Privacy Commissioner speech notes

10 Points in One Day

9.45-10.30am, 22 May 2014

The Rydges

75 Featherston Street

Wellington

TEN POINTS

Thank you for the opportunity to speak. I'm just getting into the swing of my role as Privacy Commissioner and it feels like a crucial time to be taking up the position.

There's unprecedented public interest in privacy and heightened anxiety over and concern with privacy and a perception that the right to privacy is being swamped by rapid technological advances in information collection, storage and dissemination.

We've seen how Edward Snowden and the NSA have put privacy on the global agenda and it has prompted a raft of questions about how safe and private is our information.

I've come up here with a snapshot or update if you like of where the Office is currently – our work, our priorities and the kinds of changes that are happening for the Office and in the wider privacy environment.

1. UMR Survey

Every two years, we take the temperature of just how concerned New Zealanders are about their individual privacy. The results of this year's UMR survey were released for Privacy Week earlier this month.

Among the findings, one trend has been evident for a while.

The results show New Zealanders are increasingly aware and concerned about privacy, especially over information held about them by government agencies, by businesses and online providers.

One in two New Zealanders now say they are becoming more concerned about privacy issues. This is the highest yet recorded level in our two yearly tracking survey.

Meanwhile, four out of five New Zealanders say they are concerned about the security of their own information on the internet.

One theme that has emerged from the survey is a feeling of lack of control:

- 37% do not feel in control of the way businesses use their information.
- a third of New Zealanders (33%) say they do not feel in control of the way government agencies use and protect their information.

In the accompanying qualitative research that we undertook, participants made comments about interacting with government.

One said: "*You don't have a choice because if you want to get what you want then you have to share your information and hope they won't release it*."

And another participant said: "*I think you are basically stuck there because you are in a position where you need to give them the information if you want their service.*"

There's also awareness that it isn't just the government that is collecting personal information.

Three out of five respondents say they use Facebook. But this has led to an interesting change that indicates there's a growing level of social media literacy among New Zealanders. For example, three out of four New Zealanders (77%) say they have changed the privacy settings on their Facebook page.

The internet and online social networking are fields of work that couldn't have been envisaged by the architects of the Privacy Act when it was enacted in 1993.

Since then, there have been huge technology-driven changes and challenges to privacy, and my Office has to keep up to speed, and where possible, to get ahead of the game.

2. My approach to compliance

The concept of privacy is subjective, contextual and dynamic and personal information is ubiquitous.

The Privacy Act is a set of principles that are sufficiently flexible to provide a framework for agencies for the vast majority of scenarios involving personal information.

Its information privacy principles are technology neutral, and based around each agency's own legitimate business needs.

Except for principle 6 in relation to public sector agencies, they are not enforceable in a court of law, but the Courts have been prepared to take notice of them in assessing the actions of parties to disputes - for example in the employment context or in discovery, as well as aspects of tort law and human rights cases.

Two significant decisions for employers are *Wrigley v Massey University* and *Waters v Alpine Energy*.

In Massey, the Employment Court held that an employer carrying out a restructuring should have to provide the unsuccessful candidates with information concerning other candidates due to the good faith obligations in the Employment Relations Act.

My office differed from the Employment Court Bench in its approach to the employees rights to other candidates' information and was asked to work with the Department of Labour (now MBIE) on a policy response.

The result of that work is the Employment Relations Bill (105-2). The Bill appears to be intended to provide the Employment Court with more options for protecting the privacy of candidates should similar fact situations arise.

Waters v Alpine Energy is similarly challenging. In March, the Human Rights Review Tribunal ordered the disclosure of all job applications, CVs and reference checks to an unsuccessful candidate, after that candidate alleged he was discriminated against on the basis of his age. The disclosure was made under discovery after Alpine Energy had refused to hand over the documents on the basis that they were confidential, or were not in the company's possession or had been destroyed.

That decision is now being appealed. I have applied to intervene in proceedings and will make submissions on how the Court might properly take privacy into account while still ensuring the parties have all the information they need to conduct the investigation.

My vision as Privacy Commissioner is to make privacy easy.

I want to make privacy easy for government and business to comply with; to make sure they make privacy an easy option for consumers to choose; and to make it easy for people to access effective remedies when their privacy is breached.

We will be engaging actively to provide advice and guidance but, in my experience, agencies need incentives to seek and take that guidance and advice on board and to apply it.

One important element of any regulatory regime is the enforcement end of the compliance triangle. I want to take a stronger line on enforcement, to make agencies more aware of their privacy obligations and show them clearly where the boundaries lie. Enforcement action also provides guidance for other agencies about what the law means and how to manage personal information successfully.

At the moment, I can't generally make legally binding rulings (except in a couple of narrow and specific areas). But there are options. For instance: I can push things down a litigation track; I can require agencies to provide information for my investigations and report my views to the appropriate people (eg chief execs, government ministers or the Prime Minister); and I can report publicly on agencies that breach the Act.

