OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Cheryl Gwyn – Inspector-General of Intelligence and Security

New Zealand Centre for Public Law Public Officeholders' Lecture Series "Spotlight on Security", Victoria's Faculty of Law, 4 May 2016

Introduction

First I would like to thank the New Zealand Centre for Public Law for its excellent initiative in organising this series. I'm grateful for the opportunity to speak to you.

I propose to briefly outline the role and functions of the Inspector-General of Intelligence and Security – what we do and what we can't do.

I will then look at some of the challenges ahead – for the public and for legislators and some that are specific to the oversight function.

Role of the Inspector-General

The role of the Inspector-General was significantly strengthened in late 2013. Previously the Inspector-General had been a retired Judge, working part-time, with no investigatory capacity. Under the amendments it became a fulltime role and the powers and resources of the office now more closely match the mandate.

As Inspector-General I have jurisdiction to:

- receive complaints (from the public, current and former staff members of the intelligence and security agencies).[1] The IGIS is also the nominated authority for the purpose of whistleblowing[2]

- initiate inquiries at the request of the Prime Minister or the Minister responsible, or on my own motion, into the legality and/or propriety of the actions of the intelligence and security agencies[3]

- I'm obliged to report publicly on all of my inquiries and annually (subject to security constraints)[4]

- review the agencies' internal systems, with a view to certifying annually whether their compliance systems are "sound"

- review all interception and intelligence warrants and authorisations (*ex post*).

These powers are coupled with a right of access to security records held by the agencies and a right of access to the agencies' premises and ICT systems.[5]

In the case of inquiries, I have strong investigative powers akin to those of a Royal commission, including the power to compel persons to answer questions and produce documents, to take sworn evidence.[6]

I want to come back to some specifics of the powers I have mentioned.

---

1 Inspector-General of Intelligence and Security Act 1996 (NZ) (IGIS Act), s 11(1)(b).
2 Protected Disclosures Act 2000 (NZ), s 12.
3 IGIS Act, s 11(1)(a),(c),(ca).
4 IGIS Act, ss 25 and 27.
5 IGIS Act, ss 20 and 21.
6 IGIS Act, ss 23 and 24.

Whistleblowing

The Snowden disclosures demonstrate how critical it is to have a clear path, with appropriate protections, for disclosing information about suspected serious wrongdoing within an intelligence and security agency. In New Zealand, the Inspector-General is the only appropriate authority to whom New Zealand Security Intelligence Service (NZSIS) and Government Communications Security Bureau (GCSB) staff may make protected disclosures under the Protected Disclosures Act 2000 and I am working with the agencies to ensure that there are appropriate policies and mechanisms in place.

Propriety

My jurisdiction extends to both legality and propriety. "Propriety" is not defined in the legislation but is clearly intended to have a broader reach than specific questions of legality. In my office's NZSIS/Slater inquiry in 2014,[7] propriety encompassed whether the NZSIS acted in a way that a fully informed and objective observer would consider appropriate and justifiable in the circumstances. Depending on the context, "propriety" might be akin to the requirements of good administration or to the model litigant obligations that apply to the Crown.

Right of access to security records

Total, unmediated access to security information held by the intelligence and security agencies is essential for effective oversight; ultimately, it must not be left to agency staff to determine whether or not to provide information.

In New Zealand that right is protected by statute,[8] but recent experiences in the United States demonstrate how the right of access can be encroached on. The US Inspector General Act of 1978 provides that inspectors-general, who in the US cover many federal departments, including the intelligence and security agencies, and who are often based in

---

7 "Report into the release of information by the New Zealand Security Intelligence Service in July and August 2011", pp 70-71.

8 IGIS Act, s 20, though note the right is subject to s 26(3).

the agencies they oversee, should have access to “all records” needed to do their job. Some of the agencies have, during the Obama administration, attempted to systematically thwart that access for whole categories of information. For example, from 2010 lawyers for the Federal Bureau of Investigation (FBI) started to claim they were barred by law from handing over certain documents.

The effect has been to slow down investigations and inspectors general have spent time and taxpayers’ money arguing for access to documents they should, by law, have to hand.

