Making privacy work in the digital world

Privacy Commissioner John Edwards

Institute of IT Professionals - Wellington Branch

24 May 2016, Wellington

Good morning and thank you for the welcome.

I recently gave an introduction at one of our lunchtime Technology and Privacy Forums for Vikram Kumar who was speaking on the topic of the Internet of Things and how it will impact on consumer privacy.

Before the forum, I asked my office if anyone had any Internet of Things jokes.

I didn't get a big haul but I did get a few.

Question: How far is it from the toaster to the jug?

Answer: About a smart meter.

Question: What do you call smart jewellery?

Answer: The Internet of Blings.

And so it goes - the Internet of Things, drone deliveries, Artificial Intelligence, robotics, driverless cars, virtual reality, augmented reality, facial recognition technology.

These are all part of the next generation of technological upheaval that will inevitably present new challenges to consumers, governments, businesses and privacy regulators like me.

Panic in Privacy City

The view from my office is that new technology is a force for good because it is encourages and stimulates innovation.

Some of you will be familiar with Gartner's 'hype cycle'.

Gartner is an American IT research and advisory firm.

It's 'hype cycle' concept applies to new technologies.

The concept is the idea that each promising new technology goes through a similar set of phases before it is widely adopted.

It's a concept that can also be applied to privacy fears.

Step one: A new technology is developed.

Only experts really understand it at first. It features more in academic papers than it does the media.

People with their ear to the ground probably know about it.

Inventors, innovators, designers and engineers are getting their hands on it and are figuring out how to monetise it.

Word starts to get around about the capabilities, people get excited about it.

Step two: The “Privacy activists” find out about the new technology and come to dampen the mood of excitement.

They spread warnings about worst case scenarios which get picked up by the mainstream media.

In turn, public perceptions start to shift.

Once the technology becomes more widespread, once we start to see real world applications and realise it might not be so bad, we get to step three.

This is when the fear deflates.

Step three is punctuated by mini panics over time, but the general direction of anxiety is down.

Some recent examples include Samsung’s Smart TV, the Jeep Cherokee smart car and other devices like the Amazon Echo smart speaker.

What’s important to recognise is that the impact of each privacy ‘scare’ plays a part in ensuring that future developments are more privacy-friendly.

Privacy warnings form a vital part of risk assessment.

When business and government assess the risks of a project, even where a risk is high impact but unlikely, it still gets put in the risk register.

Panics are not simply unfulfilled prophecies, but form part of the overall process of developing privacy laws and norms.

Where good privacy analysis comes in is recognising the value in, or even predicting, that panic, and in designing solutions that prevent those fears being realised.

Privacy panics help shape approaches for the future.

They help businesses and innovators know where the danger zones are and how to avoid them.

One of those danger zones is the collection and sharing of personal information.

One of the enduring things about the Privacy Act is that it is technology neutral, so it can provide a framework for reassurance through the panic and fear of the hype cycle.

That’s some of what I want to talk to you about today, and how my office can help you take the right direction when there is a privacy panic about the customer data you work with.

Public opinion

Every two years, my office commissions UMR to undertake a public opinion survey.

We revealed the results of the latest survey during Privacy Week, earlier this month.

What we've found is a continuation of a long term trend.

Nearly half of all New Zealanders polled said they were becoming 'more concerned' about privacy issues.

That was the consistent with the result two years ago and considerably up on four years ago.

Meanwhile, about two-thirds or 65 percent of New Zealanders continue to be concerned about privacy.

This result is statistically unchanged from previous surveys in 2014 and 2012.

A large majority of those respondents - 75 to 81 percent - say they are concerned about issues related to identity theft, credit card and banking details, businesses sharing personal information and security of information.

However, the respondents expressed a decreased level of concern about the way government and health organisations are sharing information.

The full results of the survey are available on our website.

The main points that I want to emphasise are:

A significant majority of New Zealanders are concerned about privacy.

New Zealanders are concerned about data or information sharing by organisations - both public and private sector.

We trust government more than we trust businesses.

Our opposition to information or data sharing falls if there are more safeguards in place.

Putting a price on privacy

But here's the thing - our digital age has given rise to manifold ways of easily collecting huge amounts of customer information.

But just because you can collect massive quantities of data, does it mean you should?

The answer is no.

At the heart of the Privacy Act are the twin concepts of data minimisation and proportionality.

You should only collect what you need, not what you might or might not find a use for in the future.

