Privacy versus Security

The False Dichotomy and the Myth of Balance

Privacy Commissioner John Edwards

New Zealand Institute of Intelligence Professionals Annual Conference

8.45am – 9.25am

Wednesday, 15 July 2015

Rydges Hotel

Wellington

Introduction

Today you will hear many speakers talk of the need to "balance" different rights and powers in society. In my area, privacy, at its extreme, I hear even quite senior and supposedly sophisticated individuals present the community with a stark choice. You can have your privacy, and get blown up on a bus or train or airplane, you can give it up to the benign forces working to protect us and be safe, confident that only those who mean us harm are the targets, so the rest of us have nothing to be worried about.

I urge you to reject such insultingly simplistic false choices. To reject the notion of dichotomy as a useful means of framing the debate. When we engage in that debate the options are presented as poles on a spectrum, and that our only task is to allocate the trade-offs and arrive at that point of equilibrium, or "balance" between our right to individual liberty, autonomy and privacy, and … what? The right or duty of the state to keep us safe? We are entitled to both privacy and security.

One of the reasons we must reject an approach which necessarily implies an engaged population willingly entering into a social contract to surrender certain rights and liberties in exchange for certain services of security and intelligence agencies is that, to borrow from economics, we have a market failure. A contract (be it social or economic) requires each contracting party to have good information. The nature of

intelligence and security work means that that is not possible. Much of that work must take place in secrecy. The techniques employed must remain a mystery to the populace. This creates an information asymmetry between the supposedly contracting parties. My basic education in economics and public policy tells me that an information asymmetry is one of the causes of market failure, and is a legitimate reason to look to regulation to even the playing field.

So how does society engage in the conversation with government when it lacks the information necessary to make a fully informed choice about the "balances" and trade-offs?

Today I'd like to talk about the relationship between security and intelligence agencies and the community. How those agencies derive their legitimacy, and how that legitimacy can be harmed, or enhanced. I would no more presume to tell you how to do your job than I would instruct a surgeon on how to remove a tumour, but I, like everyone else in the community has an interest in ensuring that the surgeon is properly trained and resourced to do her job, and is supported in a culture of continuous improvement, and self reflection and is subject to robust systems of accountability.

We live in a time of unprecedentedly rapid technological, and geopolitical change. This presents opportunities, and threats for the security community. To return to the medical analogy for a moment, when a new technique or device is discovered or invented, we want the surgeon to be able to use it (especially if it relates to our own illness), but we also need to ensure that the potential risks and benefits are properly understood before deploying it. I'd like to explore how accountability mechanisms can keep pace with change, and not get left behind and rendered obsolete.

Artistic perception

There is some urgency to this discussion. The activities of security and intelligence agencies have never been such a prominent part of the public consciousness, popular culture or public discourse. This year's New Zealand representative at the world art fair, the Venice Biennale this year is Simon Denny, who's project "Secret Power" takes the New Zealand connection with Five Eyes and the NSA in particular as its theme. The $1million project ($700 000 of which is publicly funded) has been

given two exhibition spaces; the Biblioteca Nazionale Marciana (Marciana Library), in Piazzetta San Marco, in the heart of the city, and the terminal at Marco Polo Airport, on the outskirts. Here is the description of the work from the website

> In the Library, Denny has installed a server room, with server racks and a workstation. In addition to holding computer equipment, the server racks and workstation double as vitrines, displaying a case study in NSA visual culture, consisting of sculptural and graphic elements based on the work of a former NSA designer and Creative Director of Defense Intelligence David Darchicourt and the Snowden slide archive, suggesting links in iconography and treatment. The server room resonates with the Library's decorated Renaissance-period interior, with its maps and allegorical paintings—Denny's inquiry into the current iconography of geopolitical power being framed within an obsolete one.
>
> The Airport terminal—a busy hub for millions of travellers—incorporates restricted spaces, surveillance spaces, and interrogation spaces, and is equipped with high-tech security systems. Reproductions of the Library's decorated interior across the floor and walls of the arrivals lounge traverse the border between Schengen and non-Schengen space.

