



Cheryl Gwyn
Inspector-General of
Intelligence and Security
New Zealand



Amsterdam 2015

37th International Privacy Conference
Amsterdam: 26 October 2015

How do security and intelligence oversight bodies contribute to wider public confidence about privacy and data protection?

How can a credible balance be struck between disclosure necessary to secure public confidence and non-disclosure of national security information? How does the work of such bodies relate to wider Data Protection Authority (DPA) work?

Thank you for the opportunity to speak to you and share some of your conference.

The short answer to the first question may be that, on the evidence of the Edward Snowden revelations, we (security and intelligence oversight bodies) haven't done at all well in ensuring public confidence about privacy and data protection and need to get our house in order.

For the purposes of today's discussion, the Snowden disclosures revealed two important fundamentals. First, that the legal frameworks governing the operations of some, probably many, intelligence and security agencies are stretched or broken.¹ In addition, oversight mechanisms have been seen to be inadequate or to have failed completely.

The second revelation is the extent to which intelligence and security agencies cooperate on a bi-lateral or multi-lateral basis to share intelligence.

The Snowden revelations have led to a consequent loss of public confidence – in both specialised oversight bodies and data protection bodies, to the extent that the public know of and distinguish between us.

Broken systems

I will address the questions in an illustrative, rather than theoretical way.

I want to look first at the “broken” systems. There are two aspects to these – the legislative and policy frameworks governing the intelligence and security agencies themselves and the extent to which they are subject to oversight bodies who have a full oversight mandate and whose powers and resources adequately match that mandate.

Questions about both arose in my jurisdiction, New Zealand, even before Edward Snowden became a prominent person in our lives.

¹ Paul Chadwick, moderator of the *Surveillance vs Dataveillance* session at the 36th International Privacy Conference.

You may be familiar with the larger than life figure of Kim Dotcom.

In January 2012 indictments were filed in the US against Mr Dotcom and six Megaupload associates, for offences relating to the cyberlocker site.

The New Zealand Police, at the request of the FBI, began investigating Mr Dotcom, who was living in New Zealand.

The Police sought interception assistance from the New Zealand signals intelligence (SIGINT) body, the Government Communications Security Bureau (GCSB).

The Police, in cooperation with the FBI, mounted an armed raid on Dotcom's mansion and arrested him and his associates.

The legislation then governing the GCSB said that it may not act for the purpose of intercepting the communications of a person who is a New Zealand citizen or permanent resident.

"Permanent resident" is someone who has a residence class visa.

Kim Dotcom was such a person: he had been granted residency in New Zealand in November 2010. The GCSB had misread its own and related legislation and acted unlawfully as a consequence.

The effect of the Dotcom fiasco on the GCSB was significant. The Prime Minister ordered an inquiry into the circumstances of unlawful interception by the GCSB. That inquiry, by the then Inspector-General of Intelligence and Security, found that the GCSB had acted unlawfully in providing assistance to the Police.

The then Cabinet Secretary, Rebecca Kitteridge (ironically, now Director of the New Zealand Security Intelligence Service) was appointed to undertake a review of the capability, governance and performance of the GCSB. Her report, published in March

2013,² found that the legislation governing the GCSB was simply not fit for purpose and recommended, among other things, legislative reform to clarify the application of the GCSB Act to the GCSB's work; implementation of a compliance framework; and work to strengthen the office of the Inspector-General of Intelligence and Security.

Snowden

Then came Edward Snowden. In June 2013 *The Guardian* published the first of the Snowden releases. While the initial focus was on the NSA's own activities, subsequent releases highlighted the role of the Five-Eyes partnership, including the GCSB.

It was in that context that the first round of legislative changes occurred in New Zealand. Part of that legislative shakeup was a commitment to hold periodic reviews of the intelligence and security agencies, the legislation governing them and their oversight legislation. The first such review is underway now and will report to the Intelligence and Security Committee of Parliament by February 2016.

That context of recent and imminent legislative change in the intelligence and security sector, partly triggered by Snowden, partly by the counter terrorism/foreign fighters' question, will be familiar to many of you in your own jurisdictions.

Operating frameworks

The first step in legislative change to reassure the public that agencies are exercising their intrusive powers lawfully and with regard to the privacy of citizens, is to repair the legislative and operating frameworks for the agencies themselves. This is necessary so that it is clear (to the agencies, the public, the oversight body) what it is that the agencies are being held accountable for.

² Rebecca Kitteridge, *Review of Compliance at the Government Communications Security Bureau*, March 2013.

