Public Interest Law Journal of New Zealand

(2025) 12 PILJNZ 113

ARTICLE

Tell Me Your Secrets and I'll Tell You Mine: Foreign Intelligence Sharing and Human Rights Protections in the Intelligence and Security Act 2017

RAPHAEL ZERDA*

Intelligence agencies, including New Zealand's, regularly share intelligence with their foreign counterparts. This practice (foreign intelligence sharing) nets individual agencies with an immense supply of intelligence they would otherwise not have been able to acquire themselves. Yet this same practice could see states complicit in human rights abuses committed by the sharing or receiving parties. With this in mind, the Intelligence and Security Act 2017 bears provisions that aim to protect human rights in the context of foreign intelligence sharing. It also provides for oversight bodies that could oversee such relationships. This article argues that these provisions do provide strong protection for human rights in this context, though its oversight bodies are of mixed efficacy. It begins by outlining foreign intelligence sharing and its implications for human rights and state liability. It then examines the relevant provisions in detail, alongside the Ministerial Policy Statement that governs the practice of foreign intelligence sharing for New Zealand's agencies, and the provided oversight bodies. Ultimately, this article finds that these legislative provisions do effectively protect human rights, in large part because of how they interact with the existing constraints controlling these intelligence sharing relationships. But it also finds that, of the two oversight bodies provided by the Act, only the Inspector-General of Intelligence and Security can provide effective oversight of intelligence agencies' foreign intelligence sharing relationships.

* BA/LLB(Hons), University of Auckland. I would like to thank John Ip for his invaluable assistance during the research for this article. I would also like to thank Milutin Jovic for his support and feedback throughout the drafting of this article.

I Introduction

In September 2024, three academics and activists wrote to the Inspector-General of Intelligence and Security (IGIS).[1] Their letter called for an investigation as to whether intelligence collected by New Zealand's intelligence agencies was being shared with Israel. Even if there is no direct intelligence sharing relationship between them, Israel and New Zealand are both allies of the United States. The letter therefore suggested it was plausible that New Zealand intelligence was being on-shared by our American allies to Israel. This gave rise to worries that such intelligence might aid Israel in prosecuting its invasion of Palestine. New Zealand could well be complicit.

This is just one very recent example of the controversies that can arise from intelligence sharing agreements between two states. Recent history is replete with such occurrences: the Saudi Arabian-led intervention in Yemen received American intelligence support, while drawing condemnation for airstrikes on civilians;[2] a 2017 Nigerian airstrike on a refugee camp was allegedly based on United States intelligence;[3] and the United States continues to share intelligence with Israel in its campaign in Gaza.[4]

Despite this, the sharing of intelligence between the intelligence agencies of two states is unlikely to cease. This practice, which I call "foreign intelligence sharing", is simply too useful. It supplies intelligence agencies with a treasure trove of intelligence from partners, be it in the form of raw data or analysis, in quantities simply unobtainable through unilateral action. New Zealand's agencies have certainly benefited, with the New Zealand Security Intelligence Service (NZSIS) receiving around 170 reports for every one report it shares with its partners.[5]

But foreign intelligence sharing can and does implicate human rights protected by both domestic and international law. The right to privacy comes to mind immediately. Intelligence, after all, often includes personal information.[6] That it is the personal information of terrorist suspects does not diminish its private nature. The right to be free from torture, or cruel, inhuman or degrading punishment is also implicated by these agreements—intelligence shared may have been acquired through torture. Relevant to the examples provided above, foreign intelligence sharing can absolutely be the basis for state responsibility.[7]

---

1 Thomas Coughlan "NZSIS, GCSB: Academics, activists call to investigate intelligence agencies over potential co-operation with Israel's invasion of Gaza" *The New Zealand Herald* (online ed, Auckland, 12 September 2024).

2 Mark Hosenball, Phil Stewart and Warren Strobel "Exclusive: US expands intelligence sharing with Saudis in Yemen operation" (11 April 2015) Reuters <www.reuters.com>.

3 Rachel Nostrant "Congress calls for answers on US role in fatal 2017 Nigerian airstrike" *Military Times* (online ed, Virginia, 14 September 2022).

4 Margaret Brennan "US provided support to Israeli forces in rescue of 4 hostages in Gaza" (8 June 2024) CBS News <www.cbsnews.com>.

5 Michael Cullen and Patsy Reddy *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand* (29 February 2016) at [3.43].

6 Craig Forcese "The collateral casualties of collaboration: The consequences for civil and human rights of transnational intelligence sharing" in Hans Born, Ian Leigh and Aidan Wills (eds) *International Intelligence Cooperation and Accountability* (Taylor & Francis Group, Abingdon (UK), 2011) 72 at 73.

7 Sophie Duroy "The Regulation of Intelligence Cooperation under International Law: A Compliance-Based Theorization" in Arianna Vedaschi and Kim Lane Scheppele (eds) *9/11 and the Rise of Global Anti-Terrorism Law: How the UN Security Council Rules the World* (Cambridge University Press, Cambridge (UK), 2021) 179 at 182.

With this in mind, one hopes that the Intelligence and Security Act 2017 (the Act) provides strong protections for human rights in the context of foreign intelligence sharing. This article argues that the Act does provide robust protections for human rights in the legislative provisions that govern New Zealand's foreign intelligence sharing agreements. It also argues that the oversight mechanisms it provides are of varying quality; one is effective, while the other requires improvement if it is to effectively oversee such agreements.

Part II will discuss foreign intelligence sharing in detail, including what it is, why states engage in it, and the human rights and international law issues it entails. Part III will discuss both the Act's provisions on foreign intelligence sharing and the ability of its oversight mechanisms to oversee the practice, alongside a few recommendations for improvement. Part IV concludes the article.

II What is Foreign Intelligence Sharing?

I will first establish the definitions I am using for "intelligence" and "foreign intelligence sharing". Intelligence is the "collection and analysis of publicly available and secret information with the goal of reducing policymakers' uncertainty about a foreign policy problem".[8] Similarly, intelligence sharing is the practice of a state communicating intelligence it possesses to another.[9]

Foreign intelligence sharing arrangements are agreements between the intelligence agencies of two or more states, to share intelligence collected by each party. I refer to this practice specifically as "foreign intelligence sharing" to distinguish sharing intelligence between states from sharing intelligence between agencies belonging to the same state (as when an intelligence agency shares intelligence with the police or military). This article focuses purely on the former type of intelligence sharing.