Acclaimed rock band Shihad last year released an album entitled "Five Eyes". It includes the following lyric:

> They hear everything you said
>
> The days of privacy are dead
>
> You've been lead to believe in this fantasy
>
> In a country where freedom's been sold
>
> Five eyes
>
> Looking down
>
> From Waihopai they can spy on you and me

From ECHELON the world's spied on indefinitely

In another corner of the artistic spectrum, my office commissioned an exhibition of privacy-themed artworks by Vincents Community Art Workshop in Wellington.

We didn't give them any steer on what to produce, but it was interesting to see that in the exhibition, a number of the artists explored the theme of government surveillance on the individual. I'll be showing you a number of those images this morning.

Public perception

If artists are canaries in a coal mine - revealing warning signs of issues that go on to grip the wider public's imagination – then the privacy implications of surveillance is evidently one of these issues.

Every two years, we gauge public opinion about privacy issues.

In the 2014 survey, we found 63 % of respondents were concerned about surveillance in New Zealand by overseas governments. 52% were concerned at surveillance by New Zealand government agencies.

Survey results elsewhere also indicate a level of public concern about surveillance which did not realistically accord with the activities of surveillance agencies. The National Security Communications Team commissioned a survey last year which found that 29 % of respondents think that New Zealand intelligence agencies are interested in their private communications!

The former head of the GCSB, Ian Fletcher, told our Privacy Forum last year that no state – even the most fearful - had the resources to monitor the internet closely. But that doesn't alter the perception and the perception can affect people's behaviour as well as sense of well being.

His comments presaged a panoply of security events and threats. We've had the rise of Islamic State, the Charlie Hebdo killings in France, and extremist attacks in Canada, Australia, China, India, Tunisia, Egypt, and the United States.

Deliberate, cold blooded targeted violence against the public and our national interests creates a justification for surveillance powers to be exercised by the state.

But if you are a democratic country that values transparency the use of those powers needs to be proportional, and accompanied by checks that ensure accountability.

Intelligence overreach

There is an element of selection bias in reporting the accountability and adherence to the rule of law sound governance in relation to intelligence services. That is, we only hear about things when you are caught out getting things wrong. But there have been some instructive examples of operational overreach which can undermine the legitimacy of the agencies actions in the eyes of the public.

You will all be familiar with the most famous of these. Dr WB Sutch, was accused of breaching the Official Secrets Act by passing information to a Russian national in Wellington in 1974. He was acquitted. There was an Ombudsman's investigation and a change in the focus of the SIS from counter-subversion to counter espionage.

It was not until 2008 that Sir Guy Powles' Top Secret report was published. It said the Service was involved in "clear breaches of the law", in the manner in which it entered Dr Sutch's office, and tapped his telephone.

In 1996, after SIS agents broke into the home of the free trade activist Aziz Choudry in Christchurch, the Crown was again found to be in breach of the law, and was forced to settle a damages claim from Mr Choudry and to apologise.

The Ahmed Zaoui affair between 2002 and 2007 also left a deep impression on many that government agencies might well have been working with the wrong intelligence, and that the reliability and motivations of intelligence agencies in other jurisdictions could not be taken for granted..

More recently, there have been the well explored repercussions to the GCSB for illegally intercepting Kim Dotcom's communications.

Bill Sutch, Ahmed Zaoui, Aziz Choudry and Kim Dotcom - these four names became household ones, in main or in part, because of perceived or actual operational and legal intelligence failures.

Confidence was also dented by the Police in its Urewera operation in 2007, and once again with the more recent Red Devils case – both of which involved covert surveillance, and in the latter case, deceit.

While it is true that there is something of a silver lining, in that these cases show how accountability can work, they also highlight the risk to the reputation of the agencies, and the legitimacy of their work by suggesting an operational culture that functions outside the Rule of Law. Now I don't believe that to be true, but if that is the message from those cases that is reaching those who are already sceptical, or suspicious of the intelligence community, then that perception can skew the public discussion, and call into question the legitimacy of those agencies operations and role in society.

