

PROTECTING PERSONAL DATA AND THE ROLE OF A REGULATOR

PRESENTATION BY NEW ZEALAND'S PRIVACY COMMISSIONER JOHN EDWARDS

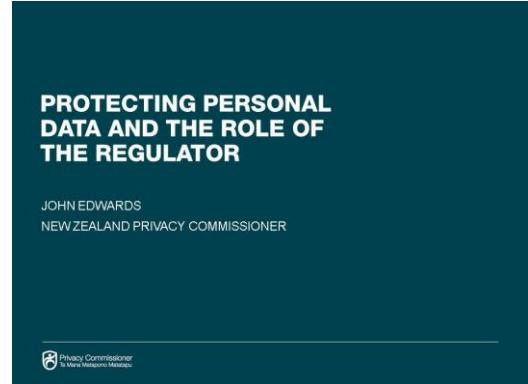
SINGAPORE PERSONAL DATA PROTECTION COMMISSION (PDPC)

3RD PERSONAL DATA PROTECTION SEMINAR

SINGAPORE – 8 MAY 2015

It is my pleasure and honour to address this 3rd Personal Data Protection Seminar.

Ever since I was a child, when my family hosted many visitors from Singapore I have heard about this miraculous island and its extraordinary success, and diverse but cohesive cultural and ethnic mix. The dominant message I remember was about this “small island”, this “tiny country”. This created some kind of Lilliputian impression in my childhood imagination, so you might be surprised to find that my immediate reaction on this, my first visit has been “Its so big!”



I'd like to begin by offering my condolences to the Singaporeans here today for the recent passing of your nation's founding father, Mr Lee Kuan Yew. It is not often that the world sees the like of such a remarkable statesman and I'm sure he is greatly missed.

I'd also like to acknowledge and thank Mr Leong Keng Thai and his team at the Personal Data Protection Commission for their generosity and hospitality in inviting me and hosting my visit.

On my way to Singapore, I puzzled over the exam question that was posed to high school students here recently. You might have seen the question yourselves - after it went viral on the worldwide web: How to solve Albert, Bernard and Cheryl's birthday maths problem.

The question has achieved a degree of global renown and many might say it has enhanced the reputation of Singapore's education system. If this is the kind of question Singaporean educationalists give fourteen year olds, I hate to think what happens at university. If you haven't seen it, I suggest you Google it.

Without going into the details of the problem itself, the upshot is that this head scratching question concerns personal data. Cheryl gives Albert and Bernard different sets of information about the date of her birthday. Only by comparing the two sets of data can the answer be reached – information sharing and matching. Each set of information by itself is useless. But put together, the secret can be unravelled – encryption and decryption.

Information matching, information sharing, and encryption – this is the stuff of data, how we use it, how we share it, how we protect it and how we make sense of it.

It reminds me of the late distinguished economist and Nobel Prize Laureate, Ronald Coase who said “torture the data and it will confess to anything”. This is especially pertinent against a universal backdrop of the inevitable wider use of and re-use of data in business and government.

For the private sector, collecting and using personal information can give you a competitive edge in finding new customers and targeting services better to existing ones. I see many representatives of the commercial sector here – some of you are bankers, insurers, software developers, telecommunications providers, credit reporters, media agencies, legal adviser, auditors and business consultants. All of your sectors work on trust. But we've seen what happens when large numbers of people lose trust and confidence in, for example, the banking system. Trust and confidence are foundations of a well functioning economy. Respect for customer data is essential for the maintaining that trust and confidence.

Data protection on boardroom agendas

This poster was one of nine made for all the Asia Pacific Privacy Authorities – of which Singapore and New Zealand are members – to help mark Privacy Awareness Week this year. This is Privacy Awareness Week and it is an appropriate message for today's event.

Organisations are investing a great deal of resources in getting their personal information and data protection practices up to date and future facing. They are doing this because the consequences of getting it wrong can be even higher than the cost of that investment.



The international technology and market research company Forresters is predicting 2015 as the year privacy and security become competitive differentiators. And one leading New Zealand law firm recently advised its clients that while it was all about health and safety last year, this year data protection and privacy should be on every boardroom agenda.

Many of you will have heard about a retail chain called Target in the United States which nearly two years ago suffered a crippling data breach leading to the loss of customers' credit card data. That case now serves as a cautionary lesson on how bad things can get when they go wrong.