In an intelligence context, accountability includes:³

- procedures for approval of the gathering, storage, analysis, sharing and dissemination of intelligence
- *ex post facto* review of the propriety, legality [and, sometimes, effectiveness] of the agencies' actions.

As David Anderson QC, the UK Independent Reviewer of Terrorism Legislation, said in his recent report, "*A Question of Trust*:"⁴

"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."

The Anderson report recommends that a transparent legal framework should include:

- the types of data collection measures undertaken by intelligence agencies
- who can exercise them
- what the objectives are
- who might be subject to them
- the threshold and procedure for justifying their use
- the duration of the warrant or authorisation
- the procedures regarding retention, deletion and disclosure of data
- sharing parameters
- oversight and review procedures.

³ Born, Leigh and Wills, *International Intelligence Cooperation and Accountability* (Routledge, 2011); Leigh at p 6.

⁴ *A Question of Trust - Report of the Investigatory Powers Review*, June 2015.

In many jurisdictions, New Zealand included, the legislation fails to meet many or most of those requirements. Frequently the legislation is incomplete and ambiguous, sometimes deliberately so.

Intelligence and security oversight bodies can be an important voice at times of legislative review.

On many of these issues DPAs too can and should offer a perspective. For example in the New Zealand context my colleague the New Zealand Privacy Commissioner (the co-chair of today's session) has made extensive submissions to the independent legislative review team, applying an expert privacy protection lens to these issues.

Oversight frameworks

In New Zealand, as in other jurisdictions, the framework of oversight for the two intelligence and security agencies, has a number of elements and layers.

The principal external oversight body is my office, the Office of the Inspector-General of Intelligence and Security.

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. Some other national oversight bodies have very similar mandates and powers as my office, eg the Australian Inspector-General of Intelligence and Security and the Dutch Review Committee on the Intelligence and Security Services, but I will use my own role for illustrative purposes.

As Inspector-General I have jurisdiction to:

- receive complaints (from the public, current and former staff members of the intelligence and security agencies).⁵ The IGIS is also the nominated authority for the purpose of whistleblowing⁶
- 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 agencies⁷
- I'm obliged to report publicly on all of my inquiries (subject to security constraints)⁸
- 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 their agencies' premises, ICT systems and staff.⁹

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.¹⁰

⁵ Inspector-General of Intelligence and Security Act 1996 (NZ) (IGIS Act), s 11(1)(b).

⁶ Protected Disclosures Act 2000 (NZ), s 12.

⁷ IGIS Act, s 11(1)(a),(c),(ca).

⁸ IGIS Act, s 25.

⁹ IGIS Act, ss 20 & 21.

¹⁰ IGIS Act, ss 23 & 24.

The inspection of all warrants¹¹ is a very good 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 an intelligence 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,¹² 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.

Public accountability

While intelligence and security agencies have special powers (and some protections that go with that) in many respects what they do is not unique. Other agencies – Police, Customs, border control, Defence, Foreign Affairs – have some of the same or similar powers in terms of interception and/or surveillance.

The agencies can and should be subject to many of the accountability mechanisms that apply to those other public bodies.

Need to embed privacy and freedom of information rights in intelligence and security frameworks

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

¹² Government Communications Security Bureau Act 2003 (NZ) (GCSB Act), s 15C.

In New Zealand, the GCSB is required, in consultation with the Privacy Commissioner and the Inspector-General of Intelligence and Security, to formulate a policy on personal information¹³ and the GCSB must report the results of audits conducted under the policy to the Privacy Commissioner who can then raise any issues arising with my office.

The Privacy Commissioner can investigate complaints about access to and correction of personal information held by the intelligence agencies (information privacy principles 6 & 7)¹⁴ but they are exempt from the other privacy principles. And an agency may refuse to disclose personal information requested [under principle 6] “if the disclosure of the information would be likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand or prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by the Government of any other country or any agency of such a government or any international organisation.”¹⁵

There are limits to the use of unique identifiers by the New Zealand intelligence and security agencies.¹⁶

Similarly, freedom of information laws have some, but limited, application to intelligence and security agencies.

In New Zealand they are subject to the Official Information Act 1982 and the Ombudsman’s jurisdiction in respect of that legislation. The principle underpinning the Official Information Act 1982 is that official information shall be made available unless there are good reasons for withholding it.¹⁷

¹³ GCSB Act, s 25A.

¹⁴ Privacy Act 1993 (NZ), s 6.

¹⁵ Privacy Act 1993 (NZ), s 27.

¹⁶ Information Privacy Principle 12.

¹⁷ Official Information Act 1982 (NZ) (OIA), s 5.