There's a huge temptation to collect everything you can - the more data points you can string together, the more useful conclusions you are likely to draw.

But when you collect information from somebody in New Zealand, you need to be able to tell them why you're doing it.

"Keep it because one day we'll figure out a use for it" as a justification doesn't cut it.

If you cannot explain how a piece of information is related to the service or product you're providing then you shouldn't collect it.

That's why it's important to be clear on what you want to do before you decide what you need to know.

The Privacy Act sets out the obligation to inform people about the information you are collecting, but you need to make sure you're working towards informing users, not just as an exercise in legal compliance.

When people try and comply with the Privacy Act, there's a tendency to go heavy on the legalese.

We don't think the people should have to have a law degree to read the terms of service.

There is a responsibility to speak to people in language that they understand.

To ensure that when they do consent, it's informed.

Privacy is part of the landscape, and your customers and clients are getting more and more privacy literate.

If you treat them with respect, they'll be more likely to trust you.

Take for example, the world's cheapest smartphone which is being sold in India for four US dollars.

We all know that if something is too good to be true, be suspicious.

With deals like a four dollar smartphone, consumers need to know the hidden price they will have to pay when they use one of these phones.

What's the value of the personal information they are trading away and the cost to their privacy?

The organisation that has collected the information will have a price for it but how does that price compare to the value to the individual?

In 2014, a Dutch student Shawn Buckles decided to illustrate the market for data by selling his personal information at an auction.

After a few weeks and 53 bids, his information sold for 350 euros - or about 570 New Zealand dollars.

Shawn Buckles' data bundle included all sorts of private information - every thing from online browsing data to email conversations.

He told a media organisation that he had read that a person's data could be bought for under a dollar.

That's because organisations bought data in bundles and that made it cheap to do so.

He said he had added lots of value to his data, but it included his most intimate information - and there was no fair price for that.

Buckles hoped his auction would help people understand that the issue was about people.

His stunt was designed to illustrate what data was being collected and how private this data was.

“Our digital data says more about us than our living rooms. A question to you: do you have curtains?" he asked.

Trading health information

Take this recent example out of the United States where employers can employ ‘wellness firms’ to monitor their employees’ health.

Imagine the wellness firm and insurers working together with the employer to mine the health data of the employees.

Should, for example, the employer know what prescription medicines you are taking?

While employers don’t get access to which individuals are flagged by this data mining, they do receive aggregated data on the number of workers at risk for particular health risks or conditions.

This presents a real risk of re-identifying individuals from the anonymised data - but more on that later.

In the meantime, while wellness firms, insurers, and employers all extract benefit from the data, what’s in it for the employees whose information is being mined?

Who benefits the most?

Trouble with Uber

Uber is a topical example of an enterprise that to an extent justifies its place in the panic and fear point on the hype cycle, and had to raise its game.

It’s a new business model that challenges the traditional taxi industry.

Since it was founded in 2009, Uber has grown spectacularly but as a brand it has been clouded by a number of privacy controversies.

Through its app on a customer’s phone, Uber is able to track a customer’s movements - a feature that was known within the company as ‘God’s view’.

God’s view shows an aerial view of all customers and drivers in a particular area.

One Uber executive bragged the company - if it wanted to - could use its tracking ability, to dig up dirt on the personal lives of journalists who were critical of the company’s business practices.

In one incident, the company showed a journalist how it tracked her on her way to interview another top Uber executive.

There was also the notorious incident in which a well known businessman was told by an acquaintance that his movements in an Uber taxi in New York were being shown in real time on a big screen at an Uber launch party in Chicago.

The name of the businessman who suffered the privacy breach at the Uber party in Chicago is Peter Sims.

In a widely read blog post, he asked ‘Can we trust Uber?’ observing that “a great, long-lived brand begins and ends with trust”.

Uber has since been addressing its privacy failings to placate US regulators.

These include password-protection and encryption for the location data of passengers and drivers, limiting employee access to the data, and adding more security tools to protect personal information.

Uber has also agreed to notify the authorities if it started to collect GPS data from customers' smartphones when they were not using the app - something the company claimed it didn't do.

Trust and confidence

Collecting and using personal information gives any organisation an advantage.

In the private sector, it gives companies a competitive edge.

In government, it helps in the allocation of scarce resources.

But we've also seen what happens when large numbers of people lose trust and confidence in, for example, the banking system.

