IAPP 2023: KEYNOTE ADDRESS, Wed 29 November 2023

Introduction

[Mihi]

I had … a wakeup call … a few weeks back.

In early October the Communications and Engagement team at my Office asked me to sign off on a media release about proposals by some schools to install CCTV in school bathrooms.

As you'd expect, the release covered the privacy issues that need to be considered, and recommended that schools carry out a privacy impact assessment to identify the privacy risks.

To be honest, while seeing the importance of the issue, I was a little surprised that we were proposing to use our valuable and limited media bandwidth on such a release, given we were up to our eyeballs at the time dealing with a whole range of important issues - around privacy and artificial intelligence, around a proposal to roll out facial recognition technology into supermarkets, around the future regulation of biometrics, around the growth of the surveillance state – such grand and important things!

I had already been on Breakfast TV that morning talking about FRT, and had taken part in a 20 minute interview on FRT on one of New Zealand's most well regarded radio current affairs programmes the Friday before.

And then … I get … cameras in school loos.

The Office team told me that this was a significant issue, and that several schools and parents had been in touch to check out what was allowed in this area, and so I agreed to making some public comment.

The media release went out … and the world went crazy.

In the space of the next two days, on the subject of CCTV in school bathrooms, I did several pre-record radio interviews for stations listened to by hundreds of thousands of listeners. I was interviewed live by the drive time radio host for one of the most popular radio stations in our biggest city. I appeared again on Breakfast TV, and CCTV in school loos was a story on most major radio, TV, internet and print news sources.

I have a number of reflections about this:

- People care more deeply about the right to privacy than many agencies may think;
- People have a well-developed radar when it comes to privacy intrusive proposals that might just cross the line;
- Privacy is not just cutting-edge tech and massive cyber-hacks; it's real and ordinary and therefore in some ways matters even more; and

- Any move for opinion makers and shapers to dismiss privacy as some sort of woke concern - that gets in the way of efficiency, effectiveness and productivity – needs to be rapidly reassessed.

Surveys, in New Zealand and overseas, and media stories, and the growth in complaints around alleged interferences with the privacy of individuals, back this up.

After 18 months in the role, I believe that I can detect a growing consciousness of the importance of individuals' right to privacy of personal information … and perhaps an increasing acceptance that my Office and its regulatory functions have a valid place in the institutional landscape.

These are important gains.

My first message to you all is that we'll continue to work with those in the broader privacy ecosystem to ensure privacy's place and value is nurtured and developed.

It is all our efforts that have led to this consciousness raising, and, because of the work you do, I wonder if we are on the cusp of privacy leaving the wings, and coming to centre stage.

OPC: Strategic focus

I thought it might be useful for me to remind you all of some of my strategic priorities as Aotearoa New Zealand's Privacy Commissioner.

People often say to me, "how will you know whether you're doing a good job as Privacy Commissioner?"

When I started in the role, and went out to meet stakeholders, and they asked me "the question", I told them that my Office will have achieved the needed change in approach and culture when privacy is treated as a core focus for agencies, as much as health and safety, or good financial reporting.

Privacy as a core focus will, I said, contribute to three desirable outcomes:

1. individuals will be more confident that their privacy is protected (just so you know, surveys show people right now aren't all that confident!)
2. agencies will better achieve their own objectives through respecting the privacy rights of New Zealanders; and
3. the right to privacy and the protection of personal information is valued in New Zealand.

In a world where all rights are being debated, defended, attacked and encroached – we say the rights of the individual, including the right to privacy, though not absolute, are of paramount importance.

We welcome the contest of ideas, but we will always hold to the overarching value or right to privacy of personal information.

The last 12 months

It has been another active 12 months for my Office.

We've tackled emerging and increasingly topical privacy issues, such as generative artificial intelligence or AI, biometrics, and children's privacy.

We've found ourselves responding to an increase in privacy complaints from individuals; these jumped from 486 in 2021-22 to 870 in 2022-23.

That's a 79% increase.

We've continued to record an increase in privacy breach notifications, from 657 in 2021-22 to 838 notifications in 2022-23 – a 28% increase.

Serious breach notifications increased 59% from 270 in 2021-22 to 429 in 2022-23.

With our Australian colleagues, we launched an investigation into the Latitude Financial data breach, New Zealand's largest.

I set out my expectations for agencies looking to implement AI, and followed that up with further guidance and advice.

And we have continued progressing our work around the regulation of biometrics.

Biometrics

On that, last year at this Summit, I said that we'd launched engagement to hear what New Zealanders had to say about the growing use of biometric technologies.

Last week I announced that my Office would issue an exposure draft of a biometrics privacy code, in early 2024.

Such a privacy code of practice would change how some of the principles in the Privacy Act apply, when organisations use technology to analyse biometric information.

We have concluded that the draft code should focus on requirements around proportionality, transparency and purpose limitation.

It has three parts:

A proportionality assessment would require agencies to carefully consider whether their reasons for using biometric technologies, to analyse biometric information, outweigh the privacy intrusion or risks.

