“Making privacy work for local government”

Privacy Commissioner John Edwards

To Christchurch City Council

12 September 2016

Introduction

Thank you for the warm welcome.

I’m here to talk about how local government can address privacy concerns.

Two privacy-related topics in particular stand out as being relevant to local councils – the availability of online property and building information, and the use of CCTV and body worn cameras.

I thought I’d begin by mentioning a recent news story involving Trade Me and the Stratford District Council.

You might have seen it on the Herald or Stuff websites.

Trade Me made a request to all local councils in New Zealand to provide property and sales data in their respective localities.

Trade Me asked for the information because it wanted to provide a yet-to-be released new service on its Property website to customers.

Sixty-one councils agreed but the Stratford District Council - with its population of just over 9000 people - said no.

Trade Me says it is not asking for access to any data that contained personal information and publishing the data would not be a breach of privacy.

But the council said it did make specific sales information freely available to the general public.

Clearly not all communities feel the same way about privacy as Stratford demonstrated by taking this stand on property sale data.

And this instance does highlight the concerns of re-identifying individuals from anonymised data in small communities.

It would be obvious to many in a 9000-strong community whose property sold and for how much.

It is also a good starting point for our discussion today.

My office has developed some general guidelines which should help future online record developers avoid some common privacy pitfalls.

But first, I thought I'd talk a little about what my office does.

What does the Office do?

The functions of the Privacy Commissioner are set out in section 13 of the Privacy Act.

We do many different things including:

- investigating privacy complaints
- providing policy advice and practical guidance
- monitoring technology developments
- promoting understanding of the 12 information privacy principles
- and monitoring compliance.

Over the years, the Office has received many complaints about the online publication of information, and has carefully monitored online information developments while advocating for a cautious and privacy-enhancing approach.

It is also an area that attracts a fair bit of media attention with recent stories about the availability of online property information in Hawke's Bay and Queenstown.

Public registers such as rating information databases and building consents create a tension between people's privacy rights and a wish to have certain information publically available to serve some public purpose.

This same tension applies to online property information.

So how can we tackle this tension over online information?

Hastings District Council case study

I'll start with a case study.

Last year, Hastings District Council created an award-winning online property system that made getting property information easier and more convenient for potential property owners and other interested parties.

The online property file search system contained a combination of statutory documents and general correspondence, including but not limited to:

- building information
- details of resource consent applications
- swimming pool inspections, and
- health inspections.

The creation of this system reflects government's commitment to open information, a desire to decrease the burden for councils of meeting LIM requirements, and an increased expectation that local authorities are efficient and user-focused.

However, as Hastings District Council found out, when they decided to temporarily shut down their system to address privacy complaints, there are some privacy risks of making records available online including:

- confidential information, such as the name and contact details of informants or domestic violence victims, being made public;
- bots extracting an entire database of information for marketing or scams, and
- building plans and specifications of public figures becoming available to criminals.

This is because online records often contain personal information such as names, contact details, financial information and information about disputes.

For example, using the Marlborough District Council's property file system, you can see the name of the person who applied for a resource consent and their phone number.

This creates a headache for all government record holders.

On one hand, there are a number of statutory mandates to collect and distribute information; on the other, there are statutory mandates to protect individual privacy.

The legal relationships concerning government-held information are complex.

The nine Acts of Parliament

Here I have a diagram of just some of the laws that apply to council-held property and building information.

These nine Acts either:

- specify the types of property and building information councils must collect;
- outline how this information should be provided to the public; or
- set out general principles for how councils should treat information.

Pro-active release of certain types of property and building information, such as building consent records, is a requirement of statutes such as the Building Act and the Resource Management Act.

The LGOIMA does not specify how councils should release other types of property and building information.

The Privacy Act sets expectations about the need to treat personal information with care.

This means that information releases should be assessed with the following in mind:

- Does the information need to be made public under another Act (such as the Building Act or the LGOIMA)?
- Can the council take reasonable steps to ensure people know that their information is being collected and disclosed?
- Can the council take any steps to ensure that people can only use the information for its intended purpose?

While there are a number of ways to release information pro-actively, some are more conscious of privacy than others.

For example, an online database of rateable values, searchable by address only, complies with the legislative mandate to make this information available without compromising personal privacy.

By contrast, a database that allows people to search names to see which properties they own and how much they're worth would likely compromise these people's personal privacy.

There is no one single way to manage this tension.

Central and local government need to consider and manage privacy risk in a way that is specific to their systems, processes and community expectations.

The Privacy Act

The Privacy Act can be used as a guide on what to consider when releasing information.