The Target data breach by the numbers:

40 million - The number of credit and debit cards stolen from Target.

70 million – The number of records stolen that included the name, address, email address and phone number of Target shoppers.

100 million - The number of US dollars Target said it would spend upgrading its payment terminals to support Chip and PIN enabled cards - which if it had been done in the first place might have prevented the theft.

200 million – Estimated dollar cost to credit unions and community banks for reissuing 21.8 million cards - about half of the total stolen in the Target breach.

53.7 million - The income that the hackers likely generated from the sale of two million of the cards stolen from Target at an average of nearly 27 dollars each.

46 - The percentage drop in profits at Target in the fourth quarter of 2013, compared with the year before.

0 - The number of people in Chief Information Security Officer or Chief Security Officer roles at Target at the time of the thefts.

The Target story is a good lesson for regulators like me – and for organisations everywhere. Just ask Sony and Apple, two recent high profile victims of personal data theft. Another American company AT&T last month agreed to pay US25 million dollars in civil penalty to the US Federal Communications Commission as well as create a new data security program.

The settlement is the largest concerning a data breach and customer privacy in the FCC's history. It follows an investigation which found employees at three overseas call centres used by AT&T - in Colombia, Mexico and Philippines - sold thousands of customer records to criminals who attempted to use the information to unlock stolen mobile phones.

In New Zealand, a state owned insurer which provides no-fault personal injury cover for all New Zealand residents and visitors to New Zealand, suffered a similar reputation-destroying data breach a few years ago.

In the case of our Accident Compensation Corporation (or ACC as it is known), the personal information of over six thousand people was not stolen but disclosed through human error.

Now while ACC is a state-owned enterprise in New Zealand, it operates as any private sector insurer would and its lessons apply to any insurer, and the wider business sector. ACC handles 1 700 000 per year, or 1 new claim involving personal information every 18 seconds, so the number of movements of personal data at any given moment is enormous.

The event and ensuing mess sent a shudder through the country because at some point in every New Zealander's lives, some information is collected and stored by ACC – and this happened because an ACC manager inadvertently clicked and dragged an email from his computer desk top and attached it to an unrelated email to an ACC claimant.

What followed next reverberated for months because the matter became widely reported and caused others to come forward with other examples and this culminated in a widespread loss of confidence in the organisation. The organisation's chairman resigned followed soon after by its chief executive.

About ACC

- Monopoly provider of personal injury insurance
- 1.7 million claims per year (NZ population 4.4 million)
- 1 claim every 18 seconds

Source: ACC

My office commissioned an independent report into the ACC breach and it concluded there were systemic weaknesses at the organisation and that it had an "almost cavalier" attitude towards claimants and their personal information.

The organisation has since responded positively to the recommendations in that report and others, and embarked on a process of reconstructing and reconfiguring how it handles personal information.

Privacy and data protection is now a top priority for ACC.

As we know, new threats are emerging all the time, especially in the cybercrime and cyber security area. But as the ACC breach demonstrates, the biggest potential risk often lies within an organisation with systems that allow for human failings.

At one of our technology and privacy forums recently, a privacy manager from one of New Zealand's major

banks told the audience that in her organisation's experience, nine out of ten data breaches are caused by human error because of insufficiently trained staff or flawed processes.

In an age where with a few mouse clicks or a telephone call, consumers can switch power companies, banks and mobile or internet providers, a loss of confidence due to a data protection error can lead to a migration away from the company, and a subsequent loss of shareholder value. Being careless or complacent with personal data has financial and economic implications.

From the large corporate security breach involving thousands of individuals' data, I'd like to move to an equally damaging malicious and vindictive act of petty revenge, a recent New Zealand case in which a collection and disclosure of personal information about one individual by her former employer lead to a record breaking award by the competent tribunal.

The Plaintiff, Ms Hammond held a dinner party to celebrate her moving on from her employment at NZCU Baywide ("NZCU"). She posted to her private FaceBook account, a photograph of a cake baked for the occasion, that had been iced with an obscene message about NZCU. She shared the image with a small circle of friends.

When NZCU received knowledge of the photo's existence, its human resources manager coerced a junior employee to reveal the photo on her Facebook page so the manager could make a screenshot and disclose it to other senior managers.