Having said that, people do accept that much of the work carried out by our intelligence and security agencies needs to be carried out in secret but there's also an expectation that there must be oversight and proportionality.

I hope I am able to make the argument that trust and confidence in our intelligence networks has positive effects for our society, our international relationships and our economy.

Economic implications

This talk of perceptions, and legitimacy and the social contract is all very well, but what does it mean in practice?

One aspect of the fallout of the documents leaked by Edward Snowden, and interpreted by him and his journalist collaborators is that overseas buyers now trust American-made technology less because of fears of built-in access for US spy agencies.

A report by the Information Technology and Innovation Foundation this year says the American technology industry is underperforming because of the Snowden leaks.

It is the reverse of what the Americans have been accusing the mainland Chinese telecommunications company Huawei of having the capacity to do for the government in Beijing. The irony is writ large.

In a report in 2013, the ITIF put a dollar figure on what the lack of trust in American cloud computing might look like by 2016 - between 21.5 billion to 35 billion US dollars.

It has since revised its original estimate to encompass the entire US tech industry saying that by next year, "the economic impact of US surveillance practices will likely far exceed ITIF's initial 35 billion US dollar estimate".

The updated report concludes the US government's failure to reform many of the NSA's surveillance programmes has damaged the competitiveness of the American tech sector and cost it a portion of the global market share.

EU adequacy status

Here's an example that involves us.

EU law requires that when personal data is transferred outside the European Union, EU countries must ensure that the country receiving the data provides an "adequate level of protection" for the data.

In 2012, the European Commission examined New Zealand's privacy and data protection laws and determined that New Zealand had an adequate level of protection for the personal data of EU citizens.

My Office worked for a number of years towards this outcome. It has assisted successive governments in amending the Privacy Act to meet EU requirements and has worked with European institutions to gather the information they needed to make their assessment.

This was the European Union saying we trust you, we've examined your laws and institutions and we are giving you a special dispensation – a status accorded to only a small number of countries outside Europe: Argentina, Canada, Israel, Uruguay and New Zealand.

But after the Snowden's NSA revelations, the European Parliament instructed its Committee on Civil Liberties, Justice and Home Affairs to conduct an enquiry on electronic mass surveillance of EU citizens.

The committee's report noted the involvement of New Zealand, Canada and Australia in the Five Eyes programme. It questioned whether our "adequacy" determination should be revisited in light of mass NSA surveillance.

I have met with the head of the Data Protection Unit at European Commission, who expressed a desire to be kept appraised of any developments which might affect New Zealand's adequacy rating. I have undertaken to provide him with information that he needs to respond to questioning from the European Parliament, and I am hopeful that New Zealand will not be unfairly tarnished by allegations of mass surveillance undertaken by our Five Eyes partners.

Given our strong co-operative links with overseas intelligence agencies, it is vital to be mindful of the knock-on effects that international developments in this space can have on other aspects of our international obligations.

Recent overseas experience

Ian Fletcher – while he was in his role as GCSB director - last year assured New Zealanders that their metadata was not being vacuumed up by the GCSB.

He used Chairman Mao's analogy that the guerrilla must move through the people like a fish through water.

The state wants to catch fish, he said, the people doing really bad stuff. If you don't know you're a fish, then we don't care.

But in the United States, the hoovering up of phone metadata by the NSA could be analogous to sucking up the water as well as the fish. They are draining the lake, loading up the aquarium onto trucks and storing it away for later. We know there's been considerable kickback from America's allies, big internet companies and civil libertarian groups.

In 2014 the Privacy and Civil Liberties Oversight Board, which is a bipartisan body appointed by, and reporting to the President of the US issued a report finding the wholesale collection of telephony metadata from telecommunications providers, "lacked a viable legal foundation".

The board said that even though some secrecy in surveillance was needed, transparency could increase public confidence in intelligence and surveillance programs. It also concluded bulk data collection had not stopped terrorist attacks and had “limited value” in combating terrorism more broadly.

So – in the view of a government privacy watchdog, the collection was disproportionate, unnecessary, and unlawful.

