provides insufficient clarity in several areas about the guidance, safeguards and restrictions it contains relating to overseas cooperation. In our respectful opinion, however, an overarching difficulty is the overly wide delineation of the purposes for which intelligence sharing takes place through simply aligning these with the statutory objectives of the agencies being

[6] Privacy International *Stakeholder Report Universal Periodic Review 32nd session period – New Zealand: The Right to Privacy in New Zealand* (July 2018) <https://privacyinternational.org/sites/default/files/2018-08/UPR_The%20Right%20to%20Privacy%20in%20New%20Zealand.pdf>

[7] For example see MPS paragraphs 20, 32, 35-46.

national security, the international relations and well-being of New Zealand and the economic well-being of New Zealand.[8] The difficulty is made more acute by use of the term "cooperation" which as noted at the outset of the MPS is broader in scope than the sharing of information with partners.

When information sharing takes place, the purposes for this need to be more narrowly circumscribed and be proportionate to their need. The difficulty is illustrated by paragraph 47 of the MPS where a valid purpose is said to be the establishing or maintaining of international relationships that will support the New Zealand agencies. There is a danger here of the means being mistaken for the ends and, furthermore, the paragraph is inconsistent with paragraph 17 of the MPS which contemplates the New Zealand agencies being able to disagree on specific matters with Five Eyes partners without thereby damaging the broader relationship with them.

Reasonableness and proportionality are contemplated by paragraphs 48 and 49 of the MPS and these should be retained. The framing of other paragraphs is problematic, nonetheless. For example, paragraph 46 allows the use of information derived through human rights abuses to be considered for purposes of public safety and the protection of life and property. The Gwyn Report found this unacceptable.[9] Likewise, paragraphs 27 and 28 of the MPS are inconsistent with the Gwyn Report's statement that torture is non-derogable.

These reservations aside, information or data privacy does contain useful techniques that could be adopted within the architecture of the MPS. Such techniques include Privacy Impact Assessments (PIAs), purpose limitations as well as accountability through clear internal policies, training and regular reporting.

For example, the Gwyn Report states that intelligence and security staff had been unaware as to the CIA detention program as well as overseas concerns about it.[10] This exposed the agencies to risks which a comprehensive PIA would have averted.[11] For example, it would have obviated the requirement identified by the Inspector-General whereby information that has been obtained by unlawful means now must be purged.[12] How might such a PIA have been undertaken? General reliance on the human rights record of the country in question would not be enough. Evidence of torture, as noted in the Gwyn Report is rarely likely to exist directly.

Agencies undertaking a PIA ought therefore to engage with human rights civil society organisations and NGOs through in the first place researching their recent public statements and concerns in relation to the area of operation in question. When

[8] MPS at [41].
[9] At [257].
[10] At [95].
[11] At [18.8].
[12] At [185].

necessary this could extend to communicating directly with the organizations themselves. These may include Amnesty International, Human Rights Watch and The United Nations Committee Against Torture. Such consultation ought to be an integral requirement in PIAs.

Clear internal policies and documentation are also crucial. As noted in the Gwyn Report MOUs and written agreements should have Ministerial approval and be available to oversight bodies.[13] Further techniques include segmented cooperation through confining assistance to certain categories of information.[14] There is precedent for this: witness New Zealand's quarantining of nuclear weapons and nuclear powered vessels from its military relationships. Such policies are also consistent with data privacy practices. For instance, it is common to only share certain categories of data or to confine shared data to aggregated and anonymized data. Record keeping is also vital in such instances.[15]

Training as to how to implement human rights obligations, as opposed to generalized awareness of them, is a further ingredient. As noted by the Gwyn Report reliance on individual experience and judgement is insufficient: systemized support and training are necessary pre-requisites.[16] To complement this training, staff must also be well-versed in their right to make a protected disclosure directly to the Inspector-General if that person is aware that the agencies are acting improperly with regard to their co-operation with overseas public authorities.

Inadequacies in supporting and training staff in applicable policies and procedures is referred to at the outset in the Gwyn Report's recommendations.[17] Two major obstacles referred to by the Inspector-General are the so-called "unspoken general rule" and "need to know" principles within intelligence sharing. These are completely inconsistent with transparent and accountable information sharing practices and may be instances of the irreconcilable tensions referred to in the general observations made at the outset of our submission.

One possible solution that is hinted at by the Inspector General is to formalize a systematic process to require monitoring, assessment and evaluation of intelligence sharing. [18] One possible solution to address the obstacles referred to above might be sourced from practices common within international joint ventures. Each member of the venture might nominate a representative on a committee that can sign off any assurances that are needed. The questions, if any, are addressed to the committee and not directly addressed to the partner agency.

---

[13] At [211].
[14] At [239].
[15] At [245] – [249].
[16] At [110].
[17] At [18.5].
[18] At [134].

Finally, regular reporting on compliance with human rights obligations must exist. One way in which this could have been undertaken would be for those deployed to operational theatres to be required to provide regular reports to their Wellington support team on human rights issues arising; Wellington should have required this as a matter of course.

In this context, reference should be made to the rigorous documentation requirements contained in the GDPR which, as stated at the outset, represent international best practice. For example, article 30 of the GDPR requires detailed records of operations that can be made available, if necessary, to supervisory authorities. It is obvious such measures apply with even greater cogency to the intelligence and security agencies. The documentation may include matters such as transfers to third countries and the safeguards in respect to these as well as – where information is disclosed for limited purposes – retention schedules that can be later audited.

