Presentation by John Edwards, Privacy Commissioner to University of the Third Age

on

Future of Privacy: The Internet of Things and Other Challenges

9 August 2016

Introduction

Good morning. Thank you for the welcome and the invitation to speak to you today.

Today I'd like to talk about how our world has changed in the past 20 years, particularly in communications technology.

I'd also like to cover the kinds of things that I as a privacy regulator can do to help people understand privacy implications and how they can mitigate the risks of our digital world.

Firstly, let's begin with a topical joke: Why did the SIS agent play Pokemon Go?

It's because he wanted to have a Pikachu.

I'm not expecting that many of you – if any – will have downloaded this new smartphone game and joined the throngs of mainly young people who are out there chasing after digital cartoon characters in physical spaces.

I don't really see you as being part of the Pokemon Go demographic.

But many of you will be aware through our news media and, maybe, familial connections that this game has become a global phenomenon.

Augmented reality

What's different about Pokemon Go from other smartphone games is that it is uses smart devices to overlay digital features on top of our physical brick-and-mortar world.

In other words, you can see digital features as they appear on your screen if you are at a particular location – and in the case of Pokemon Go, digitally capture them.

This technology - augmented reality - is also being incorporated in other industries, apart from gaming and entertainment.

For example, the global furniture maker IKEA has introduced a catalogue app that allows customers to place furniture pieces in an augmented reality environment before buying them.

The German car maker Mercedes-Benz and the aviation manufacturer Airbus have developed augmented reality systems capable of identifying glitches in advance during the parts assembly process.

And there was a recent Guardian opinion article that said Pokemon Go had done Britain's National Health Service a huge service - it had succeeded where many healthy living advocacy groups had failed, by getting people to exercise regularly by walking!

However, there has also been a - some might say inevitable, but I would argue essential - privacy scare.

Pokemon Go

It began when a blogger raised concerns about the permissions the Pokemon Go app asked for when it was downloaded onto a smartphone or tablet.

The blogger - an IT security architect - discovered that it appeared he had given the app full access to his Google account - including emails and documents.

He said the Pokémon Go app, and its parent company Niantic, in theory could now read all his emails, send emails as him and access all his Google Drive documents. It could also look at his search and Maps navigation history and access any photos he might store in Google Photos.

My office was asked if we would be investigating.

At that stage, I decided there was little or no cause to do so.

It appeared more likely a case that the app developers had failed to accurately describe what functionalities it would have access to.

The parent company Niantic soon after clarified that Pokémon Go only accessed basic Google profile information - specifically, user ID and email address.

A Niantic spokesperson confirmed that no other Google account information was or had been accessed or collected.

She said once the company was made aware of the error, it began working on a fix to request permission for only basic Google profile information – in line with the data that it actually accessed.

So it appears it was all an embarrassing mistake.

Privacy scares

It brings to mind last year's Samsung Smart TV privacy row in which the South Korean appliance manufacturer was accused of selling a smart TV that eavesdropped on consumers.

It was revealed that voice commands directed at the TV were transmitted across the internet to a company server where they were translated and relayed back to the TV to action.

This had been inadequately described in the product's terms and conditions and technology writers jumped on Samsung, accusing it of in-home spying.

Consumer blood pressure went up and Samsung had a public relations headache on its hands.

Hype cycle

Those of you familiar with the Gartner "hype cycle" will recognise both the Samsung Smart TV and Pokémon Go cases as two illustrative examples.

The hype cycle is a graphical presentation used by the American Information Technology research and advisory firm Gartner to represent the maturity, adoption and social application of specific technologies.

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

Step one: A new technology is developed.

Only experts really understand it. 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, and people get excited.

Step two: “Privacy activists” get wind of the new technology and come to ruin everyone’s fun.

They spread warnings about worst case scenarios which get picked up by the mainstream media. In turn, public perceptions start to shift.

Behavioural advertising and facial recognition are up near the top of the peak and wearable technology - like fitbits, drones and the broader internet of things - are in this ‘mounting unease’ phase of the hype cycle.

But 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. It is punctuated by ‘micro panics’ over time, but the general direction of anxiety is down.

Society as a whole gets on with adopting the new technology. It becomes more widespread and is seen as reaching maturity.

Privacy activist fears are largely forgotten by now because the sky didn’t actually fall.

Risk assessment

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 also form a vital part of any risk assessment of new technology or product. Panics form part of the overall process of developing privacy laws and norms.

Dire warnings play a role in finding an equilibrium that pulls an issue from peak privacy panic to something most people are comfortable with.

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.

The aftermath of one of these privacy panics can help shape approaches for the future.

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

Buyer beware

Now back to Pokemon Go - there's no doubt that apps on smart devices are getting more and more sophisticated.

As our devices aggregate more and more data about our lives through new functionalities, apps are being developed which exploit those functionalities.