In May this year, the US Federal Appeals Court similarly declared the programme illegal, finding that the NSA programme collecting the phone records of every American went beyond the authority granted by the Patriot Act.

The USA Freedom Act was anticipated to put an end to the mass collection of Americans’ phone records. It also demands more transparency of the Foreign Intelligence Surveillance Act court which oversees surveillance programmes.

But as we’ve seen very recently, the issue continues to run with the FISA court ruling the NSA could resume its mass collection programme temporarily, setting it on a potential collision course with the Appeals Court.

Meanwhile, in Britain, there’s also been a new focus on how intelligence agencies carry out internet surveillance.

Civil society groups recently unsuccessfully pushed for greater transparency in the way intelligence agencies carry out online surveillance. While the effort faltered, an inquiry by the British Parliament’s Intelligence and Security Committee concluded that security and intelligence laws should be overhauled to improve accountability.

In Canada, there’s been a lot of debate about the Security of Canada Information Sharing law and what has been called ‘total information awareness’. The law enables government information sharing for security purposes between all government departments and other agencies.

My Canadian counterpart says the law could lead to disproportionately large amounts of personal information being collected and shared and that it was excessive and lacking in balance.

Winning back trust and confidence

The overseas trends I've highlighted show a discernible movement towards more formalised oversight of intelligence agencies and their legal obligations.

I was very impressed on a recent visit to the Department of Homeland Security in United States and how the agency made privacy and transparency a top priority.

Its Privacy Office regularly subjects its activities – and this is the Department that is responsible for everything from border security to cyber security - to rigorous Privacy Impact Assessments. These are then made public on its website.

There's also been a relaxing in the United States on a prohibition on transparency reporting by companies like Google, Microsoft and Facebook on the number of people's accounts affected by government agency searches.

Companies can now report the number of requests for customer data authorised under the Foreign Intelligence Security Act, in bands of 1000 transactions. Although being able to find out how many Gmail accounts had been accessed by the NSA to the nearest 1000 is far from complete openness, it is a step up – and contrasts with the complete ban that existed before.

There are similar currents elsewhere.

A report commissioned in Britain by the Prime Minister David Cameron in response to Edward Snowden calls for a 'clean slate' approach in legislating on surveillance.

The introduction to David Anderson's 373-page report - A Question of Trust - warns modern communications networks can be used for cyber-attack, terrorism and espionage to fraud, kidnap and child sexual exploitation.

"A successful response to these threats depends on entrusting public bodies with the powers they need to identify and follow suspects in a borderless online world. But trust requires verification. 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 Global Commission on Internet Governance appeared to echo Anderson's call in its recent statement in April.

Confidence needs to be restored in the internet for it to remain a global engine of social and economic progress, the commission says, and what is required is a new social compact to protect digital privacy and security – and "abuses should be amenable to appropriate redress, with access to an effective remedy provided to individuals whose right of privacy has been violated by unlawful or arbitrary surveillance."

These calls to rethink security, surveillance and accountability are already part of a process we in New Zealand are currently undertaking.

It may be that it is folly to think that we are on a journey towards transparency and accountability of intelligence and security agencies that has an end point. It is more realistic to accept that we live in a very fluid and changing security environment, and there will be times when the threat level is such that the application of more intrusive powers is temporarily justified. The oversight and accountability arrangements need to be flexible enough to adapt to these changing environments, and robust enough to point out when those threats have lessened or passed, permitting greater restraint or scrutiny of the activities of the agencies.

Privacy Commissioner's oversight

My Office is part of the oversight matrix for intelligence and security agencies.

Domestically, the 2013 amendments to the GCSB Act included provision for the GCSB to develop a personal information policy in consultation with the Privacy Commissioner and the Inspector General of Intelligence Services.

The GCSB has to report the results of audits conducted under the policy to my office and I can then raise any issues arising with the Inspector General.

There are two other ways my office contributes to oversight of the GCSB – and the SIS.

I can investigate complaints about access to and correction of personal information.