With public reporting, if the agency has fixed the problem up, that's one story. Take for example, the independent report into EQC carried out by my Office and the Ombudsman's Office. There were serious problems but EQC accepted all the recommendations and committed to fixing them – a better look than it would otherwise have been. EQC recently advised us that it has completely dealt with the backlog of access requests.

If the agency doesn't fix their practices, that's a different story.

3. Charging for access to credit reports – a case study

We carried out an own motion investigation into one credit reporting company - Veda Advantage - and its charges for urgent requests by consumers for access to their own credit information.

Credit reports are usually to be made available to the individuals free of charge but credit reporting agencies can charge a reasonable sum for people urgently wanting their credit information.

It appeared to me that Veda built a business model around this exceptional ability to charge 51 dollars and 95 cents for access within five days. I found this to be unreasonable and unlawful.

My Office sought undertakings from Veda:

- That it only charge for the actual cost of preparing and delivering the information.
- That it cease charging for other aspects of processing urgent requests.

Veda did not provide these undertakings. In my view, Veda was, and remains, in breach of the law. Its charge for urgent requests substantially exceeds what is reasonable to charge consumers. This is not only a breach of the Credit Reporting Privacy Code but also constitutes a barrier to exercising fundamental access rights that damages public trust in industry practice.

We were then faced with various options. One of them was should we publicly name an agency? Under section 116 of the Privacy Act, the Privacy Commissioner and his staff must maintain secrecy. However, there is an exception to that obligation where the Commissioner believes a disclosure is necessary for the purposes of giving effect to the Act. For various reasons, including consumer education and the small size of the credit reporting market, I decided to publicise the identity of Veda as the agency in breach.

Our second option was to refer the matter to the Director of Human Rights Proceedings. But this would give the matter to another authority to make a determination on an issue which we had already investigated and determined was a breach of the Act. Referring the matter would also require litigation and prolong the process of resolving the issue.

What we have done is to proceed to amend the Credit Reporting Privacy Code to limit a charge for urgent access requests to 10 dollars. The submissions deadline for our proposal closed last week.

4. Law Reform – access requests

My next couple of points are about proposed law reform.

The Privacy Act has been reviewed by the Law Commission which made comprehensive and well-founded recommendations on changing a 20-year-old law

and bringing it up to date.

One of the proposed changes is to give my Office the authority to order that information be given to people. This is a very significant one because over 60 percent of the complaints that come to my office deal with requests for access. Until we get that power though, I am going to do what I can within the existing law to lift practice in this area. Have a look at the recommendations in the EQC report. They include:

- streamlining the processing of claim file information requests;
- improving the quality of information and service provided by call centre staff;
- considering the automatic provision of property reports to owners; and
- improving the website delivery of information.

These don't just apply to agencies experiencing unprecedented demand for information. They are valuable across the board for how you manage your statutory obligations to provide access to information on request.

This is not a "nice to have" for individuals; it's a "have to have". Providing access is a key part of your business, a key part of the relationship you have with your clients - not some legal compliance exercise.

I'll be focusing a lot in the short to medium term on how agencies are meeting their obligations to provide access in a timely way. Our experience at the moment is that government agencies are struggling and are not always succeeding. I'll try to help you get it right, but I won't be shy of saying when you've got it wrong. People have had a right of access to information held by government since 1982. This is not new or unfamiliar territory.

5. Law Reform – mandatory breach notification

Another potentially significant change on the horizon is a shift to mandatory breach notification. The Privacy Commissioner currently depends on voluntary breach notification and on the willingness of agencies to alert us if there's been a data breach.

A law change may not mean the end of spreadsheets going to the wrong recipients, but we'll have to be notified when serious breaches happen.

We have started to track breach notifications more formally because this is a matter of external interest and importance. There has been a noticeable pick up in the business sector particularly among large businesses.

The change to mandatory breach notification will bring us in line with many overseas countries with well developed privacy protection laws. New Zealand has been lagging internationally by having a voluntary system.

Breach notification is an essential part of the process to remedy the harm caused by a breach and to make changes to prevent it happening again. The KPMG report in 2012 on the well publicised 2011 ACC data breach made 44 recommendations. ACC has since implemented 37 of those recommendations and reduced the number of data breaches substantially.

But you will have since heard about the controversy over the ACC 167 consent form. It is an example of the long tail of the process within ACC to reinvent its privacy practices.

I also want to say a word about spreadsheets. If you hold large amounts of personal information and you're using spreadsheets to corral it all, you're opening yourself up to user error and possibly breaching your obligations under the Privacy Act.

In data breaches reported to us involving spreadsheets, the numbers of individuals affected per breach has ranged from dozens to thousands. If you have to maintain a database, you should be thinking about a purpose built database management system – one that only generates the results you need. This approach can also help lay the groundwork for a more customer-driven solution to accessing records.

If you must use spreadsheets, please don't email them around. Export the data you need from the spreadsheet and just send what you need. Convert the sheet into a PDF document or put the relevant data directly into a table in the email. Finally, if you absolutely need to email a spreadsheet to someone, use a password to protect it and check who you send it to.