Conclusive reasons for withholding include if making the information available would “prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand” or would be likely to prejudice the entrusting of information to the Government of New Zealand on a a basis of confidence by (i) the Government of any other country or any agency of such a Government; or (ii) an international organisation.¹⁸ (See also, eg (UK) Freedom of Information Act 2000, s 27; (Canada) Access to Information Act, ss 13.1 and 33.1).

Cooperation with other agencies

That leads me to the question of cooperation with data protection and freedom of information bodies.

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, 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.¹⁹

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 from individuals as to whether they are under surveillance, interception or otherwise a person of interest (POI). Also, we worked jointly on a question as to

¹⁸ OIA, s 6.

¹⁹ IGIS Act, s 12.

whether the New Zealand Security Intelligence Service was entitled to receive data collected by Immigration and Customs officials.

Good process standards

There are other aspects too of improving the accountability of intelligence agencies, by holding them to good process standards. This need not thwart their processes or undercut their security function. On the contrary, it can help to ensure better outcomes from both a privacy and a security perspective.

I have two examples of what I mean.

The first example is about security clearance vetting.

It is usual for one of the intelligence and security agencies in a jurisdiction to have responsibility for assessing whether individuals should be granted a security clearance which would entitle that person to have access to classified information and thus be able to gain, or maintain, employment within the intelligence and security agencies, or other arms of government.

The process of security clearance vetting entails the accumulation of highly personal data about the candidates – financial, sexual, health, relationships. The compilation of information is probably the most detailed and sensitive body of information held by any agency of government, certainly in New Zealand. The compilation is directed at an ultimate assessment of the security risk for the individual, but that purpose can be used, intentionally or not, to shield the agency from privacy obligations.

In New Zealand the security clearance vetting process is carried out by the NZSIS. This year I began a review of the NZSIS's systems for storing, using and controlling access to information that it compiles for the vetting process.

After I commenced the review, the need for confidence and clarity in the security of such information was highlighted by the disclosure that the United States' systems for its security clearances were the subject of a reported data breach of personal details of more than 22 million people, compiled from background checks over at least 15 years.

This is an area where the access to information, systems and people afforded to specialised oversight bodies can and should be used to address broader privacy issues.

Visual surveillance warrants

My second example of requiring good process standards relates to the power to undertake visual surveillance – a power given to the NZSIS in late 2014.²⁰ The powers were modelled on Police powers. Visual surveillance is inherently more intrusive and requires more stringent scrutiny. The NZSIS, like the Police, has a statutory duty to minimise the impacts of warrants on third parties and, irrespective of whether the visual surveillance warrant is for the purpose of detecting or preventing terrorism or serious crime, similar privacy concerns and impacts arise.

However the powers of the NZSIS do not contain any guidelines on the exercise. I am recommending the Service's activities should be subject to the kind of guidelines that govern Police visual surveillance operations, which are contained in a 2012 Practice Note from the Heads of Bench [senior New Zealand Judges]:

“Applications for the use of visual surveillance devices should include:

- The intended locations of the devices (as specifically as possible)
- Their intended field(s) of view

²⁰ New Zealand Security Intelligence Services Act 1969, s 41B.

- The procedures to be adopted to keep private images (particularly of non-targets) not required for the purposes of the investigation.

Intelligence and security agency cooperation

I'll briefly turn now to my second theme. Cooperation between selected western states in certain areas of intelligence operations (particularly signals intelligence) is longstanding. However, since 9/11 there has been a significant increase in the scope and scale of intelligence cooperation.

The collaboration has increased 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.

Intelligence sharing occurs when one state communicates intelligence in its possession to another state. "Intelligence" may and often will, include personal information. Information sharing may, therefore, implicate data protection rules designed to preserve personal privacy.

Nor is intelligence itself collected on a strictly national basis, especially SIGINT, where data are extracted from global telecommunications, often regardless of borders.

Intelligence sharing engages two important dimensions of privacy protection.²¹

- the impact of global interception capability in a world in which privacy is regulated nationally; and

²¹ Born, Leigh and Wills, *ibid*, Craig Forcese at pp 72-97.

- the consequences of the migration of private information, in the possession of governments or the private sector, across international borders, potentially from highly protective privacy environments to less protective jurisdictions. The latter of course is reflected in the *Safe Harbor* decision.

Broader and deeper cooperation between intelligence and security agencies represents a growing challenge to accountability. International information-sharing arrangements vitiate completely privacy requirements.

Privacy regulation is conducted on a national basis, creating an uneven pattern of privacy laws, some more demanding than others. Likewise, national oversight and review structures were designed for a different era and are, in the main, ill-equipped to deal with cooperation across borders. Cooperation between intelligence and security agencies has not been matched by cooperation between national oversight and review bodies.