The screenshot was then distributed to several employment agencies in the Hawke's Bay area by email. This was accompanied by phone calls from NZCU Baywide warning those agencies against employing Ms Hammond.



Ms Hammond complained to my office, and later exercised her right to take the matter to the Human Rights Review Tribunal. The Tribunal said the photo became the basis for a “sustained campaign by the company to inflict as much harm and humiliation as possible by ensuring Ms Hammond could not be employed in the Hawkes Bay area” and to get her dismissed by her subsequent employer.

The actions of NZCU Baywide made her new position untenable, forcing her to resign because the company threatened to withdraw its business from Ms Hammond’s new employer.

The Tribunal awarded Ms Hammond the largest amount ever in a privacy dispute, damages totalling \$168 000.00, close to the maximum of \$200 000.00 available to the Tribunal. That sum was made up of \$98,000 for humiliation, loss of dignity and injury to her feelings, \$38,350 for loss of income, \$15,543 for legal expenses and \$16,177 for the loss of a salary benefit Ms Hammond might have expected to obtain, but for the interference to her privacy.

The moral of the story is that privacy has become more expensive if you get it wrong. Is it any wonder that companies are finally sitting up and taking notice of their obligations to treat personal data appropriately?

Privacy and data protection in New Zealand

These are just a few of the horror stories and I’d now talk a little bit about our situation in New Zealand.

In the New Zealand context, privacy and data protection are wedded concepts under our Privacy Act. Privacy refers to the protection and management of personal information. The Act mostly governs personal information about individual people, though the Privacy Commissioner also has a wider ability to consider developments or actions that affect personal privacy.

The Act, which came into law in 1993, controls how 'agencies' collect, use, disclose, store and give access to 'personal information' and it applies to both the private and the public sectors.

Only a few organisations and people are not 'agencies' – the courts, Parliamentarians and news media. Other rules exist to govern how they manage personal information, so the Privacy Act does not cover what they do. If another law is inconsistent with the Privacy Act, that other law will override the Privacy Act.

Our Act balances privacy needs with other important social needs, such as public safety or prevention or detection of crime.

Privacy legislation in New Zealand

- One of the first countries to enact a comprehensive data protection law
- Privacy Act 1993 based on OECD Privacy Guidelines 1980
- It applies to public and private sector

The Privacy Commissioner is:

- independent
- an investigator of complaints about privacy breaches
- a public regulator, watchdog and commentator
- an examiner of proposed legislation
- and an issuer of codes of practice for industries or sectors e.g. credit reporting, telecommunications, health information.

Rather than setting strict rules, the New Zealand Privacy Act, like yours is based on a set of privacy, or data protection principles taken from 1980 OECD guidelines governing the protection of privacy and trans-border flows of personal data. This principles-oriented approach allows the Act to be flexible and relevant in an environment of constantly changing technology.

Here's a recent example: A media organisation at home developed an Android app. A customer, who was happy with the terms and conditions, downloaded it. When the next version was released for update, many of the privacy settings including what other apps and functions on the phone the app could access, had been changed, with defaults to access location and contact information. In other words, customers who had the app were alerted to the upgrade but not informed of the change to the terms and conditions and were not given the opportunity to opt out, if they didn't agree.

The customer complained to my office. We were very keen to investigate and set some expectations for this kind of development. But the customer had also complained to the company which to its credit took the opportunity to take its developers in hand, and restore the original settings to the app.

While it would have been more prudent to have been aware of and upfront about the changes prior to releasing the update, at least the company belatedly took the opportunity to respond to the privacy demands of the customer base and head off further trouble.

It is my duty to respond to increasing public concern about issues of privacy and data protection and I am doing this by getting tougher as a regulator. I am taking a stronger line on enforcement to make organisations more aware of their privacy obligations. Privacy and data protection regulators need to send a strong message to organisations about what the law means and to remind them of their obligations under the Act.

The need for modern data protection laws

In Singapore, your Personal Data Protection Act is a young one, having come into effect only last year. The New Zealand Privacy Act is now in its 24th year. In recognition of this, the Government has made a commitment to updating the law and a new Act is being drafted. We expect it to be introduced to Parliament later this year.

The Privacy Commissioner ...

