“Managing customer demands for personal information”

Privacy Commissioner John Edwards

Presentation to Christchurch insurance companies - held at Southern Response Earthquake Services – Urupare ki te Tonga

Monday 12 September 2016

What is personal information?

Privacy concerns you.

It is information about you - your information and your life.

This information can be used to help you – think electronic patient records which enable health professionals to keep get the latest information about your health status and treatment.

This information can be used to harm you – think of your bank information, credit card details, and internet passwords in the wrong hands.

Your personal information includes anything from your medical history; your employment record; details of your relationships, tax status, and even analysis of your DNA.

Think for a moment who has access to information about you and whether they have rules around the way your information can be viewed and used.

The Privacy Act in New Zealand covers “personal information”.

That means information about "identifiable" individuals.

The Act applies to almost every person, business or organisation in New Zealand.

It governs personal information about each of us – including information about our families, friends and colleagues.

What is personal information?

- Your name?
- Your phone number?
- Your email address?
- Where you bought your dinner last night?
- Where you went for a run this morning?
- Your IP address?
- Your car number plate?

Under the Act, personal information is any piece of information that relates to a living, identifiable human being.

People's names, contact details, financial, health, or purchase records: anything that you can look at and say "this is about an identifiable person".

In some cases, like your IP address or car number plate, it's going to depend on the context of the information.

Privacy Commissioner's role

So what does the Privacy Commissioner do?

I am an Independent Crown Entity, funded from the public purse, but with statutory independence.

I have a watch-dog role and independent investigation and inquiry functions.

A major part of my role is commenting on legislative and policy proposals.

My Office also has an important communications function.

We receive around 9,000 enquiries a year, including about 300 enquiries from the news media.

The public and agencies depend on us to educate, inform, advise and send the right signals about relevant privacy issues.

I can also issue industry codes of practice – in health, telecommunications and credit reporting.

My focus is on ensuring individuals are informed about what is happening to their information so they can exert some control over it, if they decide to.

I also want to help organisations maximise their potential in a way that minimises the risks that comes from poor handling of personal information.

Access to information

One basic right that all of us have under the Privacy Act is the right to access our information.

Access to information enables us to engage effectively with organisations and to have a say in decisions that may profoundly affect our lives.

It is not just a ‘nice to have’ that gives way to more important priorities in disaster recovery.

This right to ask for your personal information is one of the Privacy Act’s 12 guiding privacy principles.

Principle 6 says where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled:

- to obtain from the agency confirmation of whether or not the agency holds such personal information; and
- to have access to that information.

Principle 6 also says when an individual is given access to their personal information, they shall also be advised that, under principle 7, they may request the correction of that information.

Repair or rebuild

Returning to the definition of personal information, I want you to consider how this would also include – especially relevant in the Christchurch context – property information, including geotechnical and structural building details.

This is information set against a bewildering backdrop of variables – red or green zone; technical categories 1,2 or 3; land, building and contents damage; and under cap or over cap, for examples.

Differences in any of these variables affect what options are available to the property owner and they affect the overall decision to repair or rebuild.

You'll be well aware there's a lot at stake – especially for people seeking certainty in the aftermath of a catastrophe.

When people are not satisfied with the response they receive from an agency, they complain to us.

Well over half - 60 percent – of our complaints are from individuals asking us to review the results of access requests they have made to agencies.

Using EQC as an example, if the requester is an individual, the information collected by EQC about that individual's claim will likely be:

- a mixture of personal information about the requester and their interactions with other persons or the property
- information solely about other persons
- and information solely about the property itself.

The first category of information is subject to the Privacy Act.

The latter two categories are covered by the Official Information Act.

While separating the two types of information may be complex at times, most of the time the procedural provisions and withholding grounds in the two Acts are very similar.

EQC report

I mention EQC because in late 2013, my office and the Office of the Ombudsman undertook an investigation into a backlog of access requests at EQC.

EQC had got so bogged down in access requests that it was failing in its obligations to comply with both the OIA and the Privacy Act.

Our joint report – *Information fault lines: Accessing EQC information in Canterbury* – found that EQC was routinely breaching access to information requirements and advising people there would be a six to seven month delay before the agency could respond to requests.

The Privacy Act and the OIA both state that an agency should respond as quickly as possible within 20 working days.

Increasing demand and decreasing compliance

In the three years leading up to the Canterbury earthquakes, EQC received a total of 27 requests for information.

These were handled by about five staff.

In the 22 months between September 2010 and July 2012, EQC received 2,289 requests - at a rate of around 30 per week.

By June 2012, it was clear EQC was struggling with the volume of information requests.

By this time, the agency had 358 outstanding requests, of which 151 were overdue.

But in July 2012, EQC received an additional 254 requests at an average of 63 per week.

The majority of requests received were in-depth with some specifying such items as handwritten notes, memos, stored voice messages, recorded phone calls and emails – both internal and external.

From August to mid-October 2012, EQC was receiving an average of 50 to 70 new requests per week.

This shot up to an average of 162 requests per week between 2 November and 14 December 2012.

The agency was overwhelmed and falling further and further behind its statutory requirements to respond in a timely way to people who were desperate for information about their homes and other properties.

Speeding up the process

During the course of our joint investigation, we visited EQC to observe the processing of information requests.

In a test case, we calculated that a typical request for all the information held on a claim file.

We broke down the process into its components parts:

- checking a request
- locating the documents
- preparing a letter to the requester
- re-scanning the documents
- and peer-reviewing the request.

The process was estimated to take six hours.

We then worked with EQC to amend the process to increase compliance.

These changes were included in our report's 13 recommendations which were designed to:

- streamline the processing of claim file information requests
- improve the quality of information and service provided by call centre staff
- consider the automatic provision of property reports to owners, and
- improve the website delivery of information.