These arrangements are flexible in form.[10] In rare cases, they are multilateral and highly formalised—the United Kingdom-United States of America Agreement is the most well-known example of this.[11] More common, however, are bilateral agreements.[12] One such agreement is the Memorandum of Understanding (MOU) between the United States and Israel on the sharing of signals intelligence.[13] Such MOUs set out how intelligence sharing is conducted between the parties.[14] While formalised, these MOUs are unenforceable in court.[15] It is a reasonable inference that the same is also true for

8 James Igoe Walsh "Defection and Hierarchy in International Intelligence Sharing" (2007) 27 Journal of Public Policy 151 at 154 as cited in Forcese, above n 6, at 73.
9 Forcese, above n 6, at 73.
10 Elizabeth Sepper "Democracy, Human Rights, and Intelligence Sharing" (2010) 46 Tex Intl LJ 151 at 156.
11 At 157.
12 At 158.
13 Ashley Deeks "Intelligence Services, Peer Constraints, and the Law" in Zachary K Goldman and Samuel J Rascoff (eds) *Global Intelligence Oversight: Governing Security in the Twenty-First Century* (Oxford University Press, New York, 2016) 3 at 19.
14 Sepper, above n 10, at 158.
15 At 158.

multilateral agreements. Lastly, it is common for bilateral agreements to be informal and uncodified.[16]

A *Why do states engage in foreign intelligence sharing?*

The average person with little knowledge of the field of intelligence would recognise its inherent secrecy. So, one might reasonably ask why intelligence agencies share intelligence at all. Sharing intelligence might, for instance, risk compromising a source—like revealing the presence of a human asset in a terrorist organisation, or the technical capabilities of an agency's spy satellites. Collecting intelligence unilaterally would not. Why run that risk?

Intelligence agencies share information with each other because no single agency has the resources or capacity to unilaterally collect all the intelligence it requires.[17] Policymakers' demand for intelligence frequently outstrips the capacities of the agencies themselves.[18] But it is not just necessity driving this cooperation. Foreign intelligence sharing also has the advantage of enabling intelligence agencies to leverage their peers' advantages.[19] One agency may have access to a network of spy satellites; another may have more linguists and a better understanding of local culture. Mutual exchanges of information would allow both to benefit from each other's strengths. In this way, both agencies acquire information with greater ease than if they had tried to collect it by themselves. In a similar vein, foreign intelligence sharing agreements enable the parties to split the workload. Five Eyes, for instance, "allocates electronic surveillance collection among its members" based on their "geographic proximity to the source".[20]

These benefits lead to intelligence agencies engaging in numerous foreign intelligence sharing arrangements. For instance, by 2005, the Canadian Security Intelligence Service (CSIS) had over 250 intelligence sharing relationships.[21] There is an astounding quantity of intelligence shared through these arrangements. It bears repeating, as an example, that the NZSIS receives around 170 international reports for every report it shares, while the Government Communications Security Bureau (GCSB) receives 99.[22]

Foreign intelligence sharing is also a very useful tool for states seeking to support allies in armed conflict. Such cooperation does not necessarily involve "a large expenditure of people, equipment, and dollars".[23] It may also be more politically viable than direct participation in a conflict.[24] In such a case, intelligence support can aid in targeting for a partner state's military operations.

Lastly, pressure to engage in foreign intelligence sharing can also come from international instruments. Some United Nations Security Council resolutions call on states

16 Philippe Hayez "National oversight of international intelligence cooperation" in Hans Born, Ian Leigh and Aidan Wills (eds) *International Intelligence Cooperation and Accountability* (Taylor & Francis Group, Abingdon, 2011) 151 at 157.

17 Deeks, above n 13, at 6.

18 Richard Barrett and Tom Parker "Acting ethically in the shadows: Intelligence gathering and human rights" in Manfred Nowak and Anne Charbord (eds) *Using Human Rights to Counter Terrorism* (Edward Elgar Publishing, Cheltenham (UK), 2018) 236 at 255–256.

19 Deeks, above n 13, at 6.

20 At 6.

21 Forcese, above n 6, at 76.

22 Cullen and Reddy, above n 5, at [3.43].

23 Jonathan Howard "Sharing Intelligence with Foreign Partners for Lawful, Lethal Purposes" (2018) 226 Mil L Rev 1 at 2.

24 At 4.

to take the necessary steps to prevent terrorist acts, including "provision of early warning to other States by exchange of information".[25] This renders foreign intelligence sharing a "mandatory counter-terrorism obligation".[26] While its practical benefits likely drives much of its practice, such an obligation certainly does not detract from it.

B *Foreign intelligence sharing, human rights, and international law*

With foreign intelligence sharing now defined, and an explanation provided for its practice by states, I will now explore how it touches upon human rights and international law.

(1) The right to privacy

The right to privacy may be implicated by foreign intelligence sharing, given that intelligence will often include personal information. This right is enshrined in the *Universal Declaration of Human Rights* and the International Covenant on Civil and Political Rights (ICCPR).[27] Domestic legislation will often provide some measure of protection for it in different contexts. For instance, the Privacy Act 2020 provides a "framework for protecting an individual's right to privacy of personal information".[28]

Admittedly, the Privacy Act contains provisions that afford intelligence and security matters special treatment.[29] For example, agencies can refuse access to personal information if doing so would prejudice New Zealand's security or defence.[30] Moreover, art 12 of the *Universal Declaration of Human Rights* prohibits interference with the right to privacy only where it is "arbitrary". But the broader concern, that such a right to privacy exists and is protected under domestic and international law, remains.

Foreign intelligence sharing raises the possibility of simply bypassing domestic protections for privacy.[31] Take the following example: Agencies A and B are prohibited by the domestic law of their respective states from spying on their own citizens. They elect to bypass this by spying on each other's citizens and sharing back the reports. The Five Eyes intelligence sharing network has allegedly been used for this purpose.[32] Whether these allegations are true is unclear. The Communication Security Establishment Canada denies it, as intelligence agencies are apt to do in any case.[33]

It may be that agencies are not deliberately using foreign intelligence sharing agreements to bypass domestic privacy protections. Nonetheless, state intelligence agencies likely do receive intelligence on their own citizens.[34] This may happen in the regular course of intelligence sharing.[35] In any case, that agency now has intelligence on a citizen that domestic privacy protections would either have prevented them from getting, or made significantly more difficult to acquire. The protections have been bypassed.

25 SC Res 1373 (2001), art 2(b).
26 Forcese, above n 6, at 75.
27 *Universal Declaration of Human Rights* GA Res 217A (1948), art 12; and International Covenant on Civil and Political Rights 999 UNTS 171 (opened for signature 16 December 1966, entered into force 23 March 1976) [ICCPR], art 17.
28 Privacy Act 2020, s 3(a).
29 Sections 51 and 95.
30 Section 51.
31 Sepper, above n 10, at 173.
32 Forcese, above n 6, at 80.
33 At 80.
34 At 80.
35 At 82.

What is the recipient agency to do with that intelligence, especially if it is pertinent to national security?

(2) The right to be free from torture

Foreign intelligence sharing also implicates the right to be free from torture, or cruel, inhuman or degrading treatment. Much like the right to privacy, this is enshrined in both the *Universal Declaration of Human Rights* and the ICCPR, among other agreements.[36] Domestically, it is protected under s 9 of the New Zealand Bill of Rights Act 1990.

Intelligence sharing agreements can be formed with agencies known for engaging in torture. The recipient agency then runs the risk that intelligence shared with them has been acquired through torture.[37] As Craig Forcese notes, real world intelligence agencies do not always know the conditions under which prisoners are kept, or how interrogations are conducted by their partners.[38]

In other cases, however, intelligence agencies are aware that a partner agency practices torture. They may still seek out their cooperation, for instance, by sending questions to be asked in interrogation, with the answers being shared back to them. But the simple act of sending questions for interrogation can be interpreted by interrogators as proof that individuals detained are terrorists. In 2002, Maher Arar, an innocent Canadian citizen, was rendered from the United States to Syria, into the hands of Syrian Military Intelligence (SMI), who interrogated and tortured him.[39] The Royal Canadian Mounted Police (RCMP) sent questions to be asked of Arar, despite being advised that such questions would be taken as proof of his terrorist status. SMI proceeded to torture him on that basis.[40] As such, the demand for intelligence from partners can lead to the commission of serious human rights violations.