- is independent
- Investigates complaints about privacy breaches
- a public regulator, watchdog and commentator
- examines proposed legislation
- can issue codes of practice for industries or sectors e.g. credit reporting, telecommunications, health information



The need to update the law is driven by the new reality that people and organisations today do more and more of their daily business online. The existing law was designed and enacted in the pre-internet era. Digital information can now be collected, copied and shared - maliciously or inadvertently – in an almost frictionless way, unlike hard copy files. The new law will reflect the greater level of risk to personal information and the bigger potential for loss in consumer confidence and trust. In other words, the stakes are higher now because the potential for harm is exponentially greater.

Privacy law reform has been a long process in New Zealand since our Law Commission completed a lengthy and thorough review of our Act in 2011. The Commission stated, overall, the principles of the Act remained sound. These are principles around collecting, storing, accessing, correcting and disclosing information, much like your own. The enduring quality of our 12 principles is that like yours, they are ‘technology neutral’ or conceptually adaptable to a changing world.

This is the strength of the law and it will remain so, although the Law Commission has recommended strengthening the Act in a number of key areas to make it more future facing.

These include:

- Giving the Privacy Commissioner the power to issue compliance notices to organisations, and, where there is a good reason for it, to require an audit of an organisation’s information-handling practices;
- Streamlining the complaints process under the Act, including giving me the power to make binding decisions on complaints about people’s right to access their own personal information;
- Mandatory breach notification if the breach was sufficiently serious. This is a very significant change in the New Zealand data protection environment – if you suffer a serious data breach, you have to tell my office

Similar laws have been proposed in the US and in Australia. When the New Zealand law change comes into effect, there will be a greater compulsion for organisations to comply with the law.

Compliance costs are a good business investment

If there is one thing a business audience is interested in, it is compliance costs.

I would of course argue that in many ways good data protection laws support good business practices, and adherence to them in most cases should have net benefits to business, rather than net costs.

One of the principles in our Privacy Act says an organisation should take reasonable steps to ensure information is complete, accurate, up to date, relevant and not misleading before using it. How can that be a drag on business? It is something every business should be expected to do anyway in meeting their customers’ requirements.



I also have some advice for the advisory sector - the lawyers and business consultants in the audience. Don't scare the daylights out of your clients about the risks and costs of privacy. Integrate data protection into the advice you give across the board. If you've got a client with a big IT build, for example, instead of solely focusing on the transactional stuff, and the intellectual property that we get fixated on, look at the opportunities for hardwiring good data protection practices that reduce downstream risk.

I can give you plenty of examples where by applying principles of privacy by design, and using tools like privacy impact assessment, you are future proofing your clients risk management (including reputational risk) in a really cost effective way, in the same way as you do when you advise them about the long term implications of owning the source code versus licensing versus open source solutions.

And once you or your client have done so, make a virtue out to it. Use it to differentiate yourself from your competitors. The public interest in the protection of its personal information indicates that there is a market demand for privacy conscious enterprises.

In a marketplace where there is little difference in price for the good or service, perhaps a simple, clearly explained privacy policy will be enough differentiation for a client to choose your ISP or mobile provider over another one. We see examples of this trend all around the world. Just look at Apple and Facebook. Although both have come under criticism at times for privacy issues, both now offer products and features directly responsive to marketplace calls for easily accessible privacy options and security, including encryption.

One of the key roles that my office plays is education. We have education for both organisations and consumers. If consumers demand a high level of data protection, and more privacy options, I am confident that business and government will respond to these demands. I believe this is a trend – as I mentioned at the beginning of my presentation – that is reflected around the world.

I have also done some work at home in building and supporting a market in professional advisers, so that information can be shared, and that best practice messages and skills can be widely disseminated. Building the capacity to comply with the law and to manage personal information well, involves a partnership between my office and the advisory sector. Just to show that "great minds think alike", I am pleased to announce that this week my office launched the first two of a series of online training modules to help agencies comply with their obligations under the Act. I have been very impressed to learn that your own online education tool, developed and hosted by the PDPC has had more than 7000 users already, and I aspire to such numbers!

I was similarly impressed by the innovative approach the PDPC has taken to getting small to medium enterprises access to legal advice. Striking a deal with the Singapore Law Society to ensure that an affordable "high level assessment" is available to all companies is a great idea and should both enhance compliance, and build the capacity of the advisory sector.