In our view, EQC had adopted an over-complicated and risk-averse approach to responding to information requests.

It also had a tendency to be reactive rather than pro-active in communicating claim-related information.

EQC accepted all the recommendations and took steps to implement.

The agency engaged positively with my office and the Ombudsman in addressing the matters highlighted by our investigation.

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

One of our aims is to reduce the number of access complaints to our office by making organisations aware of this important feature of the Privacy Act.

Businesses like yours have a really important role to play in designing information systems to help 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 New Zealand gets 28,000 requests for personal information each year.

Another example - the Ministry of Social Development has a backlog of 2,100 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.

Naming policy

In the case of EQC, our involvement with them was welcomed and our recommendations were received positively and adopted.

We didn’t set out to name EQC because everyone already knew about EQC and its difficulties in keeping up with the volume of access requests.

But what happens if an agency is deliberately non-compliant and unrepentant?

There are consequences for getting privacy wrong, which I will use as part of a regulatory response.

One consequence is to be named by my office.

This is a policy we developed in 2014.

It helps us hold agencies accountable for breaching privacy by publicly identifying the organisation.

We name agencies in a number of circumstances, such as when we suspect wider systemic problems or when an agency flagrantly disregards the law.

Immigration New Zealand

Here's a recent example.

In 2011, a young Ethiopian man immigrated to New Zealand, sponsored by his aunt.

He did not know how old he was, as his parents had died when he was very young and there was no record of his birth – birth registration is not compulsory in Ethiopia.

In order to obtain a birth certificate to support his refugee application, his aunt consulted with locals and estimated his birthday to be in early 2000.

Immigration NZ used this birth date on his refugee visa.

But after he arrived, he had a bone density scan and dental examination to double-check his birth date.

The tests indicated he was at least 16 years old when he arrived in New Zealand in 2011 and could have been as old as 18.

Based on this information, the young man asked Immigration New Zealand to correct his birth date on two occasions.

On both occasions, the agency said no.

After we investigated his complaint to us, we concluded the young man's case had merit and there was a need for a legal precedent to help guide similar cases in the future.

I therefore referred the matter to the Director of Human Rights Proceedings and publicly named Immigration New Zealand for not complying with the law.

Happily, the case has now been settled.

The complainant received a confidential settlement from Immigration New Zealand and is now able to access his entitlements because of his corrected age.

Referral to the Director of Human Rights Proceedings

When we receive complaints, we have the option of referring them to the Director of Human Rights Proceedings, who may take the case to the Human Rights Review Tribunal.

As with our naming policy, we reserve this option for particularly notable cases.

The HRRT can award up to $200,000 in damages, and public judgements almost always name the respondent, which carries further reputational harm.

The damages awards from the Tribunal have been trending upwards for a couple years.

NZCU Baywide

You may have seen this next story in the news media last year.

The finance company, NZCU Baywide, disclosed a photo taken from a former employee's Facebook page and used it to damage her reputation.

The photo had been shared by the complainant on Facebook among her circle of Facebook friends.

It featured a cake with written obscenities referring to NZCU Baywide which she was at the time in the process of leaving.

The privacy setting meant only those who had been accepted by Ms Hammond as friends had access to the photo, taken at a private dinner party.

NZCU Baywide's then human resources manager coerced a junior employee to reveal the photo on her Facebook page.

The manager made a screenshot of the photo and disclosed it to other senior managers.

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

The complainant was forced to resign her subsequent job because of the threat by NZCU Baywide to boycott her new employer.

She was unemployed for 10 months and was not able to find employment in her preferred field of finance.

Her close relationships were severely affected and the stress caused significant harm to her family.

The Human Rights Review Tribunal noted that she and her partner had struggled financially and emotionally.

The Tribunal's award of $168,000 damages to the complainant is ground breaking.

The amount set a new benchmark for compensating harm caused by a breach of the Privacy Act for unlawfully disclosing personal information.

So the stakes of going to the Tribunal are getting higher – these aren't parking tickets or slaps on the wrist.

Law reform

Parliament is set to reform the Privacy Act to give my office greater enforcement powers.

These include mandatory breach reporting, and the ability to fine agencies up to $10,000 for a variety of offences.

This means if there's a data breach and it meets a certain threshold of seriousness, an organisation will have to report it to my office and explain what it is doing to fix the breach.

Currently, breach notification in this country is voluntary so we don't get to find out about all of them.

When the law changes, I'll also be able to issue compliance notices that compel agencies to take an action, or to stop an ongoing action.

What you can do

I'll finish off by outlining a few practical things you can do to maintain customer trust.

You can instil a culture of privacy by making sure everyone in your organisation has a firm base of privacy knowledge.

You can check out our newest tool – Ask Us.

These are interactive FAQs on our website.

You should be able to find answers to many privacy questions by typing them into Ask Us.

If you can't find an answer, there's a field where you can let us know – please do so!

It's a living product that is constantly evolving.

And in order to also help you get a better grip on privacy, we've put together free online privacy training modules.

You can undertake this training at your own pace, from anywhere.

There's a Privacy 101 module that gives a solid broad-level understanding of the Privacy Act.

Conclusion

I want to conclude with a checklist of some of the sorts of things that I will be looking for in the event that things go wrong:

- Organisational culture and awareness of good privacy practice
- Levels of training for staff
- Sensible, clear policies and privacy statements
- Use of privacy impact assessments
- Engaged privacy officers
- Awareness of data breach notification and mitigation

- A risk management framework backed up by effective governance

If we are investigating a complaint against your organisation, these elements will become relevant and if your organisation has got its privacy mix right, it will reflect well on your organisation.

END