In July 2015, the Office of Legal Counsel, which provides legal opinions to the President, issued a 68-page memorandum defending this obstructive behaviour. Because certain documents are protected by statute from being disclosed publicly, the memo reasoned, agency staff must determine whether to hand them over to the inspectors general.

That makes no sense. Giving inspectors general access to critical information is not the same as making that information public.

Classified information

An important aspect of the question of access – for the public as much as for the inspector-general – is the intelligence community treatment of classified information. Intelligence and security agencies apply tiers of classification to documents and other information, from “confidential” to “top secret”, in order to prevent certain information from coming to the knowledge of unauthorised persons. Such a system of classification and protection is necessary, but the classifications are not immutable: in 2014 the UK eliminated its “confidential” level of government secrecy and in March this year the US Director of National Intelligence, James Clapper, sought feedback on a proposal to follow suit. Eliminating the lowest level of classification would have a significant effect on the number of classified documents created by the government.

Much has been written about the dysfunctional, arbitrary and counterproductive nature of the US system and practice of classifying documents. Too much information is classified; there are thousands of people in government who can classify information; and the

restrictions imposed by the classification last too long. Classifications are inconsistent: in the context of calls to prosecute Hillary Clinton for having documents on her private email server when she was secretary of state (documents that have since been declared top secret) President Obama, defending Mrs Clinton, said: "there's classified, and then there's classified. There is stuff that's really top-secret, top-secret and then there's stuff that's being presented to the president or the secretary of state, that you might not want … going out over the wire, that is basically stuff that you could get in open-source".

To which Edward Snowden responded by tweet: "If only I had known**"** and, later, **"**Anyone have the number for the Attorney General? Asking for a friend."

President Obama's comments suggest that, at least in the US, much of what is classified is merely sensitive, or a little embarrassing, or there is still a policy debate in progress, and that classifications are applied inconsistently. But those distinctions aren't necessarily made in the US government's treatment of classification when dealing with news organisations, whistle blowers, or government officials accused of leaking information.[9]

The broader US experience highlights how the invocation of state secrets can be used, on the one hand, to prosecute certain individuals, on the other to dismiss legal action against the state that might expose unpleasant facts, such as dismissal of a lawsuit[10] that might have exposed details of Central Intelligence Agency (CIA) cooperation with other countries in the programme of rendition and torture.

The Dutch oversight body, the Review Committee on the Intelligence and Security Services (CTIVD) has investigated whether the Dutch civilian intelligence and security agency, the

---

9 See, eg, the cases of US Army General David Petraeus, a former director of the CIA, who was prosecuted for giving a woman who was writing his biography (and with whom he was in a relationship) notebooks of classified information, including code words for intelligence programmes and war strategy – allowed to plead guilty to a misdemeanor; Thomas Drake, a former official of the National Security Agency (NSA), accused of wrongly providing information about the agency's practices to a newspaper – charged with ten offences under the Espionage Act, later dropped and he pleaded guilty to a misdemeanour count for exceeding authorised use of a computer; and a mid-level State Department official prosecuted for telling a Fox News reporter that North Korea would most likely react to sanctions with more nuclear tests – charged with a felony and spent 11 months in prison.

10 Against Jeppesen Dataplan Inc., a Boeing subsidiary accused of arranging flights for the CIA to transfer prisoners to other countries for imprisonment and interrogation.

General Intelligence and Security Service (GISS) applies the classification of state secrets correctly, within the Dutch legislative framework,[11] including what kinds of information are properly the subject of classification, classification levels and destruction and declassification.

It seems to me that an examination in the New Zealand context of the framework within which classification decisions are made and the application of that framework, would be a useful exercise for my office at some point in the future.

Review of all interception and intelligence warrants and authorisations (ex post)

The legislation governing the issue of warrants and authorisations requires the agencies to satisfy tests of necessity and proportionality[12] and the inspection of all warrants by my office[13] is an example of how effective oversight can work in practice to protect privacy interests. The kind of questions we ask when reviewing warrants include:

- how personal data which is not the subject of a warrant or access authorisation is protected
- how the agency has proposed to minimise the impact of a warrant on a third party and whether it has adequately informed the authorising Minister, so he knows whether to include conditions in a warrant to minimise that risk
- how the agency establishes in its warrant application that the communication to be intercepted or seized is not privileged as defined by its legislation,[14] including how any unforeseen interception or seizure of privileged material is to be identified and resolved. This includes circumstances relating to legal professional privilege and religious privilege.