Transparency and notification requirements would place clear obligations on agencies to be open and transparent with individuals, and the public, about their collection and use of biometric information.

Purpose limitations would restrict the collection and use of biometrics for certain reasons. We tested several purpose limitations in targeted engagement, including restricting the use of biometrics for direct marketing or to infer someone's health information or mood, and will develop these further along with appropriate exceptions (for example, exceptions for research or providing health services).

The material on biometrics is available on our website.

Directions for change

Turning now to what next, as we look ahead, I think we can all see that digital innovation, the growth in cyber-crime, and the growing mining and use of data to ramp up service delivery, and improve productivity, all create a complex environment for privacy regulators and those they regulate.

Significant privacy breaches are occurring.

These breaches are directly harming individuals (whether financially and/or emotionally), are costly to agencies, and are undermining trust in government and institutions.

As I've said on numerous occasions over the past year, the privacy harms we're observing can be addressed through further modernising the New Zealand Privacy Act.

Our Act is increasingly out of alignment with like-minded countries, who have been prioritising privacy reform.

Privacy experts have said that this, and potential broader global perceptions that we may no longer be one of the safest places to process personal information, could put New Zealand's place in the global data economy in some jeopardy.

I am now recommending to the government a set of specific amendments to make the Privacy Act fit-for-purpose in the digital age.

Today I want to highlight four of these proposals - in summary:

- A civil penalty regime for major non-compliance should be introduced, and accompanied with new privacy rights for New Zealanders to better protect themselves.
- And stronger requirements for automated decision making, and agencies demonstrating how they meet privacy requirements, should also be established.

First, with the increasing digitisation of modern economies, many of our international partners have established new rights for their citizens, such as a 'right to erasure'.

As you know, rights to erasure provide individuals with the power to ask agencies to delete their personal information, and sets out when agencies must do so.

The European Union first introduced this important right in 2018, California in 2020 and I understand that the Australian Government has just agreed in-principle to establish a right to erasure.

The benefits from implementing a right to erasure are significant.

Just one example, this year the Latitude Finance privacy breach affected over one million New Zealanders, even though many had reportedly not interacted with Latitude for years.

A right to erasure could have reduced the harm of this breach as individuals could have been ensuring that Latitude was only holding the personal information as long as it actually needed.

Second, our investigations into privacy breaches have revealed that some agencies will never care about privacy as they know there are no significant penalties.

Here's an example; my Office is currently engaging with one multi-national agency that is not complying with a statutory information request to inform our investigation.

The threat of a fine not exceeding $10,000 is not providing sufficient incentive for them to comply with our statutory demand or the requirements of the Privacy Act.

The incentives for compliance with privacy regulations are further reduced as this agency has been fined several hundred thousand dollars under a different regulatory regime.

In contrast, other countries are steadily introducing significant penalty regimes, reflecting the digital age we live in.

Third, while the Privacy Act has requirements that an agency must meet, such as maintaining appropriate security safeguards, there is no requirement for anything to be documented.

As you know, many countries and international privacy frameworks have an 'accountability principle' that requires agencies to demonstrate the purposes for which they are collecting personal information, and how they will safely manage the information.

To help address difficulties in this area, we will be providing comprehensive guidance to agencies on how to build a privacy-protective culture – more on that later

However, the impact of our guidance will be limited if there is no requirement for agencies to consider or document how they will meet Privacy Act requirements.

Fourth, significant privacy risks arise from automated decision-making, with problems such as inaccurate predictions, discrimination, unexplainable decisions and a lack of accountability.

Failures in such tools are usually not evenly distributed, perpetuating or exacerbating poor outcomes for disadvantaged communities.

Our trading partners have been introducing greater protections for automated decision-making.

And I consider that new measures need to be included in the Privacy Act to manage the risks of automated decision making to ensure that New Zealanders are treated fairly and equitably.

Guidance

I want to say a bit more about the priority my Office is giving to guidance.

Our focus in 2023 has been setting up a programme of work to develop some practical guidance and advice to agencies about how they can build and maintain their own system for privacy risk management, with clearer statements of our regulatory expectations.

This guidance is intended to help agencies raise their capability, and set a clear standard for them to work towards, but still be flexible and scalable for the unique circumstances of each agency - who must ultimately take accountability for their compliance with the Privacy Act.

Our aim for the guidance is both to help agencies and set our expectations as the regulator.

You can look forward to hearing more from us on this in early- to mid-2024.

One of the areas of guidance is, perhaps unsurprisingly, governance.

My concern is this: privacy is hitting the mahogany ceiling in many organisations.

The New Zealand Institute of Directors can be pretty matter of fact when you discuss privacy with them.

They say that you – or I - must be able to succinctly and powerfully answer the question that all directors have: a simple question – what's in it for me; why should we as a busy board make thinking and asking about privacy part of our behaviour, our culture?

