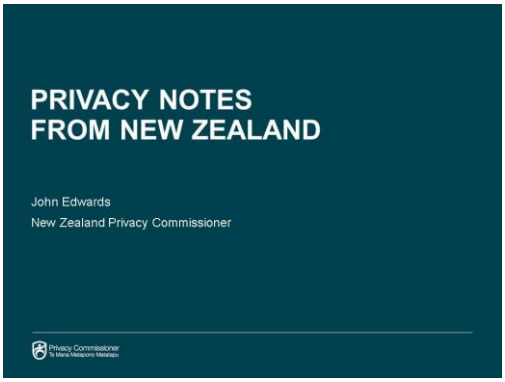
PRIVACY NOTES FROM NEW ZEALAND

PRESENTATION BY NEW ZEALAND'S PRIVACY COMMISSIONER JOHN EDWARDS

5TH EUROPEAN DATA PROTECTION DAYS
EURO FORUM
BERLIN, GERMANY – 4 MAY 2015

Introduction



Good afternoon and thank you for the kind welcome.

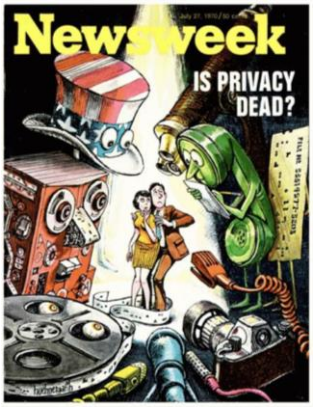
It gives me great pleasure to be invited to speak here today at the 5th European Data Protection Days Euro Forum.

I am pretty confident when I say that my office is the furthest Data Protection Authority from this meeting (albeit only in a geographical sense). You cannot get much further from Berlin, than our islands in the middle of the South Pacific – the last stop before Antarctica. I would like to think that that distance gives us a unique perspective on the issues we are here to discuss today. I am here wearing two hats. I am a Privacy Commissioner with much in common with the European Data Protection Authorities. I am also Chair of the Executive Committee of the International Conference of Data Protection and Privacy Commissioners.

I bring both perspectives to you in these brief comments, which will canvass first some general observations on "the state of privacy", the need and some of the mechanisms for international cooperation, and then what I was specifically asked to cover, the current situation in New Zealand, and the forecast reforms to our law. I am sure you will hear much that is familiar.

In the more than 20 years since I've been working in this area, I've seen countless announcements of the death of privacy. This cover of News week magazine is actually from 1970.

Is privacy dead? My answer, which I suspect I share with most of you is that despite advances in technology, despite Big data, biometrics, drones with cameras, the Internet of Things, Moore's Law despite, perhaps even because of all these things, privacy today is more important than ever.



There is a public demand for respect for personal data, for privacy and autonomy, and we have seen and continue to see that demand being met both in the marketplace and in regulation.

We here, with a vested interest in privacy and data protection are not the only ones noticing and talking about a heightened, rather than diminished sensitivity to these issues worldwide. One example - the international technology and market research company Forresters is predicting 2015 as the year privacy and security become competitive differentiators.

One of the largest law firms in New Zealand recently told its clients – "Last year it was all about health and safety". This year, it said ominously, privacy should be on every boardroom agenda.

In the United States, the business sector spent 2.4 billion dollars on privacy advice in 2014 and that is expected to rise to over 3 billion dollars this year.

Last month, the American company AT&T agreed to pay US25 million dollars in a civil penalty to the US Federal Communications Commission. Part of that settlement was to also create a new data security program.

The AT&T settlement is the largest concerning a data breach and customer privacy in the FCC's history. It comes after an investigation that found employees at three overseas call centres - in Colombia, Mexico and Philippines - sold thousands of AT&T customer records to criminal networks.

New Zealand in March saw the highest award of damages made to any individual claimant, $168 000.00 – four times the previous record, and close to the maximum of the jurisdiction of the competent judicial authority, of $200 000.00.