This increasing accountability deficit presents perhaps the most significant oversight challenge in the field of national security today.

National oversight of intelligence cooperation

The extent to which national oversight bodies can cooperate, share information, perhaps even carry out joint inquiries, is seriously limited. In some jurisdictions, the legislation governing such bodies specifically prevents such cooperation. In others – such as New Zealand – the issue is not specifically addressed in the oversight legislation. I would argue it is implicit in my powers that I can look at how the agencies for which I have oversight responsibility share information and resources, but even then we come up against 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. 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.

The prohibition on the further dissemination of information is widely 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.

The third party rule is reflected in New Zealand, as in some other jurisdictions, in the freedom of information law that I referred to earlier.

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

What can be changed at a national level? 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)²² and/or the services could be required to brief oversight bodies on particular types of intelligence cooperation activities.

It may be that national oversight bodies can – subject to the possible constraints already mentioned - initiate inquiries into the cooperation of agencies with foreign services. By

²² Canadian Security Intelligence Service Act 1985, s 17(2).

way of example, my Dutch colleagues have two investigations underway into the cooperation of the Dutch intelligence and security services with foreign services.²³

International oversight

International accountability is also under-developed. Hardly surprisingly, states have not to date agreed to international oversight of their national intelligence agencies and seem unlikely to do so.

International monitoring institutions struggle to fill the gap, for example at the United Nations, European Union and Council of Europe levels.

There are rare examples of international organisations conducting inquiries into aspects of international intelligence cooperation: the inquiries conducted in 2006-2007 by the European Parliament (EP) and the Parliamentary Assembly of the Council of Europe (PACE) into the secret detention and unlawful transfer of suspected terrorists on European territory.

International accountability could take the form of either or both of an international body or networking and cooperation between national oversight bodies. The recently appointed UN Special Rapporteur on the Right to Privacy will certainly have a role, given his extensive mandate, and stated focus on surveillance oversight.

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. My work is assisted by, eg from the United Kingdom, the Intelligence and Security Committee's report,²⁴ the RUSI report,²⁵ David Anderson QC report,²⁶ Privacy

²³ Review Committee on the Intelligence and Security Services, Annual Report 2014/15, p 17.

²⁴ Intelligence and Security Committee of Parliament, *Privacy and Security: A modern and transparent legal framework*, March 2013.

and Civil Liberties Oversight Board on s 215 Patriot Act²⁷ and the United States National Research Council report to the President on technical options regarding bulk collection.²⁸ Inquiry reports from oversight bodies in other jurisdictions are useful at a number of levels – they 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 prevent the oversight body from publicly describing the same or similar activities.

These kinds of public reports 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.

International cooperation

There is however a case for more conscious collaborative oversight of different countries whose intelligence agencies are working closely together.

Craig Forcese, a Canadian academic, advocates what he calls “borderless review”: that is, parallel investigations, undertaken by oversight bodies in two or more states to examine in a given case the role of their respective services. That however would likely require some form of international agreement between participating institutions, to provide the

²⁵ The Royal United Services Institute, *A Democratic Licence to Operate - Report of the Independent Surveillance Review* (July 2015).

²⁶ Ibid, footnote 4.

²⁷ Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program operated pursuant to section 702 of the Foreign Intelligence Surveillance Act* (July 2014) and *Report on the Telephone records program conducted under section 215 of the USA Patriot Act and on the operations of the Foreign Intelligence Surveillance Court* (January 2014).

²⁸ 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.

legal framework for such cooperation. In some jurisdictions that may be prevented by current national legislation.


Summary

In summary, oversight bodies can engage at a national level to ensure laws that are adequate to protect privacy, within the confines of national security.

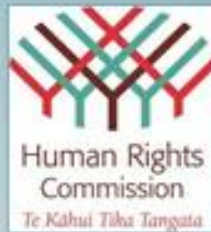
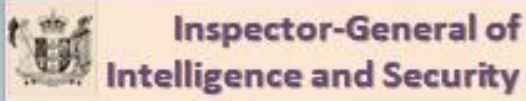
Most importantly, they can use their often significant powers to probe the activities of the agencies and to report publicly and as fulsomely as possible.

They – we – must move to enhanced cooperation, underpinned by legislative authority if possible, at an international level.

That cooperation – both domestically and internationally – increasingly needs to be between specialist oversight bodies and DPAs, if it is to be truly effective.

 @IGISNZ

NZ Network of Oversight



Amsterdam 2015