For example, you could ask:

Was the information collected or disclosed for a lawful purpose?

Some legislation requires councils to collect and disclose certain information, such as section 216 of the Building Act.

Has the council taken reasonable steps to ensure residents are aware that this information could be made publicly available?

Councils could use privacy statements or terms and conditions to let individuals know how their information could be disclosed.

Has the council taken steps to prevent information collected for one purpose from being used for another purpose?

Councils could limit the use of pro-actively released information by limiting search terms to address - rather than name - and not allowing bulk downloads.

These are the sorts of questions that we would ask if we received a complaint about information being made available online.

Privacy proofing online records

How do government bodies privacy-proof their online records?

Digital information systems introduce different privacy risks because of the accessibility and immediacy of electronic records in comparison to paper-based systems.

This is because electronic records are:

- more immediately accessible
- able to stored and copied at negligible cost
- more easily linked to other online information sources, and
- do not rely on administrative expertise for members of the public to access specific records.

One way to incorporate these guidelines into your information systems is by using a technique called Privacy by Design.

Privacy by Design is an approach which sets out a sensible way to think about all aspects of system design and implementation.

A privacy impact assessment is another tool which can be used to design systems in a Privacy by Design way.

You can refer to the privacy impact assessment toolkit on our website, which includes templates and guidance.

Our guidance

In the course of looking into this issue, I have seen different councils adopt a range of responses.

These can range from one that requires people wanting access to property files to physically present themselves to the council offices, to those which allow the unlimited download of all building consents without restriction.

While it is not for my office to direct councils how to design efficient and user friendly property and building records systems, I am here to help.

Earlier this year, my office published a report – our Privacy and Online Property Information Report – which is intended to provide guidance to local authorities.

You can find it on our website or by contacting my office.

Since we started the project last year, my office has heard of many innovative privacy-enhancing safeguards being developed by councils.

For example, one council informed us that it was going to cross-match unpublished electoral rolls to online property and building records to ensure that the addresses of people who have a demonstrable need for greater privacy are protected.

I am looking forward to seeing and hearing about the creation of new privacy safeguards by councils.

If you are developing or considering changes to your online records, contact my office.

We are happy to provide advice about how to make these record systems privacy-enhancing by being both legally compliant and reflective of the expectations of privacy that your constituents have.

Barking dogs

Earlier this year, the news media reported that Christchurch City Council's dog control unit had been using listening devices to monitor dog barking, generally with the homeowner's consent.

Using environmental devices to assess and monitor a problem through the collection of information can be a good idea.

It can help diagnose the nature and extent of the problem and then help select an appropriate response.

But in one case – which I am sure you are all aware of – a Christchurch couple was shocked to discover a recording device under a shrub.

You probably don't need me to remind you of the need to be mindful of the potential privacy impacts of using environmental devices to collect data – and to be mindful of giving the local newspaper the licence to write a headline that refers to a 'secret listening device'.

These privacy impacts can usually be managed by getting the consent of the people likely to be affected.

The use of devices by businesses or public authorities in a way that could potentially collect personal information needs careful management and oversight.

Councils in Britain got into strife some years ago for secretly spying on local residents to catch dog fouling and rubbish infringements.

Although there is a public interest in catching infringers, the public saw the level of surveillance as disproportionate to the level of offence being investigated.

As I discussed earlier, the Privacy Act's information privacy principles provide a general framework:

- Principle 3 says that an agency collecting personal information has to make sure the individual is aware that it's being collected and why

- Principle 4 says that an agency can't collect personal information in a manner that is unfair or unreasonably intrudes on the individual's personal affairs, or in a way that's unlawful.

As well as the Privacy Act, other laws could be relevant to operating a device, like the Search and Surveillance Act 2012 and the Bill of Rights Act 1990, and civil law that limits privacy intrusions.

It's worth keeping these in mind when operating any device that has the capacity to collect people's information, be it CCTV, body worn cameras or audio recording devices.

CCTV and body cameras

The use of body worn cameras on council parking enforcement and animal welfare staff is becoming an increasing feature of those who work for councils in those areas of responsibility.

At least three councils, including Christchurch, are now using them.

This is an understandable response to the physical and verbal threats made by a small minority of the public - and the use of cameras can have a deterrent effect.

But they can also be seen as a provocation by some people.

Our CCTV guidance – which is also available on our website – applies to body worn cameras because the same principles apply in helping to identify the privacy risks of recording in a public setting.

It's important that you define exactly what you are going to use the cameras for - and therefore how they will not be used.

For example, the purpose might be to prevent or record for evidential purposes abuse and assaults against parking enforcement officers.