---

11 CTIVD no. 33, 13 June 2012.

12 Government Communications Security Bureau Act 2003 (GCSB Act), s 15A(2); New Zealand Security Intelligence Service Act 1969 (NZSIS Act), s 4A(3).

13 Mandated under IGIS Act, s 11(1)(d)(i).

14 GCSB Act, s 15C; NZSIS Act, s 4A(3)(d).

We select some of those warrants and authorisations for deeper analysis – a comprehensive check of the process and path by which the application for the warrant was formulated, from the intelligence case, to the application for the warrant prepared by the Director, the warrant itself, signed by the Minister (and Commissioner of Security Warrants where required), through to a review of what intelligence was collected under it and how that informed decisions about cancellation/non-renewal or renewal of the warrant.

Our role is primarily *ex post facto* – that is, after particular operations have concluded. The underlying rationale is that oversight bodies should review, but not direct or approve in advance, the management and operational decisions of the intelligence services. This approach does not preclude the agencies briefing me on planned or ongoing operations. Although it is not my role to approve operations in advance, there are situations where prior discussion with my office can help to ensure clarity about the legality and propriety of any planned activity.

Public reporting

Mandatory public reporting – annually and of specific inquiries - is an important aspect of effective oversight.[15] But there are, of course, limits on what can be contained in those reports. The Inspector-General may, after consulting the chief executive of the intelligence and security agency concerned, determine the security classification of a report into an inquiry,[16] but I cannot disclose matters which would prejudice security, endanger safety of any person, prejudice the entrusting of confidential information etc and the Minister may ultimately certify that a proposed disclosure of information by the Inspector-General may prejudice any of those matters and should not be made, or should be made only on terms and conditions.[17] To my knowledge the Ministerial certificate provision has not been invoked.

---

15 IGIS Act, ss 25A(1), 27(6A).
16 IGIS Act, s 25(8).
17 IGIS Act ss 25A and 26.

Interestingly, CTIVD, the Dutch oversight body – which I think is a very robust oversight body – has had to deal with a situation where the responsible Minister required that certain information not be disclosed by the CTIVD. It noted in its Annual Report for 2014-2015: "The Committee wanted to mention in the report against how many persons an organisation GISS had exercised the power to intercept in 2012-2013 and how many SIGINT operations took place in the year. The Minister removed these figures from the public report invoking the obligation of secrecy. The Committee regrets this."

Maintaining security and being bound by the rules around classified information does sometimes make it difficult to report publicly on issues as fully as I think is desirable in the public interest. I have asked the Directors of both agencies for their full cooperation to assist me in making as much information public as possible when I come to report on the various inquiries into their agencies.

Work behind the scenes

While mandatory reporting is vital, much of our work is done away from public scrutiny. For example, our regular review of all warrants and access authorisations frequently gives rise to questions, sometimes to identification of deficiencies, and a discussion with the agency about how changes might be effected. Those changes do happen.

Limits on IGIS powers

I want to talk a little now about the limits on the Inspector-General's powers.

Intelligence and security agencies

First, my oversight extends only to the NZSIS and GCSB, although there is provision[18] for declaration by the Governor-General by order in council of any other agency as an

---

[18] IGIS Act, s 2.

intelligence and security agency. There are no criteria stated for such a designation and the provision has not been used to date.

The Cullen/Reddy report[19] broaches the question of oversight of the intelligence assessment function. It looks at the role of the Combined Threat Assessment Group (CTAG), an interdepartmental assessment unit, comprising the GCSB, Police, Defence Intelligence and the Aviation Security Service, and located within the NZSIS. Its focus is purely on assessing terrorist threats to New Zealanders and New Zealand, and providing advice on the domestic threat level.

The Inspector-General has jurisdiction over CTAG.

