Trade Me speech
Friday 15 August
Wellington
20 minutes

Vision

Thanks for the opportunity to outline my approach, my priorities and to let you know what's coming up in the privacy environment.

I understand that the Chatham House Rule applies here. I'll exempt myself. I'm happy to talk on the record, and to be quoted and attributed. Rule or no rule, I wont be saying anything about Nicky Hager's book today.

In one of my earliest public appearances as privacy commissioner, I said one thing I might usefully do is to 'make privacy easy'. That has since become something of a mission statement.

- I want to make it easy for government and business to comply with the Privacy Act.
- I want to make privacy an easy option for consumers to choose.
- I want it to be easy for people to access effective remedies when their privacy is breached.

Communicating that vision

- We are taking more steps to communicate this vision and to build public confidence in the role the Office plays in safeguarding personal information.
- We've got to tell people what we are doing, so that agencies can learn from the way we resolve complaints and know about the contribution we make to policy projects.
- People need to have good information about their rights, the limits on those rights, and what to do if things go wrong.
- And we also want to be on the spot to help business make privacy work for them.

Engaging online

- One of the ways I'm trying to change the way the Office works is to do more to engage and interact online and through our website.
- This means using our blog, Twitter, YouTube and Facebook channels.
- One new initiative is to have a directory of privacy professionals on our website, to help develop a community of expertise.
- I want to ensure that our complaints process is as effective as it can be in obtaining resolutions for people. At a practical level, we will be providing for the online lodging of privacy complaints.

Being a tougher regulator

- Making privacy easy is the velvet glove. I also need to deploy the iron fist from time to time. Iron? Well maybe that is overstating it, lets call it a fist made of something between syrofoam and a reasonably heavy alloy.
- I want to better exercise the statutory powers that I have as a regulator.
- I plan to take a stronger line on enforcement and make agencies more aware of their privacy obligations.
- New Zealanders are becoming more concerned about privacy, especially about whether their personal information is well managed and protected.
- Our latest survey shows that half of all New Zealanders say they have become 'more concerned' about privacy issues over the past few years.
- It is my duty to respond to increasing public concern about privacy issues by getting tougher as a regulator.
- A crucial resort of any regulatory regime is enforcement.
- Responsive regulation means having a choice of responses in cases of non-compliance.
- Effective enforcement sends a strong message to businesses and government agencies about what the law means and how to manage personal information successfully.

Naming policy – Example 1

- One example of the type of enforcement response that we are looking at is to publicly name agencies in appropriate cases.

- Public exposure can be an effective tool – and sometimes it will be the best lever to ensure a change in practice.
- We're considering a departure from previous practice where an agency was rarely named in public - even where it appeared the agency had breached the Privacy Act.
- The new policy will enable my office to be a more effective regulator - especially in cases where non-compliance is repeated or systemic.
- For example, we named Veda as part of our process in amending the Credit Reporting Privacy Code.
- We've written a discussion document that will be circulated in the next couple of weeks.
- It will be followed by a submission process to allow the public and relevant stakeholders to comment on the naming policy before it commences.

Credit Reporting Privacy Code – Example 2

- A second example is the recent change to the Credit Reporting Privacy Code as an example.
- I was presented with a report earlier this year that showed that one of the largest credit reporting companies, Veda Advantage, was flouting the law and over-charging customers who were in urgent need of their credit information. You want your credit information? Sure, wait 20 days they said, or pay $51.95.
- I had several choices – do nothing but highlight the report; refer the case to the Director of Human Rights Proceedings (and wait three years for a result), or move to amend the Credit Reporting Privacy Code.
- I chose to go down the path of amending the Code.
- That amendment takes effect on 1st September and will limit the amount a credit reporter can charge for urgent access to credit information.
- That limit will be $10 – considerably less than $51.95 charged by the company in question.

Compulsory conferences – Example 3

- Another recent example of applying my our regulatory powers with more rigour is holding compulsory conferences between complainants and respondents.
- Calling compulsory conferences is a power that my office has under the Privacy Act and we've under-utilised this statutory tool in the past.
- It is now time to dust it off and apply it more often to bring complainants and respondents to a meeting and, hopefully, to reach a resolution.
- It can be a restorative form of justice for those who have suffered harm in a privacy breach.
- We'll soon be highlighting a recent case in our blog which we are using as an informal way of communicating and projecting the work of the office.
- You can expect a demonstration soon of how compulsory conferences work in an upcoming post.