We've recently published our Data Safety Toolkit. It is a guidance resource on preventing and dealing with data breaches and it is now available on our website – privacy.org.nz.

6. Funding boost

My Office has been operating with static resources for some time and its workload has been steadily increasing. It is therefore good news to us that we've been allocated an additional 1-point-9 million dollars for the coming financial year and 1-point-7 million dollars in ongoing years, to deal with the new work from Better Public Services initiatives, for example.

This additional funding will enable my Office to better tackle its workload and to be pro-active in anticipating changes in the privacy domain and to work better to protect an individual's right to privacy.

7. Approved Information sharing agreements

One of the Law Commission's most significant recommendations is to provide for a mechanism by which government policy programmes involving inter-agency cooperation could be facilitated in an administrative way that did not involve statutory amendment.

The government fast-tracked that recommendation and it was enacted in February 2013. The framework provides for the authorisation and oversight of Approved Information Sharing Agreements – or AISAs.

Since then, one agreement has been passed and there's a handful under further development. Potential uses include protecting vulnerable children; improving multiple services for youth with complex needs; and making tax and welfare fraud easier to detect.

AISAs will be able to clarify and improve the rules around how agencies share personal information, while ensuring safeguards are in place to protect an individual's privacy.

8. Centralised data collection and analytics

The argument for government to maximise the value of data it collects as a by-product of the services it delivers is compelling and an increasing trend. Governments are becoming more and more interested in ensuring that limited resources are used where they are most effective.

With the greater integration of data and new techniques in analysing it, there's great potential to reinforce the evidence base behind policy decisions.

But the wider collection and availability of data about people comes with risks to individual privacy. As more data sets are linked together, there are an increased number of vectors for re-identifying individuals.

In New Zealand, we've recently seen aggregation of data sets across departments, with the government's decision to significantly expand Statistics New Zealand's Integrated Data Infrastructure.

There is an important conversation to be had about whether the private sector should also have access to data held by government. It is for this reason that the ministries of finance and statistics have instigated the New Zealand Data Futures Forum – to explore the future of data sharing between the public and private sector.

The Data Futures Forum is currently seeking feedback on how businesses, government, researchers, and the public can safely share data in an environment where privacy is paramount and trust is maintained. I encourage you to get involved in this vital discourse.

9. New priorities

The government is promising a stronger focus on privacy and security across the public sector. One of its responses to a number of privacy embarrassments among several leading government agencies has been the creation of a Government Chief Privacy Officer.

This new role allows for centralised leadership of privacy protection across government and provides support to the Government Chief Information Officer. It sends a very strong signal but it comes with a caveat. The success of the GCPO will depend on the extent of support and uptake among individual government departments.

For my part, I am looking forward to working with the GCPO because we both have important roles that complement and reinforce our highly compatible agendas.

Another relevant development is the Harmful Digital Communications Bill. The Bill is the government's response to findings of the Law Commission that existing remedies for harmful communication did not effectively address new forms of harm made possible by digital communication.

The Bill tackles cyber-bullying but it also changes the Privacy Act. Currently, under section 56, the Privacy Act does not apply where an individual collects or holds personal information for his or her own personal, family, or household affairs. Among other things, this means that the Privacy Act does not apply when people publish invasive and distressing photos of others they know in their personal capacity.

That's about to change. The Bill will amend the Harassment, Privacy and Human Rights Acts. When enacted, the existing section 56 exemption in Privacy Act would cease to apply once personal information is collected, disclosed, or used, if that collection, disclosure, or use is highly offensive.

10. Intelligence services

The GCSB has been thrust into the limelight following the Kim Dotcom extradition process which led to litigation which led to Rebecca Kitteridge's report which led to law reform. All of this coincided with the Snowden revelations and suddenly, everyone was discussing international intelligence and domestic intelligence surveillance operations.

The GCSB Amendment Bill was an omnibus piece of legislation that made amendments to the Government Communications Security Bureau Act 2003, the Inspector-General of Intelligence and Security Act 1996, and the Intelligence and Security Committee Act 1996.

The purposes of the bill were to make clear the statutory framework governing the activities of GCSB and to enhance the external mechanisms for the oversight of the country's intelligence agencies.

Our submission on the GCSB Amendment Bill last year advised that in our view it was not yet clear what type and level of oversight was most appropriate for the agency. Under the Privacy Act, the Privacy Commissioner can only consider whether the GCSB has properly responded to requests for access to, and correction of, personal information

I have no mandate to consider whether the GCSB is acting within the law under intelligence gathering, the collection and use of information and in providing assistance to other agencies. None of this changed with the Bill.

But the law change does improve the current controls over GCSB's collection and use of personal information. It requires GCSB to develop an internal policy in consultation with the Privacy Commissioner, for the activities covered by that code to be regularly audited, and for the results of the audit to be reported to me.

This provides my Office with a window into the activities of GCSB that did not exist before, and it signals a strong intention that GCSB would behave appropriately and be accountable for its activities.

Thanks for being here and listening to my own ten points. I'd be happy to answer any questions you might have.

ENDS