While security agencies have an exemption from many of the privacy principles under section 57 of the Privacy Act, they are still subject to principles 6 and 7 - the

rights to access and correct personal information. Principle 12 also applies limits to the use of unique identifiers by our intelligence agencies.

People are entitled to request access to information held about them by the GCSB and the SIS, and if they receive it, to request correction of that information.

The other contribution I can make is through regular meetings with the other agencies responsible for overseeing security and intelligence agencies.

These meetings include my office, the IGIS, the Chief Ombudsman, and the Auditor-General. Together we will be able to ensure that our efforts are as informed and coordinated as our respective legislative schemes permit.

Any complaints to me about the intelligence agencies are subject to a special process.

These complaints may not end up in the Human Rights Review Tribunal, but my office can refer a complaint to the Inspector General or I can investigate and report it to the agency concerned.

If the agency does not take appropriate action in response, I can then report to the Prime Minister who must table the report in Parliament.

Intelligence agencies also have statutory requirements to consult with my office about any proposed changes to the handling of personal information. For example:

- As I've already mentioned, the personal information policy being developed by the GCSB
- the rights of direct access by the SIS to the Customs databases, in accordance with section 280(m) of the Customs and Excise Act.

One of my functions is to also to make statements to government and public statements about adverse impacts on the privacy of the individual.

I can also carry our own motion investigations into any matter, if I consider there are systemic issues that need to be addressed.

Transparency reporting project

I welcome the encouraging steps I have seen security agencies taking to be more open about their policies around personal information, and to take a genuine, case by case approach to decision about what information should be made available both under the Privacy Act and the Official Information Act.

Another area that I am in the process of exploring, which holds some promise in terms of the promotion of openness and accountability is the practice of transparency reporting. Transparency reporting has the potential to increases public awareness of the information gathering activities of law enforcement and security agencies and encourages companies that hold the information to be open with consumers about the limitations of confidentiality, and the ways in which they cooperate with agents of the state.

Businesses increasingly hold a wealth of personal information that may be useful for governments' law enforcement and national security activities.

Agencies such as the Police, Inland Revenue, the Ministry of Social Development, and a host of others have powers to obtain information from corporations, about individuals, often without the knowledge of those involved.

Transparency reporting, publishing reports of how often these requests or demands are made, and how many individuals are affected was initiated by Google, and others such as FaceBook, Vodafone, Trademe, and others have followed suit.

There is value in a public declaration by those holding the information about the disclosures they have been compelled to make.

My office has been working on a pilot transparency reporting project. We've recently finished meetings with our initial group of stakeholders and found agencies generally supportive of the concept.

This year we intend to trial asking companies to keep a standardised record of requests for information from law enforcement agencies and to report this information to us. We will then publish this information. If you are interested in seeing how our work in this space develops, keep an eye on our website as we publish the results of our research, and the first of the transparency reports.

We accept that intelligence agencies operate with a high degree of secrecy. At this stage our transparency reporting pilot will not include information about access to personal information by intelligence community.

However one of the downsides of operating under strict secrecy is it creates gaps in the information that the public has available to it.

This space is then filled with speculation and conspiracy theorising which have a deleterious effect on agencies, their ability to operate, and their social licence.

Conspiracy theorists work in a vacuum of information or give truth to the maxim that a little information is a dangerous thing. On a page full of dots, they are able to plot their own lines.

Take, for example, the 2011 Southland Times' story that a team of Mossad agents were on an identity theft mission in New Zealand and fled the country after the deaths of three countrymen in the Christchurch earthquakes.

Because the Southland Times believes it to be true, doesn't make it true.

Another risk of secrecy is that complacency and unprofessional practices can creep in. We have seen this in material released by NZSIS about Kim Dotcom. I applaud the Director's decision to release emails whose authors clearly never thought they would be seen outside the organisation, let alone published by the Herald!

The biggest risk of a rule of near total secrecy is that unverified and possibly inaccurate information is gathered and relied upon. Such information can have extremely prejudicial effects on individuals, for years or even decades, with those affected having very little right of recourse. There will be people here who continue to believe Ahmed Zaoui is a terrorist, or that the recently released Mitrokhin Papers prove WB Sutch was a Soviet "asset". Both claims will be hotly denied by advocates for those who insist those two, and goodness knows how many others were victims of duplicitous intelligence agencies in other countries, with their own murky motivations.