The dedicated assessments agency is the National Assessments Bureau (NAB), which sits within the Department of the Prime Minister and Cabinet (DPMC). It assesses the veracity of the intelligence from the collection agencies, filters it for relevance and contextualises it for government decision-makers.

In Australia, which has the most directly comparable oversight regime (the New Zealand IGIS Act is modelled on the Australian IGIS Act) the Inspector-General has jurisdiction over the assessment role carried out by the Office of National Assessments (ONA), broadly the equivalent of New Zealand's NAB. (The Australian Inspector-General also has jurisdiction over the defence intelligence functions.)

The 2004 Philip Flood *Report of the Inquiry into Australian Intelligence Agencies* recommended that the Inspector-General IGIS should have a general own motion capacity in respect of ONA and should conduct periodic reviews of ONA's statutory independence. The recommendation arose out of the intelligence assessment of Iraq's weapons of mass destruction that led to launching of the second war against Iraq. Subsequent legislative amendments to the *Inspector-General of Intelligence and Security Act 1986* gave effect to those recommendations.

---

[19] "Intelligence and Security in a Free Society", Hon Sir Michael Cullen, KNZM and Dame Patsy Reddy, DNZM, 29 February 2016.

The Cullen/Reddy report[20] recommends that the NAB should be established as a departmental agency and that the government consider including its functions in the single Act which is proposed to cover the intelligence and security agencies and the oversight bodies. Sir Michael and Dame Patsy stop short of recommending that the NAB be subject to Inspector-General oversight.

Legality & propriety only

My jurisdiction extends to questions of legality and propriety. It's not for my office to:

- examine the "policy, administration, and expenditure" of the agencies. That is a role for the Intelligence and Security Committee[21]
- question how well the agencies deliver value to their customers and New Zealanders. Essentially that is a State Services Commission, Performance Improvement Framework (PIF) process. So, unless it were a strict legality issue or a question of propriety, it is not for me to say that in carrying out a particular intelligence task the agency did an excellent, or a woefully poor, job from an intelligence perspective
- audit how the agencies are operating and accounting for their performance, in accordance with Parliament's intentions. That is for the Controller and Auditor-General.

I can't declare an intelligence or interception warrant or authorisation invalid. I can say the application for the warrant that was put before the Minister (and the Commissioner of Security Warrants where applicable), was seriously deficient in x respects or was plain wrong, and make recommendations about what should happen as a consequence, but ultimately it is for the decision-maker(s) to decide whether the warrant should be revoked, whether intelligence collected under it should be destroyed, and what other steps should follow.

---

20 Ibid, at 4.35.

21 Intelligence and Security Committee Act 1996, s 6(1).

Nor does the Inspector-General have a judicial review function, although some of the ends of judicial review (helping to prevent abuses of power, helping to improve the process of decision-making) may be achieved through a combination of our complaints, inquiry and review functions.

Challenges ahead

I want now to talk about some of the challenges ahead – for the public and for legislators – and more specifically for my office as an oversight body.

New legislation

We now have the Cullen/Reddy report as a comprehensive basis for the drafting of new legislation.

Their recommendations about oversight are clear and, in respect of my office, if I may say, are necessary and sensible and unlikely to be contentious. If the past is any guide, political consensus in favour of strengthening oversight often develops where politicians cannot agree on more fundamental reforms. But all the oversight in the world is no substitute for getting the scope of the government's surveillance powers right in the first place. That will be the hard part.

The Cullen/Reddy review refers to various overseas reports, among them David Anderson QC's 2015 report.[22] Speaking about the UK legislation, Mr Anderson said:

> *"Each intrusive power must be shown to be necessary, clearly spelled out in law, limited in accordance with human rights standards and subject to demanding and visible safeguards."*

---

[22] David Anderson QC, *"A Question of Trust",* Report of Independent Reviewer of Terrorism Legislation, June 2015.

As the Anderson report recommended, a transparent legal framework should include:[23]

- the types of data collection measures undertaken by intelligence agencies [I'll come back to this question of the need for clarity around exactly what it is the agencies do]
- who can exercise them
- what the objectives are / for what purpose they are exercised
- who might be subject to them
- the threshold and procedure for justifying their use
- the duration of any warrant or authorisation
- the procedures regarding retention, deletion and disclosure of data
- sharing parameters
- oversight and review procedures.