The answer is out there:

- Privacy protective cultures and systems will have a positive bottom-line impact for a company or organisation.
- There are significant real costs associated with responding to and recovering from a privacy fail.
- There are significant revenue forgone costs associated with losing actual and potential customers' trust and confidence because you have suffered a privacy fail.
- There is a competitive advantage in being known as the organisation that is cyber smart, that securely holds and manages personal information.
- There is a positive rate of return in taking the time and effort to embed privacy into risk management planning and reporting, into internal audit programmes, and into the performance accountabilities from the chief executive down.

In order to get busy boards and directors to focus on privacy as a factor that they need to take seriously, we all need to share strategies and ideas on what works.

For example, the Institute of Directors sensibly points out that boards consist of people with different professional backgrounds – accountancy, IT, operations, strategy, te ao Māori, legal, engineering, and so on – so do the analysis of your board members and speak to them in briefings that target the lens through which they look at problems and opportunities.

As one year ends and another begins, I encourage you all to say to yourselves, and your teams, and your allies in your efforts to have privacy taken seriously: "This … this is the year – more than ever before - we take privacy to the boardroom!"

AI

I couldn't talk about privacy issues and trends globally without talking about generative artificial intelligence, or AI.

On one side, AI is the productivity holy grail; on the other side, we have had the AI doom merchants, some of whom, perhaps a little ironically, are the thinkers and developers behind AI, having their Oppenheimer moment!

Just a reminder of what some have been saying:

- In May the UK PM acknowledged the potential existential threat of developing a superintelligent AI without appropriate safeguards.
- the Google chief executive, said at the same time, "I still believe AI is too important not to regulate, and too important not to regulate well."
- Around the same time Sam Altman, I think still CEO of Chat GPT maker OpenAI was one of hundreds of experts who warned about the risk of human extinction from AI, saying mitigating that possibility "should be a global priority alongside other societal-scale risk such as pandemics and nuclear war."

It all seems a bit, as one recent tech magazine article put it in a headline, "Five ways AI might destroy the world."

I would say in response, it's more balanced than that – there's both good and bad, positive outcomes and negative outcomes.

Late last year, the management consultancy McKinsey published a survey, focused around digital trust, consumer confidence and AI.

The results are well worth reflecting on:

When it comes to AI, consumers want companies to provide clear information about their AI and data practices, they expect rigorous data protections to be in place, and they will make purchase decisions based on whether these expectations are being met.

72% of respondents say that knowing a company's AI policies before making a purchase is important.

And just under half of respondents would consider purchasing another brand if the company they are considering purchasing from is unclear how it will use their data. The percentage was closer to 60% for the Asia-Pacific region.

Over half of the executives surveyed said they had experienced an incident in which AI produced outputs that were biased, incorrect, or did not reflect the organisation's values.

These AI mishaps saw employees lose confidence in using AI – which of course could well have downstream implications in terms of innovation and productivity - and also resulted in financial losses in just under 40% of cases.

As I said earlier, I recently outlined my expectations around New Zealand agencies, businesses, and organisations using AI – the material is on our website privacy.org.nz.

Privacy is an enabling framework of "how to, not don't do", and my Office is here to help agencies achieve their goals in ways that uphold privacy, including when they use AI tools.

While we are using the regulatory tools we have, we will need better tools to meet new challenges.

New Zealand is currently behind international counterparts, who are moving quickly on regulation to support the benefits of AI.

We will continue to focus on advocating for legislative reform to our Privacy Act, to ensure it includes within it the powers and responsibilities necessary to regulate future directions in AI.

Conclusion

I have this morning wanted to talk privacy, ambition and action.

My concern … my worry … is that many agencies well know about the privacy threat environment – like the threats posed by AI – but are doing little in response.

Over the course of this Summit, I hope **you** will all spend a fair bit of time talking about ambition and action – about bringing about necessary privacy change.

Change is such a small word, but such a big and gnarly concept.

It's very hard for individuals to change.

It's even harder for organisations to change.

Appointing a vanguard for change is required.

I expect that the people in this room are already in the privacy change vanguard, and have a pretty good idea who it would be useful to have in there with you.

It can seem a daunting task, but the best advice I received about this was the old Desmond Tutu quote: "there is only one way to eat an elephant: a bite at a time."

What he meant by this, of course, is that everything in life that seems daunting, overwhelming, and even impossible can be accomplished gradually by taking on just a little at a time.

That may sound very evolutionary rather than revolutionary, very practical rather than visionary.

But can I ask you over the coming days to think about how, from the perspective of building cultures and systems that protect and respect privacy, you can have it all?

In doing so, there are two questions that we all need to keep at the front of our minds:

- How innovative do we need to be to achieve our mission? And
- How secure do we need to be to achieve our mission?

Innovation by itself can be a risky game, and security by itself will never see needed changes made.

As with most things in life – including protecting individuals' right to privacy- it's all about finding - and landing on - that place of balance.

Kia ora koutou katoa; thank you for the privilege of speaking to you all this morning.

END