In a very recent example, I was asked to comment on one of the unfortunate outcomes of the collapse of the Dick Smith Electronics retail chain.

The liquidators were planning to put the Dick Smith customer data base up for sale and our office received a number of enquiries from concerned customers.

They were worried about the possibility that information about them would pass from a retail chain that they had entrusted their information to an unknown third party they did not know or trust.

Respect for personal information is necessary for the maintenance of your customers' trust and confidence.

Encryption

Encouragingly, it appears that many online service providers appear to be listening to the public.

Recent much publicised revelations and fears about online surveillance has created a market for encryption services.

For example, if you are a WhatsApp user, when you and your contacts use the latest version of the app, every call you make, and every message, photo, video, file, and voice message you send, is end-to-end encrypted by default.

Major tech companies like Apple, Google, Microsoft, Yahoo, Twitter, Facebook and Dropbox have all implemented encryption of customer data and are resisting the US government's calls for 'backdoors' into their products or services.

Encryption has become an industry standard because consumers want it and because companies that don't do it are providing an inferior service to their competitors.

Encryption is also a way of protecting customer data.

Should an agency be the subject of a data breach in which customer data is stolen or lost, the damage would be considerable less if the data was securely encrypted.

Would the Ashley Madison data breach have had anywhere near the fallout that occurred if the data had been encrypted and unusable to a criminal third party?

You have an important role in creating the security settings and culture needs to protect your organisation's reputation and financial viability.

Government and big data

In 2013, the government introduced its Integrated Data Infrastructure, a project led by Statistics New Zealand.

The project combines information from a range of government organisations to provide the insights into how the government can improve social and economic outcomes for New Zealanders.

With all personal information removed, integrated data gives a safe view across government.

The project is particularly useful to policy makers and social researchers working on addressing complex social issues such as crime and vulnerable children.

For example, earlier this year, the government released a data visualisation tool based on the Integrated Data Infrastructure.

By using it, you can see how many vulnerable children there are in your region or in your neighbourhood.

I'm on record as describing the Integrated Data Infrastructure as a 'grand bargain' in terms of how privacy and confidentiality are not compromised.

The IDI promises that personal information is never seen by researchers.

This is done by anonymising the information and removing identifying information like names, addresses, and dates of birth.

The research findings are then grouped in a way which makes it impossible to identify individual people.

Re-identification

One of biggest concerns about big data is techniques that can re-identify individuals when previously anonymised data are combined with other data sets.

The Privacy Act says organisations should collect personal information for a stated lawful purpose.

Organisations can't use personal information collected for one purpose for another purpose.

The way around this is by anonymising or de-identifying the information so that it is stripped of information about identifiable individuals.

In theory, anonymised or de-identified data is no longer personal information and therefore not subject to the Privacy Act.

But does de-identifying data as a fail safe to protecting personal information work?

It depends on what you mean because it has been observed that as data sets become more sophisticated, the technical possibility of undertaking 'jigsaw' re-identification of individuals increases.

Jigsaw re-identification is the ability to identify people using two or more different pieces of information from two or more sources of information.

The Care Data initiative in Britain was derailed recently because of concerns about the robustness of the de-identification.

Another study showed that in an anonymised dataset of location data over a year of 1.5 million telecommunications company subscribers, researchers could identify individual records with 85 percent accuracy, if they knew where they had been just four times in than year.

These cases reveal that our intuitive beliefs about anonymity and identity are often misplaced.

The distinction between personal and non-personal information is becoming increasingly blurred.

Rapid advancements in technical capability exacerbate that blurriness even more and raise ethical issues in relation to informed consent, trust and what security of information means and how best to secure it.

These ethical issues are currently being hotly debated among lead commentators in the area of re-identification.

There is an emerging argument that governments should consider a prohibition on re-identifying anonymised personal information.

Regulating open data

The New Zealand's government's efforts to provide open data have excluded personal information so far, although as we've just discussed - what constitutes personal information is not necessarily well understood.

While our office plays a role in setting the limits on what can be done with personal information, my role does not include a mandate to promote the wider use of data.

That role is not, as yet, part of any organisation's mandate.

There is also an important distinction between privacy and ethics in data use and there is no body charged with providing advice on what constitutes ethical practice - apart from the National Ethics Advisory Council's role in the health sector.

We are fortunate in New Zealand that we already have a robust legal framework for managing data with the Statistics Act and the Privacy Act as the pillars of that framework.

