Putting privacy first in local government

Privacy Commissioner, John Edwards' speech

ALGIM conference

27 July 2015

Palmerston North

Thank you for the opportunity to speak today.

I was pleased to receive the invite because we're at a topical moment for local government.

Technology developments are giving local governments more data about residents. This helps you deliver better services – but needs to be balanced against privacy.

Or does it?

"Balance" is a word I often hear in privacy-related discussions.

How do intelligence agencies balance privacy against their mandate to keep us safe?

How do DHBs protect patient privacy while delivering high-quality care?

And how do local governments holding large amounts of sensitive information about residents, balance the need to do their jobs against the obligations of the Privacy Act?

These questions, while thought-provoking, are based on a flawed premise. They assume that it's a zero-sum game – that to protect privacy, you have to shirk on your core services, or vice versa.

In reality, you can have it both ways. You *should* have it both ways. The Privacy Act doesn't have to impact on your ability to do your jobs, and your jobs do not have to impinge on peoples' rights to privacy.

Today I want to talk about how you can deliver on your Privacy Act obligations without compromising other obligations by making sure privacy is present in the culture and values of your organisation.

Survey results – Section 28c

I want to set the scene by talking about a survey my office recently completed.

Under section 28C of the Local Government (Rating) Act 2002, people can ask local governments to withhold their name and address from public records.

People should be aware of this right, because 28D requires local councils to inform them of it at least once a year.

The relationship between section 28C and privacy is pretty clear, so we took the opportunity to survey local governments and find out how many people were exercising their section28c right, and where.

As you can see, people in Wairoa are very circumspect.

As you can also see, there is a huge range between the different councils.

A substantial number have had less than 1% of their public records withheld at the ratepayer's request.

This shows how subjective privacy is.

Most people in New Zealand don't seem to mind having this kind of information made publicly available – or at least they don't mind enough to make the special effort to get it taken down.

As Wairoa shows, that doesn't mean that they sacrifice the right to do so.

Local governments need to make sure they have the processes and systems in place to deal with these requests.

Lack of education and misconceptions

The biggest issues my office faces come from misconceptions and lack of education about the Privacy Act.

A recent case my investigators dealt with was a stark reminder of how big a job my office has to do in this area.

In this case, a group of teenagers shoplifted from a retail store. The store's owner posted the pictures from the CCTV footage on Facebook, saying that they had 'forgotten' to pay.

Unfortunately, only two of the three teenagers had actually shoplifted.

The third teenager had nothing to do with it, but ended up being emotionally harmed from being publicly shamed on Facebook.

We went back and forth between the girl's father and the retail owner for awhile and eventually arrived at a settlement that cost the shop owner a reasonably large amount of money.

What struck me about this case was the fact that the shop owner was not trying to be malicious in any way.

She wasn't a "bad guy." She was just unaware of the implications of her actions.

In the case of larger organisations, such as local governments, we run into misconceptions about the Privacy Act rather than complete lack of education.

I've heard this referred to as "BOTPA." Because of the Privacy Act. "Because of the Privacy Act, we can't . . ." This is the major misconception of the Privacy Act – that it is a set of hard-and-fast rules that restrict behaviour.

The reality couldn't be further from the truth.

My vision for my role as Privacy Commissioner is to clear up these issues by making privacy easy. I want everyone – regular people, business owners and government workers to have a clear understanding of their rights and obligations under the Act.

I'd like to see a culture of privacy in every organisation, including local government. I want every person in the organisation to think about privacy as they go about their jobs.

In my view, this is the best way to prevent privacy breaches and the resulting investigations, settlements or referrals to the Human Rights Review Tribunal.

It's also the best way to make sure you can do your job without getting held back by the Privacy Act.

Online education

Online education is one of the ways we're making privacy easy. In the past, you may have joined us for one of our in-person privacy training workshops.

We've worked with professional educators to adapt the content of those workshops to a series of online modules called Privacy 101.

Privacy 101 covers:

- Key definitions
- The relationship between the Privacy Act and the Official Information Act
- The 12 information privacy principles – and how they apply in practice
- The consequences of breaching the Privacy Act
- My office's complaints process

These modules work by giving you information on a slide, then quizzing you along the way – so it's more active than passively reading a slide deck.

You can do these modules at your own pace, from your own desk, so it's a much easier time commitment for you and your staff.

They're also free.

This means you can have more people in your organisation take it and develop expertise about the Privacy Act.

I recommend that everyone take this course. You can do it in fits and starts, when you have a few minutes here and there, and the end result is a solid understanding of the privacy principles.

It should be part of staff induction.

My office is always working on new educational modules for specialist areas. If you'd like to see a module devoted to local government, get in touch through our website – if there's enough demand, we'll build it.

On the other side of the coin, resources like this means there are even fewer excuses should you find yourself in breach of the Act.

You have everything you need to create a privacy culture in your organisation; you just need to make it happen.

Encouraging a privacy-friendly culture

Engaging with our education offering is just the first step. Newly-trained privacy experts need to know that they are in an organisation that respects and champions privacy.

There needs to be a culture of "privacy by design" in your organisation.