An intelligence agency sharing intelligence with a partner would also do well to give sharing more thought. Shared intelligence could, intentionally or not, lead to the torture of individuals it identifies. Indeed, it was information shared by the RCMP to American authorities that led to Arar's rendition and torture in the first place.[41] Concerns such as this have seen the United Kingdom's intelligence agencies procure "humane treatment assurances" before providing intelligence that could be used, for instance, in someone's capture and torture.[42]

(3) State liability

Foreign intelligence sharing that results in human rights violations may also render states liable under the *Draft articles on Responsibility of States for Internationally Wrongful Acts* (*Draft Articles*).[43] That a partner state committed the human rights breach does not exempt

36 *Universal Declaration of Human Rights*, art 5; and ICCPR, art 7.
37 Forcese, above n 6, at 87.
38 At 88.
39 Sepper, above n 10, at 179.
40 At 179.
41 Forcese, above n 6, at 72.
42 Deeks, above n 13, at 18.
43 *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries* [2001] vol 2, pt 2 YILC 26 [*State Responsibility*] at 65.

the sharing partner from responsibility. Chapter IV of the *Draft Articles* would certainly capture it. Article 16 will most likely be engaged:[44]

> A State which aids or assists another State in the commission of an internationally wrongful act by the latter is internationally responsible for doing so if:
>
> a) that State does so with knowledge of the circumstances of the internationally wrongful act; and
>
> b) the act would be internationally wrongful if committed by that State.

Of course, the *Draft Articles* are not a binding treaty. But many of its articles do reflect customary international law. For instance, art 16.[45] The articles are, in that sense, enforced, with liability determined in such forums as the International Court of Justice (ICJ).

As an example, Agency A shares intelligence with Agency B. The intelligence is the location of a high-profile terrorist. The parent states of both agencies are bound by international obligations not to engage in torture. Agency A knows that Agency B practices torture. They know that if Agency B, acting on the intelligence, captures the terrorist, he will likely be tortured. Agency B does exactly that.

Sharing intelligence that significantly contributes to the commission of an internationally wrongful act would certainly fall under "aid[ing] or assist[ing]".[46] Agency A, in our example, aided Agency B through sharing intelligence, and they did so while knowing that it would likely lead to the terrorist's torture; the first element is satisfied. So is the second: the torture would still be an internationally wrongful act had Agency A (and so their parent state) committed it. Responsibility can clearly be established under art 16.

The commentary to the *Draft Articles* speaks of intention as a "second requirement", despite the article itself saying that only "knowledge" is required.[47] A state will only be responsible where it "intended, by the aid or assistance given, to facilitate the occurrence of the wrongful conduct".[48] Whether intention is, in fact, a requirement, has yet to be determined by thte ICJ.

If the ICJ does address the question of intention, it is unlikely to be in the context of a foreign intelligence sharing case. There is some doubt as to the suitability of the *Draft Articles* for the intelligence context. The *Draft Articles*, as Sophie Duroy notes, depend on states to hold their peers accountable.[49] But can a small state really be expected to hold a more powerful one accountable? Power dynamics aside, no state has ever held another to account under the *Draft Articles* in the context of intelligence cooperation.[50] To do so would risk being seen as an unreliable partner and being excluded from the flow of intelligence.[51]

---

44 At 66–67.

45 *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Judgment)* [2007] ICJ Rep 43 at 217.

46 *State Responsibility*, above n 43, at 65.

47 At 66.

48 At 66.

49 Duroy, above n 7, at 182.

50 At 182.

51 Sophie Duroy "Remedying Violations of Human Dignity and Security: State Accountability for Counterterrorism Intelligence Cooperation" in Christophe Paulussen and Martin Scheinin (eds) *Human Dignity and Human Security in Times of Terrorism* (TMC Asser Press, The Hague, 2020) 123 at 134.

That does not mean a state does not risk being held accountable for the human rights violations arising from its foreign intelligence sharing activities. States can be held accountable through international forums where the state has already consented to the forum's authority.[52] These forums may not always be courts, but being held liable for human rights violations can still bear reputational costs.[53]

United Nations expert bodies serve as one set of forums. Indeed, they have already handled complaints of human rights violations in the context of intelligence cooperation. Ahmed Agiza and Mohamed Alzery complained to the United Nations Committee Against Torture (UNCAT) and the United Nations Human Rights Committee respectively.[54] In 2001, the two were summarily expelled from Sweden—arrested, mistreated at Bromma airport by United States agents, and rendered to Egypt via a Central Intelligence Agency (CIA) plane. Egyptian intelligence proceeded to take both into custody, where they were tortured.[55]

Four years later, UNCAT found that Sweden had breached art 3 of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment when it refouled Agiza to Egypt.[56] Egypt was known to engage in torture; the odds of Agiza being tortured in Egyptian custody (as indeed eventuated) were high. UNCAT found that the diplomatic assurances sought by Sweden were insufficient to guard against this risk of torture for lack of actual enforcement mechanisms.[57] The United Nations Human Rights Committee also found Sweden to have breached art 7 of the ICCPR, among other violations, in rendering Alzery to Egypt.[58] Moreover, they found that Alzery's mistreatment at Bromma airport was properly imputable to Sweden—state officials were present, and, in doing nothing, effectively acquiesced.[59] That itself was a breach of art 7.

Another example is the European Court of Human Rights. *Al Nashiri v Poland* and *Abu Zubaydah v Lithuania* saw the two complainants held in CIA black sites in Poland.[60] Consequently, the Court held Poland responsible for the complainants' arbitrary detention in its territory and their subsequent transfer. However, it also explicitly found the United States to be responsible for torture and held Poland responsible for its acquiescence.[61] As Duroy notes, this makes it clear that responsibility can arise "out of intelligence cooperation".[62]

These examples fall under the broader umbrella of intelligence cooperation, of which foreign intelligence sharing is simply one form. I see no reason to think that the same mechanisms would not work in the narrower foreign context.

52 At 136.
53 At 136.
54 At 140.
55 At 140.
56 *Ahmed Hussein Mustafa Kamil Agiza v Sweden* CAT/C/34/D/233/2003, 24 May 2005 at [13.8].
57 At [13.4].
58 *Mohammed Alzery v Sweden* CCPR/C/88/D/1416/2005, 10 November 2006 at [11.8].
59 At [11.6].
60 *Al Nashiri v Poland* ECHR 28761/11, 24 July 2014; and *Abu Zubaydah v Lithuania* ECHR 46454/11, 31 May 2018. See also Duroy, above n 51, at 143–144.
61 At 144.
62 At 144.

III The Intelligence and Security Act 2017

Given the potentially immense implications on human rights borne by the practice of foreign intelligence sharing, one would hope that the Act provides adequate protections and oversight. However, while the protections themselves are robust, the oversight mechanisms leave something to be desired.