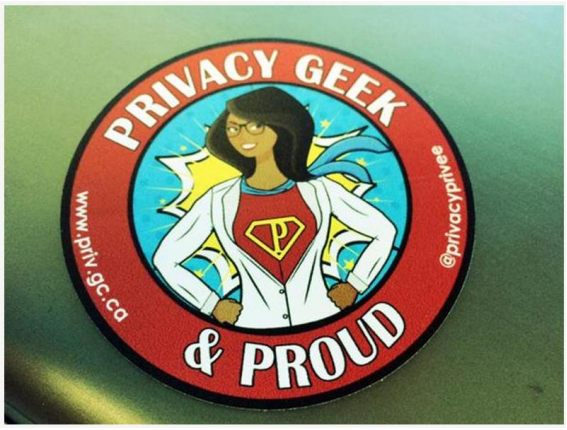
We've also seen a steady stream of stories about government and corporate surveillance.

Not least of these has been the drip feed of new revelations from the leaked National Security Agency documents by the American whistle-blower, Edward Snowden, and his media partners.

As news of data breach after breach confirms, the consequences of getting privacy wrong are expensive and potentially crippling.

All of this means there are both big challenges and opportunities for privacy and data protection authorities around the world.

International cooperation



In the early 1990s, when I started working in the privacy field, I could probably name most of the people in the world whose work included a significant privacy focus. Nowadays, privacy and data protection is an area of law and public policy that engages tens of thousands worldwide.

Privacy and data protection today is truly global with multinational service providers – think of Vodafone, IBM, Google, Microsoft, Facebook, Apple and others – present in almost every jurisdiction.

The slide, by the way, features a comic hero character created by Canada's Office of the Privacy Commissioner. I think the time has come for privacy professionals to transform from geeks to heroes.

EU adequacy status

As an Asian-Pacific jurisdiction, our links with our Asian-Pacific colleagues are crucial. However as a small nation, we are evermore aware of the importance of wider international linkages and of building globally consistent standards.

In 2012, New Zealand secured "adequacy" status from the European Union, meaning personal data can be sent to New Zealand from Europe for processing without special measures being taken by the European companies.

It took 20 years of lobbying and law change for New Zealand to achieve the EU adequacy status. It has been difficult to achieve for New Zealand but having done so, businesses can operate in Europe seamlessly and without the need to take extra steps to demonstrate compliance with EU standards.

After Edward Snowden's revelations about the alleged actions of the NSA and its "Five Eyes" partners blew up last year, a committee of the European Parliament then expressed disquiet about New Zealand's involvement in this cooperative intelligence network.

It was suggested that our EU adequacy status should be reviewed in light of claims of mass surveillance involving Britain, the United States, Canada, Australia and New Zealand.

Maintaining strong links with European privacy regulators and the European Commission is essential for maintaining New Zealand's data protection reputation and preserving our hard won EU approved status. I have met with some of those key influencers on this trip, and made the case that there is nothing in the Snowden papers which ought to call into quesiton the 2012 judgement that New Zealand should be regarded as adequate. I have given some background and reassurances, and have received a sympathetic reception.

International Conference of Data Protection and Privacy Commissioners

At the International Conference of Data Protection and Privacy Commissioners in Mauritius last year, New Zealand was elected Chair of the executive committee of the ICDPPC.

The responsibility of chairmanship brings with it the responsibility of providing a secretariat for the Committee.

Part of the secretariat's role involves accrediting privacy agencies wishing to join the conference and implementing resolutions such as the 2014 resolution on international cooperation.

The international conference secretariat provides a direct link between the nearly 100 economies with data protection authorities or privacy commissioners.

The role of Chair is an opportunity to have a voice in the ongoing discussion about the role of privacy regulation at this critical time of technological development, mounting international concern about security breaches, and heightened sensitivity about the activities of transnational corporates and intelligence agencies.

There are quite marked cultural and legal differences in approach to privacy between Europe and North America. This fundamental tension has dominated the global privacy discourse and has distracted attention from other models of privacy regulation around the world.