The work of the Data Futures Partnership builds on these existing foundations of data management and seeks to unlock the opportunities of large scale data collection while protecting the privacy rights of the individual.

The Partnership's vision identifies four key elements to be maintained as part of the framework, and these are value, inclusion, trust and control.

It is encouraging to see that the Data Futures Partnership recognises that privacy is an integral part of the national conversation about our use of data.

The Privacy Act deals particularly well with the desire to realise value from data from recombination and reuse.

But there are areas where the Act can be strengthened.

Strengthening the Privacy Act

For example, under the Act, there is currently no explicit prohibition on the re-identification of data from which identifying information has been removed.

It's food for thought that a prohibition of this nature could potentially increase public confidence in the safe use of "de-identified" or "anonymised" data.

Similarly, further work could be undertaken on strengthening individual rights to have information about them deleted.

This would raise people's confidence that information provided is not necessarily available forever and able to be combined with yet to be created datasets.

Privacy tools

IT professionals, coders, engineers, system architects and business analysts have an important role to play in identifying and exposing privacy issues for project sponsors.

Inform yourselves with our Privacy 101 online privacy learning module.

The module is a good basis to orientate yourselves with the privacy considerations that should be at the foundation of any information management system.

Our Office helps businesses build their understanding of privacy with online tools like our online learning modules and our Privacy Impact Assessment guidance.

Privacy Impact Assessments focus on identifying the ways a new proposal or operating system, or changes to an existing process may affect personal privacy.

They help organisations make more informed decisions and better manage privacy risks.

It is important to decide whether to do a Privacy Impact Assessment early in a proposal's life.

When businesses introduce an awareness of privacy to projects early on, many of the major risks can be mitigated.

This is what is meant by Privacy by Design - building privacy protections in on the ground floor.

If you fail to identify how your project is likely to affect the individuals whose information you are collecting and using, there are real risks for your organisation and for the success of your project.

You can find our Privacy 101 module and our Privacy Impact Assessment guidance on our website.

We have also developed a tool to help agencies create customised privacy statement.

The Priv-o-matic is our online gadget that can help you generate the words you can use to explain to people what you do with their information.

It takes about five minutes to complete.

These 'principle 3' statements are minimal compliance statements that you need to show your clients when you collect their personal information.

We also want to help organisations and agencies in how they respond to access requests - it's a good discipline for any organisation.

This month, my office marked New Zealand's first Right to Know Day.

Right to Know Day is a day dedicated to raising awareness of the legal right New Zealanders have to see their own information that agencies hold.

For example, if a business or organisation collects personal information, then a customer has the right to see the information that is about them.

We created an online tool called AboutMe to make it easier for individuals to ask agencies for their personal information by helping to draft a template email.

AboutMe will also help agencies by standardising requests for personal information and ensuring that they include all the relevant detail.

This will be particularly useful for small to medium sized agencies that do not receive many information requests.

AboutMe went live during Privacy Week earlier this month and I encourage you to have a look at it on our website.

Roughly 60 percent of the complaints my office receives each year have to do with access to personal information.

We want to reduce the number of access complaints by making organisations aware of this important feature of the Privacy Act.

People have a right to assert their access to information that is about them that is held by an organisation or agency.

You guys have a really important role to play in designing information systems to help organisations comply with access requests and improve the efficiency with which these requests are dealt with.

Getting the design right up front can help save millions of dollars.

For example, Immigration NZ gets 28,000 requests for personal information each year.

Another example, the Ministry of Social Development has a backlog of 2100 access requests that have extended beyond the statutory 20 working days to respond. So that agency is currently in breach of the law.

These organisations are experiencing increasing delays in responding to these requests and those delays are finding their way to my office as complaints.

Conclusion

These tools fit with one of the key goals we set for ourselves - that is to make privacy easy for organisations.

When we talked to people about our technology strategy, they asked for simple tools and this is something we will keep building on.

Privacy matters because the public still cares about it.

Privacy matters because the reputations of your organisations depend on it.

The organisations that you represent have an obligation and a responsibility to manage and protect personal information.

Our lives are becoming ever more enumerated and dissected.

If people can't trust the organisations they engage with to look after information that is about them, they will - in the private sector - look for competitors they can trust or - in the public sector - be more reluctant to share truthful and accurate information.

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.

The important thing is to learn the right lessons from the privacy panics whether they are justified or not.

ENDS