In this section, I will first outline how the Act provides for foreign intelligence sharing and the protections for human rights within the legislation itself. I will then briefly review relevant parts of the associated Ministerial Policy Statement (MPS) and the relevant Joint Policy Statement (JPS) of the NZSIS and GCSB.

Afterwards, I will analyse these sections to explain that their strength arises from their interaction with peer constraints: the main mechanism controlling foreign intelligence sharing relationships. I will also examine their weaknesses and then consider the Act's provided oversight mechanisms and their interaction with foreign intelligence sharing. I will conclude with a few recommendations to improve the protections in the Act.

A *How the Act regulates foreign intelligence sharing*

(1) Legislative constraints

To begin with, the Act provides that one of the functions of an intelligence and security agency is the provision of intelligence and analysis.[63] Such may be provided to persons overseas where it is authorised by the Minister responsible for either the NZSIS or GCSB.[64] As this is usually the same person, I will refer to them simply as the Minister responsible. But before granting such authorisation, that Minister must be satisfied that the relevant agency "will be acting in accordance with New Zealand law and all human rights obligations recognised by New Zealand law".[65]

This statutory safeguard supplements more general duties. The NZSIS and GCSB must abide by New Zealand's laws and human rights obligations and act "in a manner that facilitates effective democratic oversight".[66] Moreover, the Director-General of a given intelligence agency must take "all reasonable steps" to ensure that any foreign cooperation is done in line with New Zealand's laws and human rights obligations.[67]

(2) Ministerial Policy Statement

The Minister responsible must also issue an MPS providing guidance on cooperation with overseas public authorities, including the sharing of intelligence.[68] As it is the same Minister responsible for both agencies, this MPS does not differ between the NZSIS and GCSB. The Director-General and employees of each intelligence agency are required to act with regard to these Ministerial Policy Statements.[69]

The most recent MPS on cooperating with overseas public authorities was issued in March 2025. It defines overseas public authorities as "a foreign person or body that

63 Intelligence and Security Act 2017, s 10(1)(a)–(b).
64 Section 10(1)(b)(iii).
65 Section 10(3).
66 Section 17(d).
67 Section 18.
68 Section 207(1).
69 Section 209.

performs or exercises any public function, duty, or power conferred on that person or body by or under law".[70] Ministerial authorisation can be sought on a "case-by-case" or "standing" basis.[71] Authorisations under the latter are subject to regular reviews for consistency with the principles of the MPS. Such reviews can be triggered by an increased risk that the cooperation will bring about breaches of New Zealand's laws and human rights obligations.[72] In any case, the Minister responsible must be provided the following information in any request for authorisation: the purpose of the intelligence sharing, the particular risks involved and their odds of eventuating, and measures to mitigate those risks.[73]

While the MPS provides several principles that an intelligence sharing agreement must adhere to, I will focus primarily on the principle of respect for human rights, and the MPS's directions on the treatment of intelligence obtained through breaches of human rights. The MPS requires the Directors-General of the GCSB and the NZSIS to ensure their respective agencies are aware of the potential risks of cooperation with overseas public authorities.[74] To further this, the MPS provides for a risk assessment framework for the GCSB and NZSIS to apply in assessing the likelihood that cooperation with an overseas public authority carries a real risk of human rights violations. The MPS, however, does not expect this framework to be applied in every instance of foreign intelligence sharing. Instead, it leaves the "when" of its application to be determined by the agencies.[75]

The human rights risk assessment (HRRA) framework involves examining:[76]

- the general risk arising from cooperating with a given state or public authority;
- the specific risks arising from the proposed cooperation;
- whether any risks identified can be mitigated; and
- if there remains a real risk of significantly contributing to a human rights violation.

Such would require cooperation to either be denied or referred to the Minister responsible. If it is referred to the Minister, the IGIS must be notified.[77] The agency must also provide the Minister with its analysis of these steps and a statement on the purpose of the proposed cooperation.

The MPS emphasises that New Zealand strongly opposes both the use of torture and the death penalty, which it describes as "the ultimate form of cruel, inhuman and degrading treatment".[78] New Zealand is not to commit or be complicit in the commission of torture, nor cooperate where such cooperation will lead to the imposition of the death penalty. Furthermore, the MPS forbids the NZSIS and GCSB from requesting or using intelligence where they know or assess that there is a real risk it was obtained through serious human rights breaches including torture.[79] Where the agencies receive unsolicited intelligence gained through such breaches, the MPS directs them not to act in a way that would further contribute to such violations.[80]

---

70 Judith Collins *Ministerial Policy Statement: Cooperating with overseas public authorities* (1 March 2025) at 1.
71 At [5].
72 At [6].
73 At [19] and appendix 1.
74 At [19].
75 At [20].
76 At [20] and appendix 1.
77 At [20].
78 At [14]–[15].
79 At [21].
80 At [22].

That does not mean that the intelligence cannot be used in any capacity. However, it can only be used where it "is necessary to prevent loss of life, significant personal injury or a threat to critical national infrastructure".[81] Nonetheless, this exception is unlikely to be engaged for reasons I will discuss later.

(3) Joint Policy Statement

The NZSIS and GCSB outline how they implement the Act's and MPS's requirements on foreign intelligence sharing in a JPS. This JPS on the management of human rights risks in overseas cooperation, however, is only publicly available as a three-page summary. Nevertheless, one aspect of it is notable.

Per the JPS, agencies can request that the Minister responsible grant "approved party status" to another party, separate from a ministerial authorisation.[82] The JPS states that such a party should have a human rights situation "broadly comparable to New Zealand's".[83] This granted status allows for cooperation without needing to perform an HRRA.[84] However, the summary goes into little detail as to this approved party status, or the criteria for granting it.

In sum, the agencies must request ministerial authorisation under s 10 of the Act to cooperate with an overseas public authority. Where it is granted (for instance, on a standing basis), they may cooperate and share intelligence with that partner.[85] Depending on the intelligence sharing being conducted, an HRRA may need to be taken. This could result in the Minister disallowing intelligence sharing if there is a real risk of significantly contributing to a human rights violation. But if that partner also has approved party status, then HRRAs are not required, barring exceptions like a breach of human rights.[86]

B *Analysis*

While one would reasonably assume that the empowering legislation of an intelligence agency would address the practice of foreign intelligence sharing, this is not always the case.[87] In some states, such legislation does not mention the practice at all—Philippe Hayez gives the German Bundesnachrichtendienst (Federal Intelligence Service) as one example.[88] In other states, such as Denmark, legislation does allow for such cooperation.[89] New Zealand has attempted to incorporate human rights protections into its intelligence cooperation. Few others have tried to similarly specify conditions, claims Hayez.[90]

Of course, the presence of legislative protections for human rights is the bare minimum expected. One might question the efficacy of the legislative provisions discussed

81 At [23].
82 Government Communications Security Bureau and New Zealand Security Intelligence Service *Summary: Joint Policy Statement on Management of Human Rights Risks in Overseas Cooperation* (10 January 2023) at [6].
83 At [6].
84 At [6].
85 Brendan Horsley *Review of NZSIS and GCSB Human Rights Risk Assessments* (Inspector-General of Intelligence and Security, July 2024) at [11.2].
86 At [11.3].
87 Hayez, above n 16, at 158.
88 At 158.
89 At 159.
90 At 159.

earlier, alongside the MPS and JPS, in constraining foreign intelligence sharing so as to protect human rights.