To achieve this purpose, there is some personal information you will not need to collect, such as private conversations between passing members of the public.

Council's also need to think how the wearer can retain some privacy - is the camera able to be turned off during breaks or personal conversations?

The camera shouldn't be used to monitor the officer's own performance or working hours, as there are less intrusive ways to achieving this.

Since the cameras will capture personal information about the wearers as well as the general public, both should be adequately notified about what information will be collected and what will be done with it.

Developing a best practice user guide for your staff will help ensure that they are aware when the cameras need to operate, and how to use the cameras appropriately.

For example, if an abusive situation arises, the officer should tell people that they are being filmed and that the recording may be used as evidence.

Other matters to consider include how you will store the information securely and how long you will retain it.

The Tribunal and CCTV

In 2014, the Human Rights Review Tribunal dealt with a case involving two neighbours – a householder and the next door resident who ran a bed and breakfast.

The householder complained that the bed and breakfast business had three cameras overlooking his property.

The Tribunal found that one of the cameras breached the Act but the other two were saved by the use of masking technology.

As part of its analysis on the case, the Tribunal usefully said that "leveraging technology to enhance privacy is a valuable approach and is to be encouraged".

This is the role of "privacy enhancing technologies", known to the profession as "PETs".

Despite the apparent camera angle, the neighbour's backyard and side door were not in fact visible to anyone watching the footage live and nothing in those areas was recorded to the hard drive.

Use of the masking technology saved those cameras from being in breach of the Act.

But what we had in this case was a failure to communicate.

The problem for the neighbour was that it was not obvious whether the cameras were recording and, if so, what they were recording.

All the neighbour could see was that they were pointed at his house.

The Tribunal said this highlighted the importance of communication.

Agencies need to give clear statements about what the cameras are there to do - and other matters listed in principle 3.

Agencies also have to respond to reasonable requests by affected people to see the system and know what information it was recording, so that those people can be confident the system is working lawfully.

The concept of social licence

I want to conclude talking about the concept of public trust and social licence.

An important conversation about the future of data in New Zealand is currently being facilitated by the Data Futures Partnership, which was established by central government in August 2015.

This partnership is "a cross-sector group of influential people working together to drive high-trust and high-value data use for all New Zealanders".

The Data Futures Partnership has established a sensible approach for data sharing and use.

These principles are an important step towards a data-driven environment that respects and protects personal information while delivering better value to individuals and organisations.

The Partnership's four principles of value, inclusion, trust, and control are consistent with privacy values.

If individuals feel in control of their information, then they are more likely to feel that it is being used appropriately, and can therefore trust data holders to use this information in a responsible way which improves their lives.

Innovation is needed by local and central government to find ways to ensure that individual's retain control over their information in the face of new technologies.

Social licence is also a useful concept related to people's attitudes towards new technologies.

The idea is that as agencies' activities gain the acceptance and then the trust of their communities that they gain a "social licence" to operate.

For example, the concept of social licence applies to online property information as it illustrates the importance of community engagement and understanding.

This engagement with communities should be ongoing, as people's attitudes to how their information should be used and made available change over time.

This all leads to the conclusion that privacy is dynamic and requires end-to-end thinking and design.

People will lose trust in services which are not transparent about data use and that don't take appropriate care of their information, especially more sensitive information.

Online privacy tools

One way we have been addressing the issue of trust is by developing a number of online tools to help people take control of their information and make it easier for agencies to comply with their Privacy Act obligations.

For example, About Me is a tool to help people ask agencies like yours for information about themselves.

A request generates an email that goes to an agency.

The tool prompts people to make their request as specific as possible, hopefully saving an agency time in responding to a large scale request, and the email to the agency also includes information on how it is required to respond.

Another of our online tools is designed to help agencies set out their privacy statements in language that people can understand.

You may have already seen Priv-o-matic on our website.

It was created to help agencies generate basic privacy statements which explained in plain language what information was being collected and for what purpose.

There are also our online privacy learning modules.

I recommend anyone who works with personal information to do the Privacy 101 module.

And if you work in the health sector or with people's health information, there's one on the Health Information Privacy Code.

You'll need to register to do them but you can log out and back in again to pick up where you left off.

Lately, there's AskUs, an online enquiry tool or interactive FAQ resource.

Type in your privacy related question or dilemma and it will bring up a choice of answers that hopefully meet your requirements.

AskUs is designed to be incrementally improved and to do so we need your feedback on whether the answers met your needs.

If not, tell us and we will work on making it better.

And of course you're always welcome to email us directory at https://www.privacy.org.nz/enquiries

If we’ve got some time, I’m happy to take questions.