I haven't been able to secure discounted legal advice, but I have established a Directory of Privacy Professionals so people know where to go to get informed and practical compliance advice.
<https://www.privacy.org.nz/further-resources/directory-of-privacy-professionals/>

Getting the *right* advice is critical. If you or your client are experiencing high compliance costs for low or negative net value, there is a chance that you are doing it wrong. Maybe you are over engineering things. It should be rare that complying with data protection law should require artificial or pointless changes to business processes for no benefit. I tell companies to check with my office if it appears the advice they are getting is overly conservative.

Why international relationships matter

Getting back to the issue of reputational risk, I'd like to give you another very different example.

One growing area of our work is engaging internationally. Data flows and cyber threats happen across borders and jurisdictions. Scams and hacking attacks are trans-national because physical borders are irrelevant on the World Wide Web. Likewise for data

storage in the cloud which often happens in a single company's servers often physically located across many borders.

Aggregators of data and providers of information technology solutions and services such as Vodafone, Huawei, IBM, Google, Microsoft, Facebook, Apple and others provide their services in almost every corner of the world.

In 2012, New Zealand secured "adequacy" status from the European Union, meaning personal data can be sent here 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. Some of you may be aware with the extra hoops that need to be jumped through, if you don't have this 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.

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

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 challenges, mounting concern about data breaches, and raised sensitivity about the activities of transnational corporates and governments. When I was in the United States earlier this year, there was a great deal of talk at meetings about how the distinctly different approaches to privacy and data protection between the European Union and the United States might be reconciled.

There are quite marked cultural and legal differences in approach to privacy on different sides of the North Atlantic. This bipolar tension has dominated the global data protection discourse and has subtracted attention from other models of regulation around the world.

International networks

- OECD 1973 and OECD personal data guidelines 1980
- APEC 1989 and APEC Privacy Framework 2005
- APEC Cooperation Arrangement for Cross-Border Privacy Enforcement (CPEA)
- European Commission adequacy decision on NZ
- Asia Pacific Privacy Authorities (APPA)
- Global Privacy Enforcement Network (GPEN)
- International Conference of Data Protection and Privacy Commissioners (ICDPPC)

I am hopeful that New Zealand can play its part in reconciling the seemingly intractable differences that exist between the Europeans and the Americans. I've seen trenches and olive branches but little evidence yet of the bridges being proposed.

At a "dinner dialogue" at the Brookings Institution on "Privacy Security and the US-Europe Relationship", I found myself among an elite group of American and European privacy and data protection professionals and regulators. The participants were invited to introduce themselves in turn. I was the last to speak, pointing out that I appeared to be the only representative from a region of over four billion people while everyone else in the room was focused exclusively on matters of direct relevance only to the EU and the US.

It is important for New Zealand to pay particularly close attention to the data protection environments in Asia. The region is highly significant to us because of our proximity and deepening trade, immigration and diplomatic links. It is vital we understand how Asian data protection scenes work because so many of our markets are in Asian countries and our relationships with the region are projected to keep on growing.

Also, 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 challenges of global information risks to New Zealanders.

We live in a world of too much information. A direct consequence is figuring how to keep control of our personal information – the stuff that we don't want to share, the stuff we want to keep personal – and relaying those expectations to the organisations that collect our information. Information is about people and about their lives. If it falls into the wrong hands, the potential for harm is very real.

The death of privacy is greatly exaggerated

In the more than 20 years since I've been working in this area, I've seen countless announcements of the death of privacy. Is privacy dead? A resounding no! My answer is privacy matters because we still care about it.

Our lives are becoming ever more enumerated and dissected. The organisations that you represent have an obligation and a responsibility to manage and protect personal information. If people can't trust the organisations they do business with to look after information that is about them, there can be no business.



Big data, the Internet of Things, Moore's Law – all these developments increase rather than detract from a focus on privacy. The public demand for restraint will be met both in the marketplace and in regulation. Privacy is not dead. It is one of the most essential issues of our time.

In concluding, I wish all of you an enjoyable and productive Personal Data Protection Seminar. I'm excited by what promises to be a very interesting morning and I'm looking forward to taking part in many of the stimulating discussions that will certainly follow. Thank you for listening and the opportunity to speak.

How to find us



www.privacy.org.nz