To the extent that *new* powers are sought, the challenge for legislators – and for the public – is to ask the logically prior question: what is the effectiveness, or lack thereof, of the agencies' existing powers? Have they convincingly demonstrated that new powers are necessary because the current powers are insufficient?

Further, any new powers must be commensurate with the scale and resources of the agencies, to ensure that they can properly utilise such powers.

David Anderson points out that any new law must be couched in technology-neutral language, but also notes that those who make and enforce the law – and those who have oversight responsibility – must have some understanding of the relevant technology, and (perhaps to state the obvious) need to know exactly what technical powers their agencies currently have and use.

---

[23] "*A Question of Trust*" was in large part the basis for the draft Investigatory Powers Bill introduced into the UK Parliament in late 2015. The IP Bill aims to consolidate and update all of the current legislation covering the UK intelligence and security agencies.

So, for example, in the UK context, equipment interference/computer network exploitation (CNE), or hacking, as it's more usually known, was first acknowledged – "avowed" – by the UK government only last year. Similarly the use of s 94 of the Telecommunications Act 1984 (UK) for the bulk collection of communications data [metadata] for the use of the intelligence agencies, was avowed for the first time simultaneously with the announcement of the draft Investigatory Powers Bill.

I understand that the avowals were seen by the UK government as necessary so that when Members of Parliament came to debate the proper scope of investigatory powers they would be fully informed as to the scope of the powers currently used by the intelligence and security agencies by the intelligence and security agencies.

International intelligence and security agency cooperation & sharing

A second challenge is around international intelligence and security agency cooperation and sharing. As the Snowden disclosures revealed, international collaboration has increased vastly post-9/11, both in terms of the volume of information shared and the number of joint operations. The scope of cooperation has broadened to include a greater range of states and a wider variety of intelligence activity.

The UKUSA arrangement – the Five Eyes: USA, UK, Canada, Australia, NZ – is the most public example of transnational intelligence collection and distribution through international intelligence sharing arrangements.

Broader and deeper cooperation between intelligence and security agencies represents a growing challenge to accountability. International information-sharing arrangements generally elude intelligence oversight.

National intelligence oversight and review structures were designed for a different era and are, in the main, ill-equipped to deal with intelligence cooperation across borders. Cooperation between intelligence and security agencies has not been matched by cooperation between national oversight and review bodies.

The extent to which national oversight bodies can cooperate, share information, perhaps even carry out joint inquiries, is seriously limited. The principle of "the third party rule" or "originator control" (ORCON), which shields information supplied to an agency by intelligence partners in other countries from attribution, has the potential to impede such oversight. The rule stipulates that information shared with a foreign intelligence service or government should not be transmitted to third parties (domestic or foreign) without the prior permission of the service which originally shared the information. That prohibition is, in many jurisdictions, interpreted as applying to the recipient services' oversight, considered to be third parties. The practical consequence is that oversight bodies may be precluded from accessing large volumes of information and correspondence held by intelligence services.

Such restrictions make it difficult, if not impossible, to scrutinise what foreign agencies do with intelligence provided by our national agencies. Who has access to that intelligence? What controls are there on that access? For how long is it to be retained? Is it used only for lawful purposes? Similarly it may be difficult or impossible for the national service to assess whether the intelligence it receives from foreign partners was collected lawfully.

In terms of reform, the process and responsibility for the authorisation of all intelligence cooperation agreements and activities should be more clearly articulated in national laws. We can seek statutory requirement for cooperation agreements to be sanctioned by the executive government, whether generally or specifically.

Intelligence services could be legally obliged to share cooperation agreements with their oversight bodies (as in Canada)[24] and/or the agencies could be required to brief oversight bodies on particular types of intelligence cooperation activities.

---

[24] Canadian Security Intelligence Service Act 1985, s 17(2).