Cooperative international oversight

In this interconnected world, it has become more and more important for agencies to collaborate across boarders. The Five Eyes alliance for example creates strong bonds between the operational agencies involved - less so to date amongst the oversight agencies. I am interested in exploring, with my colleague the Inspector General, whether there would be benefits in formalising links between our counterparts in the alliance, and beyond.

The Dutch Review Committee on the Intelligence and Security Services expressed the problem nicely in its 2014 Annual Report

> The Committee points out that more and more often the question is raised in international forums whether national oversight is still sufficient. The work of intelligence and security services extends beyond national borders; operations are carried out together with other services and exchanging information is a commonplace procedure. The mandate of national oversight bodies is limited to the information about such cooperation that is available at the own national service. This makes it difficult to examine what foreign services do with data provided by a national service. Often, it is not possible for an oversight body to ascertain whether the data which the national service receives from abroad was collected lawfully. A national oversight body can only examine whether the national service provided or received information lawfully. This limit on what national oversight can do is also referred to as an 'accountability deficit'.
>
> Bridging this deficit is not easy. It has been suggested to draft an international 'intelligence codex' containing the basic rules for the work of intelligence and security services. An international oversight body would then monitor compliance with the codex. Especially the latter proposal will easily be a bridge too far in the world of national security. Cooperation between intelligence and security services is a complex process, which takes place on the basis of strict conditions. It is dictated by sovereignty and national interests. It is not to be expected that states will be willing to accept restraints on this most delicate element of their sovereignty.

This will be one of themes of the International Conference of Data Protection and Privacy Commissioners later this year.

Review of the security intelligence agencies

Meanwhile, we now have an independent review of our intelligence and security legislation.

It was interesting to hear Sir Michael Cullen emphasise the word trust in an interview on Morning Report earlier this month.

Agencies need to be seen to be acting lawfully - and our laws should support trust and confidence.

The review also makes it a convenient time to consider a fresh approach to our current oversight mechanisms.

The current model is agency-based rather than function-based. But intelligence gathering is not just limited to the GCSB and the SIS – both of which grew out of different functions – the GCSB out of the military and the SIS out of a special branch of the Police.

There are intelligence functions at the Ministry of Primary Industries, Customs, the Police and Defence. Should these agencies be included in reshaping our intelligence framework?

With the forthcoming reviews of both the security and intelligence legislation, and the Privacy Act, we have an opportunity to look at other oversight options.

Does it continue to make sense to maintain an institutional focus as opposed to a more wide-ranging and consolidated approach to oversight? The security agencies are doing important work, of course, but is it so qualitatively different from the important public service work of so many other departments and organs of state that they should have unique, and more opaque accountability arrangements?

We need to have an honest, and to the greatest extent possible, open conversation about the relationship between the security and intelligence agencies, other Government departments. Parliament, and the people of New Zealand.

The review gives us an important opportunity to have that conversation to ensure New Zealanders can have confidence in the institutions which are there to promote their interests, and keep them safe. I will be participating in that process, and

ensuring that the importance of the rule of law, of proportionality, and privacy are at the forefront of the minds of the reviewers, discharging my role, as an advocate for privacy.

My parting comment might surprise some of you. Whether the oversight arrangements for the security and intelligence agencies change, or not (and I hope they do evolve in some of the ways I've indicated), what is crucially important is that the agencies must be funded for accountability. Checks and balances are critically important, but they don't come cheap. From what I know of the intelligence agencies, they are extremely lean in terms of corporate support, favouring, as you might expect, the operational side of their work as the recipient of resources.

If we want accountable engaged agencies, then we have to resource them to be able to do some of the things I've indicated in in this talk, to review, reclassify and release old information, to undertake and to publish privacy impact assessments, and to engage with enquiries by my colleagues the IGIS, the Ombudsman and to keep pace with the developments in partner organisations overseas.

ENDS