Reconciling approaches

When I was in the United States earlier this year, there was a great deal of talk about how the distinctly different approaches to privacy and data protection between the European Union and the United States might be reconciled.

I am hopeful that the International Conference can play a part in reconciling the seemingly intractable privacy differences that exist between Europe and the US. I've seen trenches and olive branches but as yet only a little evidence of the bridges proposed by those working on an ambitious project to find common ground. The project will be road tested at the International Conference in Amsterdam when my colleague Jacob Kohnstamm of the Dutch DPA reveals the fruits of his work in this area.

By deepening our involvement with the international community, and groupings of data protection authorities and privacy commissioners, we will be better placed to face the of global privacy challenges to New Zealanders.

It is important for New Zealand to engage closely with the privacy scene in Asia. This is the world's fastest growing cluster of top 20 economies – think China, Japan, South Korea, India and a rising Indonesia - as well as being the world's most populous region.

Asia is highly significant to New Zealand because of our proximity and deepening trade, immigration and diplomatic links. It is vital that New Zealand understands how Asian data protection and privacy environments work because so many of our markets are in Asian countries and that's projected to keep growing. I would suggest that it is also vital for Europe and the US not to overlook our region when considering bridges, and means of enforcement cooperation.

International relationships

New Zealand belongs to a number of international privacy networks and global privacy enforcement initiatives, including:

- OECD - and OECD personal data guidelines
- APEC - and the APEC Privacy Framework
- APEC Cooperation Arrangement for Cross Border Privacy Enforcement (CPEA)
- European Commission adequacy decision – NZ meets legal EU data protection standards
- Global Privacy Enforcement Network (GPEN)
- Asia Pacific Privacy Authorities (APPA) network

Updating the APEC Privacy Framework

My Office has currently been assisting with updating APEC's privacy framework. It is a timely move because this year marks the 10th anniversary of the framework's adoption in 2005.

At a meeting in the Philippines earlier this year, APEC's Electronic Commerce Steering Group endorsed a Data Privacy Subgroup plan to update the framework in a number of priority areas.

The APEC privacy 'stocktake' project uses the latest OECD Guidelines on the Protection of Privacy and Trans-border flows of Personal Data.

One major path to advance the APEC stocktake was for a comparative review of the 2013 changes to the OECD guidelines and their likely impact on the APEC framework.

My Office – as part of an Australia, Canada and New Zealand stocktake group - undertook this review according to a number of priority areas.

The stocktake group has since received a mandate to continue with its work and has now been enlarged to consist of Australia, Canada, Japan, New Zealand, the United States and two guests of APEC's Electronic Commerce Steering Group - the International Chamber of Commerce and the Internet Society.

It plans to report back to APEC's Data Privacy Subgroup in August.

This high level policy work is vital to the global economy and for many nations that are now developing or updating their privacy and data protection frameworks.

Small countries like ours have the most to gain from working in multilateral international organisations because we can join our voices with others and we can cooperate across borders in an increasingly trans-national world.

New Zealand – privacy and data protection background

I've been asked to outline the privacy and data protection environment in New Zealand.[1]

New Zealand was one of the first countries in the world to enact a privacy law.[2] A 1976 law established a privacy commissioner with jurisdiction over law enforcement data.

[1] New Zealand is a signatory of the Universal Declaration of Human Rights and has ratified the International Covenant on Civil and Political Rights, both of which contain a right to privacy. In recent years, a general tort of privacy has been recognised by New Zealand courts (*Hosking v Runting*).

[2] New Zealand was also the first economy in the Asia Pacific to meet European Union data protection standards.

That law was replaced in 1993 by the much broader Privacy Act which gives the commissioner jurisdiction over all agencies in the public and private sectors. We believe this was the first comprehensive national data protection law to be enacted outside Europe.

The Privacy Act 1993 controls how 'agencies' collect, use, disclose, store and give access to 'personal information'. It applies to both the public and private sector. Unlike the European model, we do not refer to ‘data controllers’ or ‘data processors’.