I argue that these provisions do, in fact, provide robust protection for human rights. To begin with, there is presently a reasonably strong culture of compliance within the agencies. Moreover, I argue that their efficacy is further bolstered by their interactions with another important mechanism of controlling foreign intelligence relationships: peer constraints.

(1) Culture of compliance

Legislative constraints like the requirement for ministerial authorisation, and the existence of duties upon the agencies, can be effective checks on their behaviour.[91] This is dependent on there being a strong culture of compliance. The *Taumaru: Protecting Aotearoa New Zealand as a free, open and democratic society* (*Taumaru*) report finds that the NZSIS and GCSB do have such cultures.[92] Additionally, we can note that over a three-year period, the agencies undertook "approximately 1,500 human rights risk assessments" concerning foreign intelligence sharing.[93] This figure not only illustrates the scale of New Zealand's intelligence sharing involvement, but also indicates compliance with the MPS on the part of the intelligence agencies.

But there are other reasons to believe that such a culture of compliance exists, or at least should exist. Duroy argues that the instances of states being held accountable for human rights violations arising from intelligence cooperation have "changed the payoffs and costs".[94] Demonstrated willingness to hold states accountable has raised the perceived risk of a state being held accountable. Where it does, it can "affect a state's reputation".[95] As such, the greater risk of being held accountable in intelligence cooperation has increased the cost of noncompliance with international law, making compliance a more attractive option.

Additionally, the leaks of recent years (for example, involving Edward Snowden, Chelsea Manning and Reality Winner) have demonstrated to intelligence agencies that "nothing remains secret forever in today's digital world".[96] Even outside of leaks, private actors have uncovered intelligence activities and disseminated their discoveries through the internet.[97] Ashley Deeks offers the example of Stuxnet, a computer worm that destroyed Iranian nuclear centrifuges, which was discovered only when it spread outside of Iran.

Lastly, respect for human rights is part of effective counterterrorism. Its violation can be counterproductive. Torture is simply not an effective method of collecting intelligence. Intelligence sourced from tortured prisoners is unreliable, and acting on it can see innocent people "detained and mistreated".[98] To illustrate, the French practised torture in the Algerian war against captured members of the Front de Liberation Nationale (FLN). Even when the prisoners talked, it was "still difficult to separate the wheat from the

91 Terence Arnold and Matanuku Mahuika *Taumaru: Protecting Aotearoa New Zealand as a free, open and democratic society* (Ministry of Justice, 31 January 2023) at [4.8].
92 At [4.13].
93 At [10.80].
94 Duroy, above n 7, at 198.
95 At 184.
96 At 193.
97 Deeks, above n 13, at 9.
98 Sepper, above n 10, at 181.

chaff".[99] FLN members were also instructed to give their interrogators the names and locations of members of the Mouvement National Algerien. Those moderate members were tortured and radicalised as a result.[100]

These violations of human rights also provide material for terrorist organisations to use in their propaganda. Does it not stoke sympathy and anger when the so-called "counterterrorist" occupiers are barbarically torturing helpless prisoners? Indeed, Al Qaeda benefited in this exact way when the United States adopted its "enhanced interrogation techniques".[101] Putting it in the language of Duroy's payoffs and costs, violating human rights bears greater costs than the benefits it confers. Assuming, then, that the NZSIS and GCSB wish to protect New Zealand's security, it is in their best interest to protect human rights.

With all this in mind, there is good reason to think that New Zealand's intelligence agencies have at least a reasonably strong culture of compliance. And this makes the legislative constraints effective in controlling their behaviours regarding foreign intelligence sharing.

(2) Peer constraints

A key strength of these provisions, however, is in their interaction with the peer constraints controlling foreign intelligence sharing relationships.[102] These constraints have two sources.

The first source is exogenous. Domestic law binding upon peer agencies is just one example, albeit my focus for its direct relevance to the Act. I will largely focus on what Deeks calls the "informal mechanisms" of peer constraints.[103]

The second is endogenous to the agencies. It is a "shared professional ethos".[104] Intelligence professionals identify with each other due to "[s]hared practices, normative principles, and evaluative criteria".[105] As such, the profession has developed norms that guide their behaviour, which also serve to constrain that of their partners in foreign intelligence sharing relationships.

(3) Exogenously sourced peer constraints

While Deeks identifies other informal mechanisms through which peer agencies constrain intelligence cooperation, I primarily focus on what Deeks calls "Peer Domestic Legal Constraints".[106] I do this because the previously discussed provisions of the Act primarily fall under this category.

The basic idea behind these constraints in an intelligence sharing agreement, is that one agency will impose a condition on the cooperation stemming from its legal obligations. These conditions could include restrictions on the manner in which shared intelligence can be used. If the partner agency enters into the agreement, then the legal obligations binding upon the constraining agency have now also indirectly constrained the actions of the

99 Barrett and Parker, above n 18, at 248.
100 At 248.
101 At 251.
102 Deeks, above n 13, at 4.
103 At 20.
104 Sepper, above n 10, at 153.
105 At 159.
106 Deeks, above n 13, at 20.

partner. In this way, peer constraints can result in "increased individual rights protections".[107]

This is clearly relevant to the provisions of the Act. They place our agencies as constraining partners in a prospective foreign intelligence sharing relationship. Our agencies wish to abide by their obligations under the Act. Therefore, they will condition cooperation on the inclusion of rights-enhancing constraints if necessary. Indeed, as part of both a request for ministerial authorisation and an HRRA, they must consider measures to mitigate human rights risks.[108] This results in increased protections for human rights in the context of foreign intelligence sharing.

Consider the following example. The Act obliges the agencies to act in accordance with New Zealand law and human rights obligations.[109] The NZSIS wishes to abide by this duty. It performs an HRRA on an authorised partner for an intelligence sharing agreement. They find that partner agency to have a reputation for torturing terrorist suspects. Consequently, they impose the following conditions on the agreement: the partner agency must agree not to torture any terrorist suspects arrested as a result of the shared intelligence; and must allow for the presence of an NZSIS observer during interrogations. The partner agrees.

Moreover, the requirement of ministerial authorisation under s 10(1)(b)(iii) of the Act serves as a "statutory safeguard" that ensures the Minister responsible can review the risks of foreign intelligence sharing.[110] The Minister, then, is well-placed to pressure agencies to include these rights-enhancing constraints by leveraging their ability to deny authorisation. Indeed, they are obliged to deny that authorisation if they are not satisfied.[111] Similarly, the Directors-General of the NZSIS and GCSB can pressure their respective agencies to include such rights-enhancing constraints, by shaping internal policy for operations. Section 18(b) of the Act obliges them to do so.

Combined, there are three sources of pressure bearing upon the agencies to include rights-enhancing constraints where necessary in their foreign intelligence sharing relationships: the agencies themselves (due to their general duty), their Directors-General (due to their specific duty) and the Minister responsible.