Example 4

For public sector agencies, report to Ministers, even the PM

Counsel for child example

Privacy environment - increased resourcing

- It is a time of revitalisation and renewal for the Office.
- It's been a busy year so far, and our workload is continuing to grow.
- Up to now, we've been labouring under a fairly static level of resourcing.
- But that's changing, as we've recently been given more resources.
- In the last budget, the office received a funding boost of $7 million over four years.
- The increased resourcing will give us greater ability to respond to increasing and more complex challenges in privacy enforcement.
- The Government has signalled its intention to introduce a major reform to the Privacy Act.

Law reform

- Overall, my office will get more enforcement powers in a new Privacy Act.

Access determinations

- One major new change – the Privacy Commissioner will have the power to order that information be given to people.
- This is a very significant change because over 60 percent of the complaints that come to me deal with requests for access.
- I can't stress it enough to government and business: - Providing access is a key part of your business, a key part of the relationship you have with your clients. It is not some legal compliance exercise.

Enforcement notices

- A second major change is the power to issue enforcement notices to non-compliant agencies.
- I'd expect this to be a tool that will be rarely used, and probably as a last resort, but it is notably lacking from the current range of enforcement options.

Mandatory breach notification

- One significant change for both business and government will be the introduction of mandatory breach notification. This change will bring us in line with many overseas countries. New Zealand has unusual internationally by having a voluntary system.
- We currently receive numerous (and growing) **voluntary** breach notifications. These depend upon the willingness of agencies to alert us if there's been a data breach.
- We have started to track breach notifications more formally and report on them (see 2013 annual report).
- There has been a noticeable pick up in notifications from the business sector, particularly among large businesses.

- Under the reforms, actions such as failing to notify me of a privacy breach, or impersonating someone to obtain their personal information will be illegal and carry a fine of up to $10,000.
- Existing maximum fines - for example, for obstructing my office - will increase from $2,000 to $10,000.
- We are working closely with the Ministry of Justice and Parliamentary Counsel Office as they develop the draft legislation. It is likely to go before Parliament next year.
- Together with the better resourcing that the government has given the office, 2015 is looking like a big one from a privacy enforcement perspective.

Progress in information sharing across government - AISAs

- In its review of the Privacy Act a few years ago, the Law Commission was asked to consider options to facilitate information sharing between government agencies.
- The aim was to make it easier for information held by one agency to be shared with another government agency when providing public services.
- The Law Commission proposed a mechanism to allow agencies to enter into information sharing agreements that would be “enacted” by Order-in-Council.
- The Information Sharing Bill became law in February 2013 and we received the first application for an approved information sharing agreement (AISA) a few months later.
- Any agency proposing an agreement has to consult with me, and with other interested parties.
- Last year, there were some 34 proposals afoot, however, only two have been issued. We are actively working with two agencies on others.
- The realities of developing an AISA are proving more challenging in practice than it might at first have appeared.

Maximising value from data - Data Futures Forum

- We recently contributed to the New Zealand Data Futures report with a submission earlier this month.
- Looked at in a positive way, we can harness big data to gain valuable insights into the health system and health of populations, to improve clinical outcomes, and achieve cost efficiencies without intruding on privacy.
- Running against that is heightened awareness and concern around data collection and storage by government agencies and businesses.
- It is pleasing that the Forum recognises the role that good privacy regulation plays.
- Moves to implement Privacy By Design in the establishment of information collection, storage and sharing systems is very encouraging from a regulator's point of view.
- The Data Futures Forum report says in order to protect privacy and security, it recommends the application of privacy-by-design and security-by-design tools at all levels of a data-use initiative, and recommends the use of a Privacy Impact Assessment as part of the preparation of any data-use initiative.
- Another recommendation is the establishment of an independent data council, would also ensure a considered and deliberate approach to new ways of extracting maximum value from data.

Guidance resources

- My office is also intent on providing more guidance resources about how to comply with privacy laws.
- We will shortly have to embark on a comprehensive overhaul of our privacy guidance to make it as relevant as possible to the new law changes.
- This will be a big project - we have to be effective at explaining how the law reform will affect New Zealanders and their rights to privacy.
- We do have couple of new guidance resources that may be of interest to you:-
    - **Data Safety Toolkit** is an online resource on preventing and dealing with data breaches.

    - **Our Need to Have or Nice to Know** - Guidance for mobile app developers and businesses.
- Both are free and available at www.privacy.org.nz.