Privacy Commissioner
Te Mana Matapono Matatapu

PRIVACY COMMISSIONER'S SPEECH

MARKETING LAW CONFERENCE

Pullman Hotel, Auckland – Thursday 24 July 2014

Introduction

What might our weekly grocery shop say about us, our budgeting choices, income strata, gender, household size, food, cosmetics, personal hygiene and drink choices? What might our online purchases say about us? What might our internet browsing histories show?

The answer is a lot. We leave an electronic record of what we consume and what we aspire to and that information is marketing gold. It enables you to target the resources of your companies and clients better to reach the segments that are most likely to buy your products and services.

And we, as consumers, are prepared to give up our personal information for shopping and promotional deals. One fast evolving aspect of the equation between personal information and organisations that collect the information is that personal information is now a tradable commodity. It is sold or passed to third parties who then customise the information to fit their marketing agendas. People's concern - and in many cases, resignation and apathy - over losing control of their personal information is a recurrent theme in the privacy surveys we carry out.

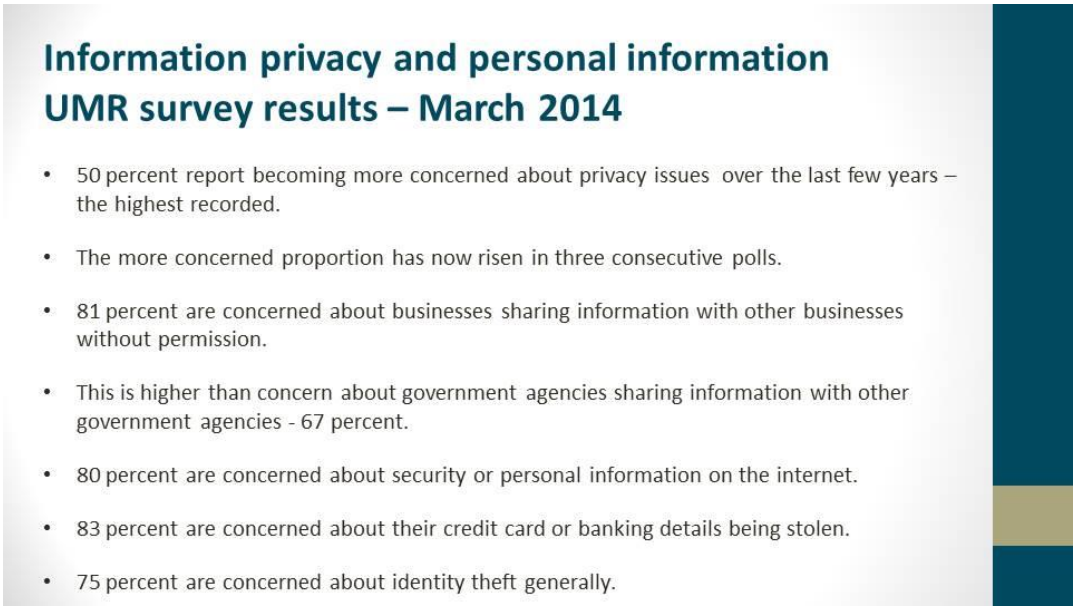
Dana Boyd, a social media researcher at Microsoft and a Fellow at Harvard University's Berkman Centre for Internet and Society says:

"Privacy isn't a technological binary that you turn off and on. Privacy is about having control of a situation. It's about controlling what information flows where and adjusting measures of trust when things flow in unexpected ways. It's about creating certainty so that we can act appropriately. People still care about privacy because they care about control."

Dana Boyd wrote this in relation to Facebook's privacy settings. While it relates to Facebook's up to recently cavalier attitude with its users' privacy, I think you'll agree that the fact that 'people still care about privacy because they care about control' is also relevant to all relationships between seller and customer, and service provider and user.

Privacy environment

So let's have a look at the public mood about privacy and personal information. We commission a two-yearly UMR survey and it is revealing for showing us the kinds of subjects and issues where there are privacy mood swings. Central to the survey is how people feel their personal information is being treated by organisations.



The main message that came out of the survey carried out in February this year said half of all New Zealanders reported becoming 'more concerned' about privacy issues over the last few years.

This is the highest level yet recorded in that category in the tracking survey – up from 40 percent in the previous survey carried out in 2012. And more young people say they have become more concerned about their privacy. This has risen to 50 percent – an increase of 17 percent on two years earlier.