Of course, as Deeks points out, this all depends on the compliance of an agency with the legislative constraints placed upon it.[112] If an agency, bound by a duty to act in accordance with human rights obligations, elects to ignore it, the effect is two-fold: they will not be constrained by the duty, and they will not constrain others as a result of the duty. But, as I discussed earlier, it appears that New Zealand's intelligence agencies have a culture of legal compliance and are otherwise highly incentivised to comply with their human rights obligations.

In sum, these legislative provisions within the Act can robustly protect human rights in the context of foreign intelligence sharing. They do so not just by constraining the behaviour of New Zealand's agencies, but also by indirectly constraining the actions of their partners in foreign intelligence sharing relationships in a rights-protective manner.

107 At 5.
108 Collins, above n 70, at [20].
109 Intelligence and Security Act, s 17(a).
110 Horsley, above n 85, at [19].
111 Intelligence and Security Act, s 10(3).
112 Deeks, above n 13, at 33.

(4) Network norms

The way in which the "shared professional ethos" of intelligence agencies constrains their cooperation requires more elaboration.[113] As previously explained, the profession has developed shared norms to guide their behaviour. Intelligence agencies are also very well-connected; the CIA has connections to over 400 agencies.[114] While intelligence sharing agreements are often bilateral, they take place within a broader network of interconnected agencies. These networks have their own norms.

Network members are pressured to comply with these norms by other members—a process called "acculturation".[115] Reputation within the network depends on the agency's compliance. Comply, and earn a good reputation, and other network members will be willing to share intelligence in greater quantities and of greater sensitivity.[116] Break the norms, and the violation reverberates through the rest of the web. An agency of poor reputation will likely not be wholly excluded, as their comparative advantages still drive others to share intelligence with them.[117] However, they will still be subject to "reputational sanctioning":[118] a slower influx of shared intelligence; less willingness to cooperate; and greater caution.

One example of a norm (and arguably the most important) is the principle of originator control.[119] It holds that shared intelligence remains under the control of the sender (the originator). At minimum, this means that shared information cannot be shared to any third party without that originator's consent.[120] Forcese also extends originator control to include use restrictions that limit the ways in which shared intelligence can be used.[121] Adherence to this principle allows intelligence agencies to trust that those with whom they share intelligence will not share it without their consent. It is no surprise that it is a norm of intelligence sharing networks.

The relevance of network norms to the legislative constraints is less obvious than the relevance of peer domestic legal constraints. I argue its relevance lies in how the legislative constraints in the Act can help create rights-enhancing network norms. Elizabeth Sepper herself doubts the law's ability to constrain intelligence agencies.[122] When she suggests that ethical standards within the profession should become more protective of human rights, I infer she means for such change to come from the agencies themselves.[123] That is, internal policy changes that lead to a more rights-protective outcome. Deeks notes that network norms are not necessarily driven by legal considerations.[124] However, that does not mean they never are, or that they cannot be.

I suggest that more rights-protective norms can be brought about through constraints like those in the Act. As explained earlier, the Act's provisions, in directly constraining New Zealand's agencies, can indirectly constrain partner agencies. By itself, this will not

113 Sepper, above n 10, at 153.
114 At 155.
115 At 163.
116 At 162.
117 At 165.
118 At 165.
119 At 160.
120 Forcese, above n 6, at 77.
121 At 77.
122 Sepper, above n 10, at 153.
123 At 184.
124 Deeks, above n 13, at 17.

create a norm of respect for human rights. Rights-protective norms could arise if multiple agencies within a network are similarly constrained. A breach of constraints to which a partner agency agreed may dissuade the constraining agency from further cooperation. It is easy to imagine that in a network with multiple constraining agencies, a breach of constraints would reverberate through them, like the violation of a norm, dissuading those agencies from cooperating with the violator. From there, a norm may develop in line with those rights-protecting constraints. Two partners in a network with such a norm, who themselves may not be subject to legal constraints requiring respect for human rights, may abide by the norm anyway, having acculturated to it. They may even internalise it, leading to greater adherence.[125]

For this to work, New Zealand cannot be the only network partner in its foreign intelligence sharing relationships with laws or regulations requiring such respect for human rights. As noted earlier, only a few countries specify the conditions for cooperation.[126] But Deeks notes that intelligence agencies have, in the past two decades, become increasingly "legalized" and subject to greater regulation.[127] I doubt that the spectre of the CIA's "sordid" enhanced interrogation program, and the reputational costs it incurred, has passed.[128] Between this and awareness of rights abuses arising in the intelligence context generally, I consider it likely that such ongoing legalisation will include protections for human rights in the context of foreign intelligence sharing.

Network norms are relevant to the provisions of the Act, albeit much more indirectly than peer domestic legal constraints and other exogenously sourced peer constraints. The provisions of the Act can help create specific network norms that protect human rights. The increasing legalisation of intelligence agencies makes such constraints more likely, raising the likelihood of such norms forming.

(5) Flaws

The legislative provisions within the Act interact with the peer constraints governing foreign intelligence sharing relationships, such that they support each other. Combined, they provide robust protections for human rights in the context of foreign intelligence sharing. This does not mean the provisions are without flaw, or that peer constraints are perfect. Peer constraints only supplement, and do not replace, other forms of oversight.[129]

I begin with the requirement for ministerial authorisation under s 10(1)(b)(iii). Such authorisation is required for sharing intelligence with a foreign partner. Originator control requires the consent of the NZSIS or GCSB before intelligence is on-shared with a third party. But it is unclear if that third party requires ministerial authorisation. If the United States wants to on-share New Zealand intelligence with France, and France, for whatever reason, is not already the subject of ministerial authorisation, then is a request for such authorisation necessary? Or can the NZSIS or GCSB approve such on-sharing themselves?

Current practice suggests that agencies can approve on-sharing without the need for ministerial authorisation for the third parties. The agencies themselves are effectively delegated the decision-making.[130] The *Taumaru* report considered that HRRAs would

125 Sepper, above n 10, at 164.
126 Hayez, above n 16, at 159.
127 Deeks, above n 13, at 13.
128 Barrett and Parker, above n 18, at 247.
129 Deeks, above n 17, at 33.
130 Arnold and Mahuika, above n 91, at [10.90].

account for on-sharing with third parties, presumably where such on-sharing could lead to human rights abuses.[131] In that case, on-sharing is either denied, or left to the Minister to decide. At lower levels of risk, the decision is purely the agencies'.

But ministerial authorisations allow the Minister responsible to assess the risks involved in the intelligence sharing before it takes place.[132] It is a statutory safeguard. However, such a safeguard is bypassed if the Minister is only involved in decisions where there is a real risk of contributing to significant human rights violations.

The agencies argue that ministerial authorisation is only required where they themselves provide the intelligence.[133] In on-sharing decisions, it is the partner agency providing the intelligence shared by New Zealand. That does not justify bypassing a statutory safeguard. For this reason, third parties should have ministerial authorisation before being on-shared intelligence.