3. The level of protection afforded to property and types of property in connection with national security

In addressing this issue Privacy Foundation New Zealand respectfully supports the statements contained in relation to it in the Gwyn Report. We have already pointed to parts of the MPS, such as paragraph 46, that are too wide in their stated objectives. We fully support the Report's recommendation that there is no place for information obtained through human rights breaches for the purposes of protecting property.[19] We also share its concerns that the overly broad nature of the agencies' functions allow them to share information gained through human rights abuses for ill-defined purposes too readily.[20] As we have stated earlier, when personal information is shared it needs to be for narrowly defined purposes and only to the extent necessary for that purpose.

Where personal information has not been obtained through human rights abuses, however, there may be grounds for it to be shared for the purpose of protecting property. That said, we believe it is important to differentiate the types of threats that necessitate the sharing of information: serious economic threats need to be differentiated from latent or contingent risks which may or may not eventuate. Consider, for instance, the recent controversy over the denial of permission for Huawei to provide its 5G technology within New Zealand. This may be contrasted with, say, credible information regarding the deliberate introduction of foot and mouth disease into New Zealand. The latter, if realised, would devastate the agricultural backbone of New Zealand's economy and could be described as an imminent threat as opposed to a latent one.

[19] At [259].
[20] At [260].

Differentiating the types of threats to property according to whether they are imminent threats or are instead contingent risks allows an assessment to occur as to the need for information to be shared or used. A proportionality test should be employed: the measures that are least corrosive for human rights (including privacy) needed to safeguard against the identified risks should be adopted. Where more intrusive measures are needed safeguards must be adopted to guard against excess. The European Union's e Privacy Directive, for instance, allows legislative measures to safeguard public security but these must be accompanied by safeguards including the right to a judicial remedy.

If one were to use the Huawei example as an instance of the contingent risk category any vetting should ideally include transparency: what are the benchmarks against which a network provider's suitability is assessed? This could focus on the assurances needed as to each element in a supply chain, say, and auditing of how a cloud service is accessed or secured. The same requirements would then need to be applied to any bidder for similar service – whether it is a Chinese, United States or French company – in order to ensure there is no targeting or bias involved. Transparency may even involve disclosing the nature of communications received from a Five Eyes partner in relation to an application with the partner's identity masked. Consideration should be given to including such policy guidance in the MPS.

4. The use and disclosure of information likely to have been derived through use of torture

We have already referred to the Inspector-General's statement regarding the non-derogable nature of the obligation.[21] While information derived through the likely use of torture is obviously unusable in legal proceedings its use in operational matters is not proscribed. Privacy Foundation New Zealand strongly believes there is no place for the operational use of such information for legal, moral and practical reasons (as the reliability of such information is questionable). This should be stated unambiguously in the MPS. The best way to discourage the use of torture is to clearly signal to partners that such information, even if received, will not be used in any manner or form whatever. Several paragraphs in the MPS including 27, 28 and 65 accordingly need re-framing.

Should it be necessary for the MPS to include the exceptional circumstances where information derived through torture might be used operationally, then regard should be given to the recommendations in the Gwyn Report that have pointed to the policies and procedures that would need to be adopted should the eventuality occur.[22] These include best practice such as the Ministerial Direction in Canada in relation to its

[21] Gwyn Report at [257].
[22] At [199].

CSIS agency. First, the thresholds for exceptional circumstance (the so-called "ticking bomb" situations) need to be defined as well as the limits on the purposes for which it can be used. Secondly, there must be accountability at a very high level meaning both responsible Ministers and oversight bodies such as the Inspector-General need to be informed in each instance. The metaphor here is a locked fire-door use of which automatically triggers an alarm.

Finally, we wish to address a concern expressed in the Gwyn Report[23] in relation to paragraph 65 of the MPS. This relates to the status of "unsolicited information". We agree there is no place for any such exception and the term itself has been extremely narrowly interpreted by adjudicative bodies. Reference should be made in this context to the decision of the Human Rights Review Tribunal in *Holmes v Housing New Zealand Corporation*[24] which involved the first of the privacy principles in the Privacy Act. The Tribunal adopted a privacy-centric approach to "unsolicited information" through opining that:

…Principle 1 is the overarching privacy principle from which the others flow and further given the need to promote and protect individual privacy, the term "collect" must be given a broad and purposive interpretation. It includes the elements of "gathering together", seeking or acquiring not just receiving.[25]

It further stated that the OECD Privacy Guidelines:

…recognise that collection is not an event (i.e. receipt of the data) but a process for the collection of data. That process must be in place, prior to the receipt of the data and contain the safeguards of 'lawful and fair means" and "knowledge or consent".[26]

We agree with the Inspector-General that any such information received in the context of an ongoing intelligence sharing relationship cannot be said to be "unsolicited".

5. Concluding comments

As has been outlined above, Privacy Foundation New Zealand has considerable concerns about intelligence sharing by the New Zealand intelligence and security agencies with their overseas counterparts. At the crux of many of our concerns is the relatively wide statutory purposes governing the functions of the agencies. Where information sharing is concerned, we believe such purposes must be more narrowly defined, subject to a robust necessity assessment and be proportionate to the needs for which they occur. Lastly, the MPS must pay more than lip service to human rights obligations, such as the obligations contained in the Privacy Act, through requirements for *ex ante* measures such as training and privacy impact assessments as well as *ex post* accountability through documentation and review.

---

[23] At [263].
[24] [2014] NZHRRT 54.
[25] *Ibid* at para 71.
[26] *OECD Guidelines (2013)* at para 75.

Lastly, as Chair I would like to acknowledge the assistance and input of members of the Foundation's Working Group on Surveillance in compiling this submission.

Yours Faithfully,

Gehan Gunasekara

Chair

Privacy Foundation New Zealand

Further information on Privacy Foundation NZ is available on its website: www.privacyfoundation.nz