The Cullen/Reddy report recommended:[25]

- that the new legislation clearly enable the agencies to cooperate and share intelligence with foreign jurisdictions and international organisations, where consistent with the purposes of the legislation
- any future bilateral or multilateral arrangements entered into with foreign jurisdictions or international organisations should be referred to the Intelligence and Security Committee (ISC) to be noted
- the Minister should formulate standard terms to allow for *ad hoc* cooperation or sharing with foreign jurisdictions and international organisations and refer them to the Inspector-General for comment.

Oversight cooperation

As to oversight cooperation, to date, national investigations have built on each other, rather than being coordinated across jurisdictions. For example, my office is currently undertaking an inquiry which entails an analysis of the GCSB's bulk data collection capability.[26] My work is assisted by three significant 2015 reports from the United Kingdom (the Intelligence and Security Committee's report,[27] the RUSI report,[28] the David Anderson QC report)[29] and from the United States, the Privacy and Civil Liberties Oversight Board (PCLOB) report on s 702 of the Foreign Intelligence Surveillance Act[30] and the United States National Research Council report to the President on technical options regarding bulk collection.[31]

---

25 Ibid, at 4.29-4.31.

26 Inquiry into allegations of GCSB interception of communications in the South Pacific, March 2015.

27 Intelligence and Security Committee of Parliament, *Privacy and Security: A modern and transparent legal framework*, March 2013.

28 The Royal United Services Institute, *A Democratic Licence to Operate - Report of the Independent Surveillance Review* (July 2015).

29 *A Question of Trust – Report of the Investigatory Powers Review*, June 2015.

30 July 2, 2014.

31 United States National Research Council *Bulk Collection of Signals Intelligence: Technical Options* (2015), defining (at S1) "bulk collection" as any collection of communications signals where "a significant portion of the data collected is not associated with current targets" and concluding at S6-S7 that "[t]here is no software technique that will fully substitute for bulk collection", but that there was scope for better targeting and better automatic access controls.

Similarly, my office is currently undertaking an inquiry into whether the New Zealand intelligence and security agencies had knowledge of/cooperated with the CIA's programme of detention and interrogation, including torture, as detailed in the US Senate Committee on Intelligence report released in December 2014. Although my inquiry was precipitated by the US Senate Committee report, I am assisted by the inquiries into the same or similar issues already undertaken in other jurisdictions such as the United Kingdom. (As I have said publicly a number of times, my decision to commence an own motion inquiry does not suggest or presuppose that New Zealand agencies or personnel were in any way connected with the CIA activities).

Inquiry reports from oversight bodies in other jurisdictions are useful at a number of levels – they may provide an explanation of technical processes which are largely universal; a published description of operational activities in one jurisdiction reduces the ability of agencies in other jurisdictions to deny or decline to comment or to try to prevent the oversight body from publicly describing the same or similar activities.

These kinds of public reports – in other jurisdictions as here - are forcefully negotiated, with the oversight/review bodies pushing the agencies to make as much information public as possible, rather than assert that it must remain classified for security reasons. That is essential to maintaining public confidence.

Legalism

To my mind, a third challenge is the risk of the development of a culture of legalism.

Acting legally is, as you would hope and expect, a significant preoccupation within the New Zealand intelligence and security agencies. Not surprisingly, that has been particularly the case post-Dotcom. As the Cullen/Reddy report observes, Dotcom led to a very risk averse approach, sometimes causing the GCSB to be hamstrung in its activities.

A different risk – or perhaps a different facet of the same risk – is the development of a culture of legalism. Much has been written about this phenomenon in the US, particularly within the NSA, which risks creating the appearance but not the reality of lawfulness.

It's been almost three years since the *Guardian* published its first story based on the Edward Snowden disclosures. Since then we, the public, have learned an awful lot about post-9/11 signals intelligence (SIGINT) programmes. For New Zealanders it was a revelation, but Americans had been there before: 1975 was the "year of intelligence" when the Rockefeller Commission, the Pike Committee and the Church Committee[32] all held their hearings and uncovered a surveillance state outside of the law. Reform took the shape of a compromise under which oversight would be significantly strengthened, but would largely remain secret (the House and Senate intelligence committees and the Foreign Intelligence Surveillance Court (FISA)).