The term ‘agency’ as defined in the Act is so broad, it is simpler to list bodies that are excluded.

Organisations that are *not* covered by the Privacy Act include:

- Members of Parliament, when they are acting as MPs. It's up to Parliament or political parties to discipline MPs for breaches of privacy
- courts and tribunals, in relation to their judicial functions
- news media in their news gathering activities. (The news media are regulated by the Press Council, the Broadcasting Standards Authority, the Online Media Standards Authority, and the courts.)

In addition:

- if another law is inconsistent with the Privacy Act, that law will override the Privacy Act (to the extent of the inconsistency).
- Further, individuals who collect or use personal information for the purpose of their own personal, family or household affairs are exempt.

As in Europe, the right to privacy in New Zealand is not absolute. The Privacy Act balances privacy needs with other important social needs, such as public safety or prevention or detection of crime.

Take a recent European example as a case in point - the terrible Germanwings plane disaster. It is not my place to speculate on the cause of the crash, or the state of German privacy laws but news stories at the time implied that “strict German privacy laws” were a factor in preventing information about the fitness of the pilot getting to the appropriate authorities, who might have otherwise intervened and prevented him from flying..

We have a saying in New Zealand - BOTPA or ‘Because of the Privacy Act’. It is an acronym or shorthand for privacy laws being an obstacle to doing the right thing. I wrote a blog post on the subject and was surprised to find that Google translate took the term and gave me a German equivalent! (https://privacy.org.nz/blog/aviation-safety/ Aufgrund des Datenschutzgesetzes). Clearly this pheonmenon is not limited to our part of the world.

Other legislation will, at times, take priority over the Privacy Act but, even if they did not, the Privacy Act also allows the use and disclosure of personal information without the consent of the individual where necessary to avoid a serious threat.

As Privacy Commissioner, I:

- am a public regulator, watchdog and commentator
- investigate complaints about privacy breaches
- examine proposed legislation

- issue codes of practice for industries or sectors e.g. credit reporting, telecommunications, health information.
- In fulfilling these roles, I must act independently, and without prejudice.

Rather than setting strict rules, the Privacy Act is based on the same privacy principles derived from the 1980 OECD committee that form the basis of most data protection schemes in Europe and beyond.

This approach has allowed the Act to remain relevant as technology changes. But as the law enters its 24th year, the New Zealand Government has made a commitment to updating and reforming the law. We expect that to happen later this year.

Law reform

Law reform has been a long process beginning with a thorough review of New Zealand's privacy law by the Law Commission. It was completed in 2011.

The Law Commission found that, overall, the information privacy principles covering collection, storage, access, correction and disclosure of information remain sound.

However it recommended strengthening the Act in a number of other key areas to keep up with the times, and to meet the demand for tougher regulation..

The main recommendations include:

- Giving the Privacy Commissioner the power to issue compliance notices, and, where there is a good reason for it, to require an audit of an agency's information-handling practices;
- Streamlining the complaints process under the Act, including giving Privacy Commissioner the power to make binding decisions on complaints about people's right to access their own personal information;
- Mandatory breach notification if the breach is sufficiently serious;
- A new framework to allow the sharing of personal information between government agencies where it is in the public interest to do so, but with appropriate safeguards – a mechanism adopted by the government in 2014 and known as Approved Information Sharing Agreements or AISAs.

Similar laws have been proposed in the US and in Australia, and several of the features are also part of the European reform package.

Privacy vision: future focus

My vision is to make privacy compliance 'easy'. This is a key message of my office when communicating to business, government and the public. To do that we are developing a number of initiatives including:

- An online training course developed by educators and privacy specialists that will be available free to anyone.
- Guidance on Privacy Impact Assessment, and the new Information Sharing Agreements
- An online privacy policy generator
- A transparancy reporting policy
- A technology strategy – Making the Future – and a data safety toolkit for any agency that has a data breach.

These resources are all available on our website and we're using contemporary digital tools like Twitter, Facebook, YouTube, LinkedIn and a blog to communicate our resources to government and other sectors.