Network norms are also flawed. To begin with, their efficacy is not dependent on the norm's "legitimacy".[134] Rather, it is dependent on peer pressure. If, for example, it became a norm to accept torture as producing reliable intelligence, network members would still acculturate and enforce such a standard. Acculturation of network norms can therefore spread "lower, rather than higher, standards".[135]

Another significant flaw of network norms is their dependence on the detection of a violation.[136] If those other members have much more limited foreign intelligence capabilities, then they are unlikely to detect a violation of network norms. The violator would then evade punishment by its fellow agencies. A rights-protective norm might proliferate—for instance, that torture is to be avoided for producing unreliable intelligence. But it bears repeating that agencies do not always know how a given source has been interrogated.[137] That norm cannot be enforced by network partners without detection.

Even peer domestic legal constraints are flawed. There are a limited number of constraining agencies (meaning agencies that condition their cooperation on the inclusion of certain constraints).[138] It is therefore possible to avoid intelligence cooperation with those agencies and acquire the same or similar intelligence from others.

Deeks claims that the bulk of such constraining agencies are Western democracies that typically have "extensive intelligence capabilities".[139] This mitigates the flaw in part, because such capabilities would still be in high demand. A constraining state, for instance, might be the only source of desired intelligence. If this is not the case, then a "less constraining alternative" may be pursued.[140] At its worst, the result may be a significant chilling effect on the foreign intelligence sharing activities of a constraining agency, without actually constraining the activities of any potential partners. The legislative provisions, in forming the basis for such constraints, may potentially result in this outcome (though it is unlikely).

131 At [10.89].
132 Horsley, above n 85, at [19].
133 At [18].
134 Sepper, above n 10, at 182.
135 At 182.
136 Forcese, above n 6, at 88.
137 At 88.
138 Deeks, above n 13, at 33.
139 At 33.
140 At 32.

The MPS is also not without flaw, though I note that those present are less severe. I stated above that the MPS allows the use of intelligence gained through torture where doing so would prevent loss of life, harm to persons, or damage to critical infrastructure.[141] That the MPS provides for such an exception may be cause for concern. New Zealand, after all, strongly opposes torture and other cruel, inhuman, or degrading punishments. Acting upon intelligence gained through such abuse may encourage it. While objectionable, I consider this flaw to be relatively minor in comparison to the flaws of the peer constraints above. This is because the circumstances that would permit such an exception to be used are highly unlikely. It is akin to the ticking bomb scenario. Just as that scenario relies on a multitude of variables lining up exactly right,[142] so too does this exception. The threat must be real; the partner agency must have the right suspect; torture must produce reliable intelligence; and the intelligence must be provided and shared soon enough, and in sufficient detail, to allow New Zealand agencies to prevent the threat. This is unlikely to happen.

Another flaw with the MPS is that the Minister responsible can still approve intelligence cooperation with a real risk of significantly contributing to human rights violations.[143] An agency may request ministerial authorisation, despite finding that the cooperation would lead to serious breaches of human rights. The Minister may approve it accordingly. This flaw, however, relies on there not being a culture of compliance within the agencies. As it stands, there is. Moreover, in practice, few HRRAs (at least of those done by the GCSB) meet the threshold of there being a real risk.[144] Nor is there a guarantee that a risk will eventuate.

A more concerning flaw is that the MPS does not require the undertaking of an HRRA for every instance of intelligence sharing.[145] It leaves it to the agencies' internal policies to determine when an HRRA is to be carried out. This raises a concern that the agencies might overlook a real risk of human rights violations in their foreign intelligence sharing relationships. However, I question if it is even feasible to conduct an HRRA for every instance. Recall that, within a three-year span, 1,500 HRRAs were conducted.[146] One can speculate on how many more instances of intelligence sharing occurred that did not warrant an HRRA. However the scale of intelligence sharing is clear. In any case, the JPS provides guidance on when an HRRA is required, which may address this flaw.[147] But as only a three-page summary is available, little more can be said on this.

Despite the flaws of peer constraints as a mechanism, and the issues with both the MPS and the legislative constraints that control foreign intelligence sharing, I still find the overall protection they provide for human rights to be fairly robust. Many of the flaws discussed above are mitigated in some way. Those that are not, I do not consider significant enough to render the protections anything but robust.

141 Collins, above n 70, at [23].
142 Barrett and Parker, above n 18, at 250.
143 Collins, above n 70, at [20].
144 Horsley, above n 85, at [56].
145 Collins, above n 70, at [20].
146 Arnold and Mahuika, above n 91, at [10.80].
147 Government Communications Security Bureau and New Zealand Security Intelligence Service, above n 82, at [7].

(6) Oversight mechanisms

While the legislative provisions provide robust protections for human rights in the context of foreign intelligence sharing, it is not the only source of such protections within the Act. It also provides for oversight mechanisms. Once again, peer constraints are only a supplement for other forms of oversight—not a replacement.

That is not to say that external oversight mechanisms have no connection to peer constraints. Much like the legislative provisions discussed above, oversight mechanisms serve as an exogenous source of such constraints. Agencies subject to "aggressive domestic oversight" may impose more constraints on, or simply avoid, intelligence cooperation bearing a real risk of human rights abuses.[148] This arises in part because such agreements might be brought to light by these mechanisms. For instance, Forcese notes that any attempts by CSIS to circumvent Canadian privacy laws through cooperation with the United States would likely draw the "ire" of its oversight bodies.[149] Partner agencies share the same fears that their foreign intelligence sharing agreements will be revealed to the public. Consequently, they will hesitate to cooperate.[150] I add that it may also cause these partners to incorporate rights-protective constraints into their agreements even before offering such cooperation, to pre-empt the need for scrutiny. Such an outcome would be good for human rights.

The question, then, is whether the oversight bodies preserved by the Act can serve as such aggressive overseers. There are two: the IGIS, and the Intelligence and Security Committee (ISC). I will cover both only insofar as they pertain to foreign intelligence sharing. I find that while the IGIS may well be effective, the ISC is rather impotent.

The Act preserves the office of the IGIS, which provides independent oversight of the agencies.[151] Part of its functions includes the conduct of inquiries into agencies' compliance with New Zealand's laws, alongside reviews of agency activities.[152] In line with this, the IGIS is empowered to summon people and "require them to give evidence on oath".[153] On the completion of an inquiry, the IGIS writes a report with recommendations, and sends it to the Minister responsible and the relevant Director-General.

Previously, the Inspector-General of Intelligence and Security Act 1996 prohibited the IGIS from inquiring into "operationally sensitive" matters.[154] Given that this included anything related to intelligence collection and information sources, it likely also limited access to MOUs and other documents relating to New Zealand's foreign intelligence sharing agreements. Fortunately, as Damien Rogers notes, no such prohibition exists in the Act.[155] At the very least, the July 2024 Review of the Agencies' application of HRRAs confirms that HRRAs are not off-limits for the IGIS.[156]

However, it is unclear if the IGIS can access intelligence shared by partners. Then-Inspector-General Cheryl Gwyn noted that the principle of originator control sees oversight bodies as third parties. Such bodies may therefore be precluded from "accessing

148 Deeks, above n 13, at 26.
149 Forcese, above n 6, at 82.
150 Deeks, above n 13, at 26.
151 Intelligence and Security Act, s 157.
152 Sections 158(1)(a) and 158(1)(f).
153 Arnold and Mahuika, above n 91, at [4.39]; and Intelligence and Security Act, ss 178–179.
154 Inspector-General of Intelligence and Security Act 1996, s 11(4).
155 Damien Rogers "Intelligence and Security Act 2017: A Preliminary Critique" [2018] NZ L Rev 657 at 683.
156 Horsley, above n 85, at [33].

large volumes of information and correspondence held by intelligence services".[157] Functionally, then, there may still be a wall concerning access by IGIS to intelligence shared by partner agencies.