It is a very real privacy concern.

The best means of protection is for consumers to exercise autonomy over how they enjoy and engage with these fun new games and other emerging digital technologies.

People get to grant permissions and if you don't take time to think about what you're granting, you really don't have much ground to complain afterwards.

Consumers have to make their own choices and - in the case of the Pokemon Go app - they can exert a level of control over it - if they have taken the time to learn about them.

This kind of awareness requires an informed public that knows where the privacy pitfalls are.

This is where I come in.

Privacy education

My office has a vital role in educating the public, as well as organisations, about privacy and how our Privacy Act works.

We try to lead by example.

For example, we have a website that collects very little visitor information and we let people know what information is collected.

We also use a web analytics tool called Piwik because it was the most privacy friendly one we could find.

We also have a number of online tools to help other organisations get their privacy responsibilities in order and also tools to help people understand their privacy rights.

We have online privacy education modules which are free to use. The two most popular are our Privacy 101 module and our Health Information Privacy Code. The first gives a general overview of the Privacy Act and the latter is an introduction to how health information should be managed.

If people have a particular privacy gripe with an organisation or agency, they can lodge a privacy complaint with us using our online complaint form.

We have a privacy statement generator – called Priv-o-matic - for small to medium sized businesses that inform people about what information is being collected and what happens to that information.

And we have just launched Ask Us - another online tool to help people – whether they are individuals seeking information about their rights or people working in organisations wanted to know their responsibilities with personal information.

Ask Us is a repository of privacy knowledge that can be accessed on our website. Anyone can enter a question in Ask Us search function and it will bring up a list of answers.

Over time we hope the search results will become more refined, accurate and even seemingly intuitive.

As examples, some of the more common questions asked of Ask Us to date include ‘can my employer record my conversations’, ‘how can I get my credit report’ and ‘can I ask for information about me from an organisation’.

Collecting information

The same technology that enables us to deliver these privacy-enhancing services is an extension of the technology that creates ongoing privacy challenges for all of us, including privacy regulators like me.

Digital technologies create new ways of easily collecting huge amounts of customer information.

But just because a business or organisation can collect massive quantities of customer data, does it mean it should?

The answer is no - absolutely not.

I’ve discussed the scares around Pokemon Go and the Samsung Smart TV and the fears around the collection of unnecessary consumer information – unnecessary because it isn’t needed for the purpose of the service the organisation is providing for you.

The Privacy Act actually prohibits over-collecting. You’re only allowed to 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 possible - the more data points an organisation can string together, the more useful conclusions it is likely to be able to draw about you.

But when an organisation collects information from somebody in New Zealand, it needs to be able to tell people why it is doing it.

“Keep it because one day we’ll figure out a use for it” as a justification doesn’t cut it.

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

The Privacy Act sets out the obligation to inform people about the information that is being collecting, but organisations need to make sure they're working towards informing users - it is not just as an exercise in legal compliance.

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

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

We believe organisations have a responsibility to speak to people in language that they understand. To ensure that when they do consent, it's informed.

If customers are treated with respect, they'll be more likely to trust the organisation.

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

Dick Smith Electronics

In a 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.

Under this kind of spotlight, the receivers set out to accommodate the concerns of former Dick Smith customers by contacting them via email.

Each customer was informed they could remove their information from the database as the sale went ahead, otherwise their information would remain in the customer database.

Losing control

This highlights one of the biggest privacy concerns - losing control over information that’s about us.

It is apparent that one of the trade-offs for having so much information at our fingertips is how much information we inadvertently reveal about ourselves.

Through our engagement with the digital world, we reveal our location, our daily travel, our spending, our tastes, our communications, our friend and family networks, and our fears.

How many of you have used search engines to diagnose a health issue only to be confronted later by advertising promising remedies for the problem?

Please don’t misunderstand me.

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

But we believe that in a world where the cheapest smartphone is being sold in India for four dollars, consumers need to know the hidden price they have to pay.

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

The organisations that collect personal information will have a price for it but how does that price compare to the value to the individual?

The value of information

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.

Mr 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.

Public opinion

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

In our latest survey, carried out earlier this year, 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 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.

Strengthening the Privacy Act

A few years ago, the Law Commission completed a comprehensive five year review on the privacy laws.

It made about 140 recommendations in its report.

The government has accepted the majority of the recommendations and draft legislation is being prepared.

When the changes go through, the new Privacy Act will give my Office more enforcement powers.

1. **Access determinations**

One significant change will give me the power to make “access determinations”.

This is a very important change to the law because over 60 percent of the complaints that come to me deal with requests for access by a person to their own personal information.

Providing people with access to their information is a part of any business. It is not some legal compliance exercise. It is their right.

2. **Enforcement notices**

A second major tool I expect to see is the power to issue enforcement notices when agencies refuse to comply.

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.