Much has been written about another outcome of the 1970s reforms – the turn towards legalism, or a culture of rule following – almost regardless of the content of those rules. In-house lawyers tend to ask the legalistic "can" question: "Can we (lawfully) do X?", rather than "should we do X?"

Some of you will be familiar with the Bush administration lawyer, John Yoo, Deputy Assistant Attorney General in the Office of Legal Counsel. Yoo, also known as "Dr Yes", wrote the "Torture Memos", which (under considerable pressure in the immediate aftermath of 9/11 to come up with the "right" answer) advised the President, the CIA and the Department of Defence on the use of "enhanced interrogation techniques" and stated that such acts, widely regarded as torture, might be legally permissible under an expansive interpretation of presidential authority during the War on Terror.

The memos were withdrawn by a later head of the Office of Legal Counsel, Jack Goldsmith, but he subsequently resigned. The memos were reaffirmed; then new legal opinions were issued, essentially to same effect. They were ultimately repudiated by President Obama in January 2009.

---

[32] The Church Committee was the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, chaired by Senator Frank Church.
The Pike Committee was the United States House Permanent Select Committee on Intelligence during the period when it was chaired by Representative Otis Pike (July 1975-January 1976). It investigated illegal activities by the CIA, FBI and NSA.
The Rockefeller Commission was the United States President's Commission on CIA activities within the United States, set up by President Gerald Ford in 1975 and led by Vice President Nelson Rockefeller.

The Yoo memos also authorised warrantless wiretapping and indefinite detention.

The torture memos were at the extreme end, but that legalistic approach has continued under the Obama administration. A new book by Charlie Savage, "*Power Wars: Inside Obama's Post-9/11 Presidency*" quotes CIA Director and former Deputy Homeland Security Adviser) John Brennan: "I have never found a case that our legal authorities, or legal interpretations that came out from that lawyers group, prevented us from doing something that we thought was in the best interests of the United States to do."

It may well be that there was a firm legal foundation in each of those cases. But there is also the possibility that in some cases a course of action was determined and the legal process then used to find a tenable basis.

It's a risk that we – the agencies, responsible Ministers, oversight bodies – need to guard against in New Zealand in the challenging context of international terrorism, when there is political and public pressure on the agencies to prevent further acts of violence against citizens. When we are talking about the use of *the* most intrusive powers, on a broad basis, against private citizens, the case for the exercise of those powers must be very clearly made out. It surely cannot be enough that the agencies can say a proposed course of action is "legally available", without more.

Challenges for the OIGIS as an oversight body

Finally I want to touch on some challenges for my office specifically.

Like all so-called "integrity agencies" we face the ongoing challenge of maintaining our independence from political control and building public trust and confidence, while also maintaining political legitimacy with the government and with the agencies we oversee.

Typically integrity agencies are set up in the aftermath of a public scandal or a build up of pressure on governments for change. The Inspector-General's office, in its current incarnation, is a creature of the Dotcom debacle.

Again typically, there is a honeymoon phase after the agency is established. The independence of integrity agencies may be beneficial to their political principals when the integrity agency is engaged in sensitive oversight tasks that have the potential to cause political backlash. Politicians can shift attention to the oversight activity and benefit from the acknowledged "blame avoidance" function of integrity agencies. That is not in itself a bad thing, but it does have the potential to lead to a degree of abdication of responsibility by the intelligence agencies themselves and by responsible politicians: the Inspector-General can look at everything and she hasn't found a problem.

And, when I took office exactly two years ago I was initially hailed (or lamented) as a left wing interloper. It may have been somewhat useful for the government to be able to hold up my background as an activist – "See, she's not really one of us; you can be sure that she really is independent."

But the organisational arrangements need testing following the initial establishment; there is a search to find workable arrangements to balance autonomy and control. How much autonomy should the oversight body have and how much control should be exercised by executive government?

That same shifting and settling process happens in the relationship between the oversight body and those it is overseeing too. I was somewhat relieved to read a recent Canadian article[33] which showed that public servants worried that the reporting requirements imposed by integrity/oversight bodies used up significant departmental resources. Those subject to scrutiny also complained that the oversight/integrity agencies pursued their oversight activities too "vigorously", resulting in staff and managers not being able to spend as much time on their operational mandate.