However, I am not convinced that lack of access to such information is overly detrimental to the IGIS's ability to oversee the agencies' foreign intelligence sharing relationships. Insofar as this concerns simply ensuring that the agencies have abided by the requirement of ministerial authorisation and have properly conducted HRRAs, originator control should pose no obstacle. The IGIS can clearly examine HRRAs, applications for ministerial authorisations, and authorisations themselves.[158] Originator control would not preclude it from looking at intelligence shared by New Zealand agencies to foreign partners. So long as its ability to inquire into operationally sensitive matters includes correspondence about the initial formation of the intelligence sharing relationship, the IGIS's ability to inquire into agencies' compliance should be unaffected.

The IGIS's powers to summon persons and compel the disclosure of information are not applicable during reviews. Both powers specify "inquiry", thereby precluding their use outside of it.[159] Despite this, the *Taumaru* report did not consider it a significant weakness. Agencies are essentially obliged to cooperate with a review, due in part to their duty to act in a way that facilitates effective oversight.[160] That it is an offence to obstruct the IGIS in the exercise of their powers likely helps.[161]

The Act also preserves the ISC, which serves to provide Parliamentary oversight of the NZSIS and GCSB.[162] Its functions include examining each agency's policies, administration, and expenditures, considering the agencies' annual reports and requesting the IGIS to conduct inquiries.[163] Through this, the ISC is supposed to check the Executive's activities (here, in the context of intelligence), serving much like a Select Committee.[164] But given that the ISC is chaired by the Prime Minister, its independence from the Executive (and therefore ability to check it) is doubtful.[165]

Moreover, the Committee's lack of powers and its inability to inquire into any "operationally sensitive" matters makes it a very lacklustre method of accountability.[166] For instance, while the ISC can request evidence from others, the Director-General may refuse its disclosure on grounds of sensitivity.[167] That includes information provided to New Zealand agencies by foreign governments, which is already subject to the principle of originator control.[168] It also includes an intelligence's agencies sources of information, likely covering material related to foreign intelligence sharing (MOUs and other documents). As an agency's foreign intelligence sharing relationships are among its "most

157 Cheryl Gwyn, Inspector-General of Intelligence and Security "Spotlight on Security" (New Zealand Centre for Public Law Public Officeholders' Lecture Series, Victoria University of Wellington, Wellington, 4 May 2016) at 14.
158 Horsley, above n 85, at [15] and [33].
159 Intelligence and Security Act, ss 178–179.
160 Arnold and Mahuika, above n 91, at [4.40]; and Intelligence and Security Act, s 17(d).
161 Section 225.
162 Section 192.
163 Section 193.
164 Arnold and Mahuika, above n 91, at [12.13].
165 At [12.47].
166 Intelligence and Security Act, s 193(2)(b).
167 Section 203(1)(b).
168 Section 202.

closely guarded secrets", it is difficult to imagine that the Director-General would not refuse its disclosure.[169]

The ISC also lacks the capacity to investigate matters itself.[170] Consequently, it is forced to rely on the agencies' word. Under this arrangement, it is difficult to see how the ISC can effectively oversee an agency's intelligence activities, let alone their foreign intelligence sharing relationships.

Of the two oversight bodies provided for under the Act, only the IGIS can provide effective oversight of the agencies' foreign intelligence sharing relationships. The IGIS may then be an effective source of peer constraints in such relationships.

(7) Recommendations

Overall, I find that the Act provides fairly robust protections for human rights in the context of foreign intelligence sharing. An existing culture of legal compliance enhances its legislative provisions, and both feed into and are improved by the peer constraints governing foreign intelligence sharing relationships. And while the ISC is impotent, the IGIS can provide effective oversight. But, as the flaws discussed make clear, there is still room for improvement.

To begin with, s 10 should be amended so that on-sharing of intelligence by a partner agency to a third party requires that third party to have ministerial authorisation. That will enable the Minister responsible to clearly consider the human rights risks of that on-sharing before granting authorisation and so increase protection for human rights.

Moreover, the IGIS's powers to summon and compel persons should be amended to also be available for use during reviews. As noted above, the *Taumaru* report does not consider this an issue. Yet the strengthening of the IGIS's powers through such an amendment as suggested would increase the IGIS's efficacy as an external source of peer constraints. If a partner sees a possible discovery of the foreign intelligence sharing agreement by the IGIS even during a review, that will place more pressure on them to comply with their human rights obligations.

Lastly, the ISC requires much amending. The Executive is meant to be "answerable to Parliament".[171] The ISC includes members of that same Executive, precluding independence and putting its ability to provide effective oversight over New Zealand's intelligence agencies into question. Much like the *Taumaru* report, I suggest that members of the Executive should be statutorily barred from ISC membership.[172]

While I do not intend to detail other amendments, I note that the ISC needs to have access to operationally sensitive material if it is to oversee agencies' activities, especially in the realm of foreign intelligence sharing. Without such access, MOUs and other documents relevant to the practice would be beyond its reach. And for the same reasons as I argued in the previous section, I do not consider that this access would need to include intelligence shared by foreign partners. Effective oversight of agencies' foreign intelligence sharing agreements should still be achievable.

169 Forcese, above n 6, at 75.
170 Arnold and Mahuika, above n 91, at [12.14].
171 At [12.47].
172 At [12.48].

IV Conclusion

Foreign intelligence sharing is a very useful practice. It allows intelligence agencies to benefit from each other's comparative advantages and split the burden of cost in their activities. The resource and capacity limitations of individual intelligence agencies, combined with the sheer demand for intelligence, makes it a necessary practice as well.

But this practice impinges on human rights. It impinges on privacy, as it enables the bypass of domestic privacy protections, and inevitably sees a state receiving intelligence on its citizens. It also impinges on the right to be free from torture, as intelligence shared may lead to torture or have been acquired through it. States have been held liable on the international stage for such human rights abuses stemming from intelligence cooperation more broadly. There is no reason to think foreign intelligence sharing cannot form the basis for such liability.

The Act provides protections for human rights in the context of foreign intelligence sharing. These come in the form of duties, a statutory safeguard, and an MPS that guides the agencies in their foreign intelligence sharing activities. These protections are robust despite their flaws. The culture of compliance within the agencies enhances their efficacy. Moreover, they serve to place New Zealand's intelligence agencies as constraining partners within their foreign intelligence sharing relationships, leading to more rights-protective outcomes. They also contribute to the development of rights-protective norms within intelligence sharing networks.

Overall, I have found that the oversight mechanisms provided in the Act are a mixed bag when it comes to human rights protections in foreign intelligence sharing. The IGIS serves as an effective form of domestic oversight, while the ISC demands much in the way of reform to be effective. For these reasons, I consider that, overall, the Act provides robust protections for human rights in the context of foreign intelligence sharing.