If you don't have this culture right, you can run into some serious problems.

For example, cast your mind back a couple years to Lakes Environmental, a subsidiary of the Queenstown Lakes District Council.

A resident emailed asking for a complaint form, and instead received – inadvertently – a spreadsheet of every single complaint the QLDC had received for the last ten years.

The list was more harmful than a list of names because it was so extensive. Names, addresses, nature of the complaint – it was all in there.

This is relevant because people make complaints understanding that they will be anonymous. They put their trust in Lakes Environmental, and Lakes Environmental breached that trust.

However, Lakes Environmental – and the person who sent the email – didn't do so out of any malice. There was no intent to breach peoples' trust.

The breach was inadvertent. However, the right culture could have helped them avoid the conditions that led to the breach.

In order to avoid a similar situation in your organisation, you need a culture where people can ask questions and challenge assumptions around privacy

A tall order, I know. That's why it needs to come from the highest level of your organisation. The people in charge need to encourage "privacy thinking," and make sure it's not shouted down or ignored.

Privacy officer is the first step towards privacy culture

You can take your first step towards creating this culture by empowering your privacy officer.

According to the Privacy Act, your privacy officer needs to be responsible for:

1) Encouraging compliance with the information privacy principles
2) Dealing with requests made in relation to the Privacy Act
3) Working with my office on investigations
4) Otherwise ensuring compliance

This is easy to comply with in a superficial way, but you can get the most value out of your privacy officer by making privacy a key part of their role – rather than just an "on-paper" compliance exercise.

Your privacy officer should be your organisation's privacy expert, assessing new and existing systems and processes, proactively educating the rest of the team and maintaining an ongoing relationship with my office.

I encourage you to empower your privacy officer like this. You can even make it a KPI that they are routinely assessed on like any other part of their job.

I've seen organisations successfully implement this concept and very quickly create a strong culture of "privacy by design".

That culture puts them in good stead if and when breaches occur.

CCTV research

Back in 2009, my office released guidance around CCTV cameras. As local councils began to adopt CCTV systems, we did a survey in 2014 to find out more information about how our guidance, and CCTV systems in general, were being implemented.

We asked councils if they used CCTV cameras. As you can see, uptake has been very strong.

We asked if they were aware of our CCTV guidelines.

A majority – albeit not a strong majority – were aware.

This is good, but not great. We'd like everyone to be aware of the guidelines.

Finally, we asked if the guidelines were used in the design of the CCTV system.

This is the most worrying result.

Only forty percent of the councils can confirm that they used the guidelines. 12% went as far as to confirm they didn't use them at all!

The most optimistic scenario for the 48% who don't know is that they used the guidance but never documented that they did so.

The worst case is that they ignored the guidance.

Both scenarios can create liability for the councils for interfering with someone's privacy, should they complain about a breach in the future.

If you followed the guidance, but didn't document the fact that you did so, my investigators have to take your word for it. Documentation will put you in a much stronger position.

And if you ignored the guidance, you won't have much of a leg to stand on.

In a privacy-first culture, people involved in a project like CCTV implementation would be aware of the fact that there are privacy obligations to be met. Further, they would know to go to the privacy officer to find out the details of those obligations.

These results indicate that a number of local councils have work still to do to build a privacy-first culture.

Writing your own Privacy Act

Recently, I opened the floor to questions after giving a talk.

One of the first questions was from someone from a leading car company.

He asked me about the rules on information retention. How long could his employer hold onto customer data? A month? A year? Ten years? Twenty? What if they needed information only to find that the Privacy Act had made them destroy it at a previous date?

He was very passionate about the thought of the Privacy Act putting an arbitrary limit on how long his organisation could retain data.

I put his mind at ease by explaining that the Privacy Act doesn't have much in the way of hard-and-fast rules.

One of the great things about the Privacy Act is that is very contextual. It puts the onus on you to define how you collect and use information – then make sure affected people know these definitions.

In other words: the Privacy Act doesn't prohibit you from collecting information. Nor does it set arbitrary limits on how long you can retain it for.

If you clearly define how you are going to use information, then as long as you are using it for that purpose, you are acting within the bounds of the Privacy Act.

This freedom comes with responsibility. While you can use information for as long as you need it, you need to also clearly define which information you're going to collect, how you're going to use it and what you're going to use it for.

In local government, a lot of these definitions are going to come from other statutory obligations, such as the Building Act, the RMA, the Dog Control Act and the Public Records Act.

These Acts are much more prescriptive than the Privacy Act, and generally supersede the Privacy Act. The Privacy Act – and your privacy statement – should define how you execute on your other statutory obligations.

Again, this harks back to your organisation's culture and values. A privacy statement is one thing; an organisation that lives by it is another.

By working to ingrain the spirit of the statement into the way you actually do things, you'll help create a culture that reflects that statement through people who live by it.

Priv-o-matic

The Priv-o-matic is another tool my office has developed to help you build a privacy culture. It's an automatic privacy statement generator.

The Priv-o-matic works like a lot of other online forms. You answer a few questions, and it spits out a statement tailored to your organisation. It takes five minutes – sometimes less.