In addition to the survey, we hold a number of focus groups which gave us qualitative results. Most respondents said they are quite concerned about the way their personal information was being used and protected. But interestingly, these concerns were often acute enough for them to stop sharing their information through loyalty cards and by registering for special deals or prizes.

Respondents also did not feel as forced to deal with companies as they are with government agencies. In a competitive private sector environment, people can choose who they deal with but in dealing with government agencies, they feel less empowered because they often have no choice but to provide information.

In the retail environment, people viewed giving up some of their personal information as a trade-off between their privacy and the goods and services they got in return. While they are very much concerned about the way organisations protect their personal information, they are less so about how those organisations use the information.

Many of the survey respondents recalled incidents when it appeared that their personal information may have been given to or taken by organisations other than the ones they were dealing with.

We were able to draw three observations about how people felt about the collection and aggregation of their information with everyone else's. You might call this a proxy for their feelings about so called "Big Data".

Firstly, the accumulation and aggregation of personal information is seen as an expansion of traditional marketing activities, with the added benefit of making it more likely that the marketing would be appropriate to them.

Secondly, survey participants could not see how they would be significantly harmed. In other words, they saw it as more people trying to sell them things but not at a financial cost to them personally – unless they choose to buy.

Thirdly, their own personal data would be 'buried' amongst thousands of other records. They felt more comfortable that they would be targeted according to algorithms rather than because someone was specifically studying their information.

Here are some quotes from our survey participants.

Regarding third party marketing:

> *"If they are only going to use it for the purpose they have gathered it but then they flog it off to a third party, we are never going to know about it because how are you going to prove it was that company that gave your details out?"*

> *"Being targeted by companies online like when you send an email and you get recipe companies coming at you – that doesn't make me happy. I sent an email once about a recipe and all of a sudden they all came flying at me. I began to feel spooky about that."*

Targeted marketing:

> *"They know what you buy so if you buy a whole lot of wine or a lot of tacos, then they will bring up something about tacos or some Mexican foods or wines. It is alright as long as they keep my information but are they selling that information to anyone?"*

> *"I use Map My Walk and I post my training days and the times I do, and I get specific targeted marketing - I don't have a problem with that. It is just when the marketing is not appropriate or no interest to me, then I am more concerned."*

And this one is what I call the Minority Report effect:

> *"I think maybe it is the way of the future. Are they tracking how many condoms you buy and how much chocolate you buy, and they say you bought 12 condoms and then another 12, then you*

obviously have had sex 12 times over two weeks – so why don't you try these this week because we know you are getting low on condoms? It might become worse and worse and worse. I guess people just adjust over time like they have with Facebook and the privacy stuff but I don't like it."

"I really like it. Countdown knows I really like vanilla bean yoghurt and when it is on special, it emails me and I whip down there and buy it."

About trust:

"I think I am more likely to trust a New Zealand company than I am to trust one from overseas. But I would never save my details on the internet for next time - that unnerves me."

"If it is a popular brand or company, they have more of my trust."

Social media:

"For me personally, advertising can try as hard as it likes. I have very specific tastes, I have a very specific style of shopping and we have a particular lifestyle. So I go, yes, they have shared my information for whatever reason, I have agreed to the Facebook terms and conditions, and they are sending me some ads and I don't care, they can try all they like."

"It is just a modern day version of your letterbox. You are getting junk mail in your letter box."

Now, let's say you have all this information about people and their spending habits and preferences. It is all the better to target your marketing better. But what happens if the retailer or marketer which holds the information fails to adequately protect that information?

When things go wrong

In the United States, a retail chain called Target last year suffered a very damaging data breach. You may be aware of it. The case now serves as a cautionary lesson on how costly it can be if things go wrong – both financially and also for a brand's reputation.

The Target data breach by the numbers:

- 40 million: The number of credit and debit card details stolen from Target during November and December 2013
- 70 million: The records stolen that included the name, address, email address and phone number of Target customers
- 1 million – 3 million: The estimated number of cards stolen from Target that were successfully sold on the black market and used for fraud
- 100 million: The amount Target says it will spend on upgrading its payment terminals to support PIN-enabled cards
- 46: Percentage drop in profits at Target in the last quarter of 2013
- 0: The number of people in Chief Information Security Officer or Chief Security Officer jobs at Target when the breach happened.