The study revealed sometimes tense relationships between oversight/integrity bodies and public servants, suggesting that the oversight work requires such bodies to navigate complex relationships and engage in contentious interactions. It noted that it is inevitable

---

[33] Jamie Baxter, "From Integrity Agency to Accountability Network: The Political Economy of Public Sector Oversight in Canada", draft August 10, 2015; forthcoming (2015) 46:2 *Ottawa Law Review*.

that tensions will arise between oversight bodies and the public servants who are subject to their oversight activity.

That has indeed been our experience.

One effect of the expanded mandate and corresponding increase in resources for the Inspector-General, which is obvious in retrospect, is that an Inspector-General's office that has the capacity to investigate, review and audit more, to ask more questions, will inevitably place demands and some strain on the agencies which must respond.

I do recognise the practical implications of that and I engage with the agencies to manage the demands efficiently and constructively, for example by prioritising requests for information and providing assistance from my staff in gathering and collating relevant information.

Some of the issues my office has identified over the last two years were longstanding and systemic in nature and, because of the limited oversight in place until the 2013 reforms, had been subject to limited or no scrutiny by the Inspector-General. As both agencies have acknowledged to me, some issues either were not appreciated or, because of competing priorities, could not be assessed and remedied.

Those kinds of questions are not simple or quick to deal with. Any challenge to longstanding practice is likely to cause a degree of tension that needs to be worked through. In addition, the greater visibility and contentiousness of the work of the Service and Bureau, post-Dotcom, combined with the greater public visibility of the Inspector-General's office, means that more security issues are likely to be raised and we are all working in the public spotlight. This has added to the demands on the agencies.

In this context cordial and cooperative working relationships are important and I am grateful to the Directors of both agencies that we have been able to maintain those relationships, notwithstanding the tensions. We have a common legislative mandate to ensure the agencies act lawfully and with propriety and it is important that the Directors and their staff feel able to raise issues with me – where they have questions about the

nature of a proposed action, where they think a mistake may have been made. My office also emphasises the need for fairness in our own investigative procedures and, where I do find issues that appear to be of concern, I am of course required to give the agencies a further and full opportunity to review my proposed findings and raise any remaining concerns.

Cooperation with other agencies

Finally, I want to touch on the importance of accountability networks.

Informal, sometimes formal, coordination and cooperation between integrity agencies may help each of them to stabilise long-term independence from political influence. We can develop relationships of mutual support between organisations specialising in a specific method of accountability, such as investigation, or audit, and with shared professional expertise and ethos.

Under my legislation, I may consult with any of the Auditor-General, an Ombudsman, the Privacy Commissioner, Human Rights Commissioner and the Independent Police Conduct Authority (each of whom has a limited mandate in respect of the intelligence and security agencies), about matters relating to my statutory functions. In doing so I may disclose any information that I consider necessary for the purpose of the consultation, despite the general restriction on the Inspector-General and staff disclosing any security records or other official information about the activities of an intelligence and security agency.[34]

At the initiative of the New Zealand Privacy Commissioner, the Chief Ombudsman, the Auditor-General, the Privacy Commissioner and I meet regularly, to discuss matters of common interest and keep each other abreast of what may be on the horizon.

In practice our cooperation may occur in quite direct and practical ways, eg a joint approach to the agencies to discuss their traditional “neither confirm nor deny” response to requests

---

[34] IGIS Act, s 12.

from individuals as to whether they are under surveillance, interception or otherwise a person of interest. I have also consulted with the Privacy Commissioner over my recent report into the NZSIS holding of security vetting information.

Conclusion

The ongoing task for my office is to ensure that we have the organisational capabilities – levels of staffing, financial resources, legal powers and technical capacities – required to make a substantial difference.

Winning the trust of the agencies we oversee and building their confidence that we have the necessary expertise and fairness, is an ongoing process.

And, vitally, we need continued political leadership at the highest levels to support our oversight operations.

Thank you.