3. Mandatory breach notification

We are also expecting to see the introduction of mandatory breach notification.

This change will bring us in line with many overseas countries. New Zealand is 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.

Government agencies are understandably sensitive about data breaches, given the high profile breaches at ACC and MSD in the past few years.

By and large, they notify us of the big breaches.

But what's interesting is there has been a noticeable pick up in notifications from the business sector, particularly among large businesses.

In a new Privacy Act, 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.

More enforcement powers, rising public concern about privacy, and the prospect of a new Privacy Act, all point to an exciting time in the life of a privacy regulator.

Transparency reporting

Transparency reporting is a developing area in privacy that doesn't require a law change.

It is also an area where I can make a difference to raising public expectations about how its personal information is managed.

Yahoo, Google, Dropbox, Facebook, Microsoft, Trade Me and others do it and we think it would be a good thing if many New Zealand companies decided to do it too.

A transparency report is a statement issued on a regular basis by a company that reveals the number of requests made by government agencies for its user data, records, or content.

It is a way that companies can to be open with consumers about the limits of confidentiality, by revealing the extent to which they cooperate with government agencies.

Transparency reporting also helps policy makers and law makers make decisions about the right balance between surveillance powers and individual privacy.

My office carried out a transparency reporting trial last year and it gave us some insight into how law enforcement, intelligence and revenue gathering agencies used their coercive powers to obtain personal information.

The trial revealed that government agencies made nearly 12,000 requests to 10 New Zealand companies for personal information.

I want to acknowledge Trade Me as a New Zealand company that really taken a lead in making transparency reporting an integral part of its corporate reporting.

Trade Me's 2016 transparency report is the company's fourth.

It revealed it had received 1508 requests for customer information from Police and 15 requests from the SIS – and we know this because the company wants its customers and the public to know.

Internet New Zealand is also helping in this space.

Last week, it launched its Easy Transparency project – a set of templates and tools to help New Zealand organisations start doing yearly transparency reporting.

So what's the idea? Internet NZ says the game plan is focused on addressing the global issue of mass surveillance and making it harder for intelligence agencies, and others, to undertake mass surveillance.

To quote Internet NZ: "We think New Zealand is overdue for a little more sunlight on government access to private information. Some government agencies have been really great in getting on board with this project. After all, why would government agencies be scared of New Zealand organisations publishing stats on agency requests and warrants? I mean, if they've done nothing wrong, they've got nothing to hide."

In the future, there'll be even more personal information travelling from one place to another, but if we do things right, we'll have more control too.

What information are we giving out? Who are we giving it to? Do we trust them? What will they do with it? What are we signing up for?

It's important that we ask these questions.

This brings me to the Internet of Things.

Barbie

Imagine a future that's really not so far way where our smart phones, cars and household appliances have the capacity to share information about what goes on in our households, cars and workplaces.

The concept of the Internet of Things is having any device with an on-and-off switch connected to the Internet and to each other.

This includes everything from smartphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of.

The American research firm, Gartner, predicts by 2020, there will be over 26 billion connected devices.

Take the popular children's toy, Barbie, as an example.

The Mattel company that makes Barbie is on track to making the toy capable of having increasingly detailed conversations with its child owners.

Barbie will be able to discuss anything thanks to cloud-powered speech recognition.

On Christmas day, while we are listening to children running around excitedly in circles, so will Barbie.

Toys like Barbie are not just a conduit to some speech recognition servers based offshore, she's also a potential security risk.

Sometimes you get more than you bargained for.

This is because Mattel isn't an information security expert. It is a company that just want to make cool toys.

That means it is really likely that people will find vulnerabilities in the software; vulnerabilities that expose user data to people that shouldn't be able to see it.

Barbie is just one reminder that products are no longer only simply toys or appliances - instead they're a relationship with a company.

We'll be increasingly relying on third party technology to gather the information and present it to us or so it can interact with us but are we relying too much on third party companies to keep it safe?

Here's the thrust of the bargain we're striking with some of the major companies: I'll buy the device off you, you collect and present the data it generates for me - but you get to keep it all on your servers.

Future of privacy

If we're going to live surrounded by sensors, we really need to get our heads around how they work.

These are issues being discussed at the top tables for privacy.

Big data, the Internet of Things, transparency reporting - all these developments increase rather than detract from a focus on privacy.

The Privacy Act isn't going anywhere - personal information is still personal information.

The people who create and deliver shiny new products and services to us need to be careful about making assumptions about what the consumer is willing to give away in personal information.

The government needs to be careful about making assumptions about what the public will tolerate in its drive to deliver Better Public Services for the same dollar.

Are people willing to trade privacy for convenience? Are people willing to trade privacy for security? These are debates that need to be had.

I believe the public demand for restraint will be met both in the marketplace and in regulation.

Privacy is a space to watch. Thank you for your attention.