While the councils you work for probably already have privacy statements, I encourage you to try the Priv-o-matic, and cross-check the result against your existing privacy statement.

It's a good way to test the way you do things against the way you say you do things. If there are prominent gaps between the Priv-o-matic's privacy statement based on the information you put in, and your organisation's actual statement, there is a problem.

Using the Priv-o-matic on a regular basis tests your privacy policies and encourages your team to engage with privacy – which in turn helps build the privacy-focussed culture you need.

DHB lost notebook anecdote

If your practices don't match your policy, you can cause a privacy breach inadvertently. Late last year I saw a good example of this.

One of my senior investigating officers came to me with a file she'd been working on.

What had happened was that a health worker out on her rounds had her car broken into. Her notebook was in the car. In the notebook were the details of some 90 clients she had seen in recent years.

Her employer, a DHB, did the right thing, and got in touch with all the clients to let them know what had happened. Some of them were accepting of the error, some were a bit upset, but one was devastated by the breach and complained to us.

It had been some years since this one client had seen the health worker and she could not understand why she would still be carrying around her extremely sensitive personal information, which revealed details of mental ill health following the birth of a child.

Often, if a third party like a thief intervenes maliciously to release personal information, it would not be fair to hold the agency responsible.

But in this case, we had to consider whether the agency had taken reasonable steps to ensure the information was protected from loss.

Information privacy principle 5 of the Privacy Act says an agency that holds personal information shall ensure that the information is protected by such security safeguards, as it is reasonable in the circumstances to take, against loss or disclosure.

While we acknowledged that there would be cases where it was necessary to take patient information 'offsite' when treating patients in the community, we were not satisfied it was reasonable to expose this type of historic information by taking it out of the DHB.

As a last effort to resolve the complaint, I arranged to meet with the chief executive of the DHB. We had a very productive conversation and were able to agree to terms on which the complaint would be settled without referral to the Director of Human Rights Proceedings.

This case highlights a key aspect of the Privacy Act: under principle 5, you are responsible for taking all the necessary safeguards to protect information. When someone hands their personal information over to you, they are trusting you to protect it on their behalf.

Use this case as a rule of the thumb when you're considering any new system or process. Ask yourself:

- Have I taken sufficient steps to protect the data?
- How will people use and access this data? Remember, the DHB breach happened because of healthcare workers copying data into notebooks, not taking the files themselves.
- Have I done my due diligence on any third party providers? Do they take the steps they need to protect your data?

These are just a few starter questions. We have more extensive guidance for a variety of situations, such as cloud storage systems.

Privacy impact assessment

The questions I just mentioned are a start, but they are by no means comprehensive. If you're going to adopt a new system you need to do a comprehensive review of its privacy implications. Not just into how it works, but how it will be used.

This process is called a privacy impact assessment – or PIA for short. A PIA is methodology that you can use to flush out any latent privacy risks in a new project. Then you can assess each risk and determine which steps you need to take in order to deal to them.

By running a PIA at the start of a project, you can avoid the time and potential expense of breaches in the future.

My office has recently released guidance to help you go about a PIA. It's divided into two parts. The first part helps you determine whether you need to do a PIA. The second part walks you through the process of actually doing one.

It also has templates you can use for common scenarios in a PIA, such as risk assessment.

Section 40

You also need to consider the information access components of the Privacy Act. I saw this in practice earlier this year.

A woman who advocated for vulnerable members of society needed records from a government organisation about the individuals she was working with.

These people were elderly, and had been in the system for a long time. Their files could be thousands of pages, going back forty years or more. What's more, the organisation itself was not very large, so getting records was a manual process that took months.

This is related to privacy because information privacy principle 6 of the Act gives people the right to access information agencies hold about them.

Under section 40 of the Act, when agencies get an access request, they need to respond as quickly as possibly – and in no more than 20 working days.

They don't have to deliver the information in that timeframe, but they do need to update the requestor in that time frame, letting them know whether their request has been accepted or denied.

The agency in this case was taking an extremely long time to comply with principle 6.

This was fine in and of itself, but the agency was *not* giving an update within 20 days, as they are required to do under section 40 of the Act.

We organised a meeting with the organisation and explained their obligations.

They are now complying with the Act. Finding and delivering the information is still taking a long time, but by keeping people in the loop rather than having their request disappear into a vacuum, the agency is complying with the Privacy Act.

They would have avoided this time-consuming situation simply by calling the advocate to let them know what was going on.

This story shows that privacy and service delivery aren't at odds with one another. The agency didn't have to hire new staff, rebuild processes, buy new systems or do something similarly expensive.

They didn't have to sacrifice their ability to deliver in other areas in order to comply with the Privacy Act. All they had to do was make sure they contacted the requestor within 20 working days.

It's an example of the Privacy Act augmenting good business practice, but not forbidding it or requiring wholescale change.

Conclusion

Privacy is important. And as technology progresses, and our society becomes more connected than it already is, it's going to become even more relevant.

But that doesn't come with tradeoffs. Privacy should add to everything you do, integrating with and adjusting your practice without being a roadblock.

The way to do that is by educating yourself, educating your team and making sure your organisation has the culture to let that education flourish in your organisation.