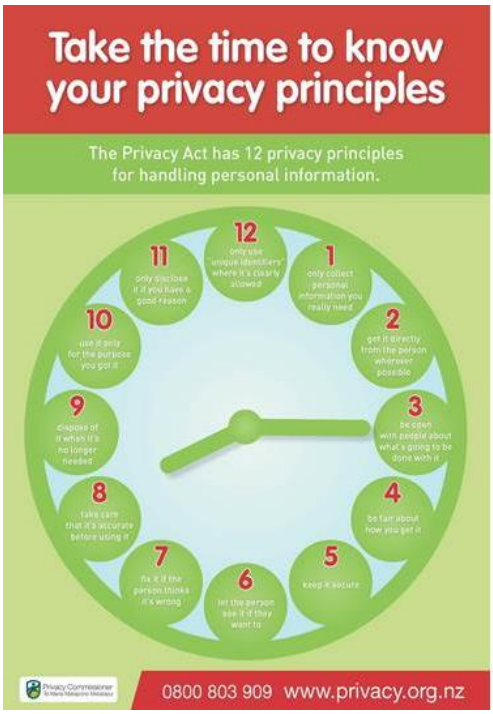
Privacy is not all about security standards and breaches. The Target data breach is a worse case type-of-scenario but it's a good lesson for regulators like me to illustrate the importance of being careful with personal information.

The collection and handling personal information to enhance customer profiles for marketing purposes also raise a number of privacy-related questions.

Ask yourself:

- Where does the information come from?
- Is it publicly available information?
- Is your organisation a 'third party' in using the information? In other words, was the information collected by another organisation?
- Has the information about individuals been de-identified or 'washed'?
- Will the information be matched and combined with other third party data about the same individual to develop a more detailed profile of that individual?
- Are you careful with information that is not personal information at the time of collection but which may become personal information when combined with other data? For example - the collection of IP addresses on free public Wi-Fi can identify people when combined with names and email addresses used to log in to the Wi-Fi network.

I urge you to use the information privacy principles of the Privacy Act as a way of measuring your practices against people's privacy – especially in terms of the collection, use, storage and disclosure of personal information.



I've several case note examples, which while they are nowhere near the scale of the Target debacle, may be helpful to you by demonstrating how my office applies the information privacy principles when we tackle the complaints we receive.

Case Note 1:

A man who was a member of a club complained to us that the club supplied his personal details to a direct mailing company and as a result he received unsolicited direct mail from insurance companies.

The man said he did not know that his personal information would be used in this way when the information was collected from him. He was unhappy about the way his information had been used and that his personal information had been disclosed to a third party.

His complaint raised issues under principles 3 and 11 of the Privacy Act.

Principle 3 concerns the collection of personal information from individuals. It requires an agency to notify individuals of the purpose for collecting the information, and the intended recipients of the information, among other things.

The complaint was made in 2008 but it seems that at its AGM in 1984, the club had decided to give members contact information to an independent direct mailing company for the purpose of providing targeted advertising material to its members.

The club had advised its members of this change through its newsletter and they continued to provide this advice to their members in the years that followed. Since the club had advised its members clearly that contact details would be disclosed, it was our opinion that there was no breach of principle 3 of the Privacy Act.

Principle 11 states that an agency that holds personal information shall not disclose that information.

The disclosure is one of the purposes in connection with which the information was obtained, or directly related to the purposes in connection with which the information was obtained or one of the other exceptions applies.

It was apparent that since the AGM in 1984, giving the information to the direct mailing company was one of the purposes for collecting the information. We concluded that there was no interference with the man's privacy.

Case Note 2:

A woman requested a copy of the responses she had given to a market research company as part of a phone survey.

The research company provided her with a copy of the factual responses she had given, including her age, gender, and location. But it refused to provide her with a copy of the remainder of her responses on the basis that the opinions she had given were not personal information about her.

The woman then made a complaint to us that the company had refused to provide all of the information she had requested.

Under principle 6, individuals have a right to request access to personal information held about them by an agency. Under the Privacy Act, 'personal information' is defined as information about an identifiable individual.

It was our view that the responses the woman had given during the phone survey, including her opinions on a number of subjects, constituted personal information about her, and as such she was entitled to a copy of the record of the survey.

We contacted the research company and advised it of our view. Based on this, the company agreed to provide the woman with a copy of the record of the phone survey, which included her responses. The woman was satisfied with the information that was provided and we closed our investigation.

Case Note 3:

A couple were on the mailing list for a real estate company. They requested that their names be removed from this list and the company said it had done so. The couple then received a letter from the company in relation to a property it had listed.

We investigated this complaint under principle 7 of the Privacy Act. Principle 7 says that individuals can ask for personal information about them to be corrected.

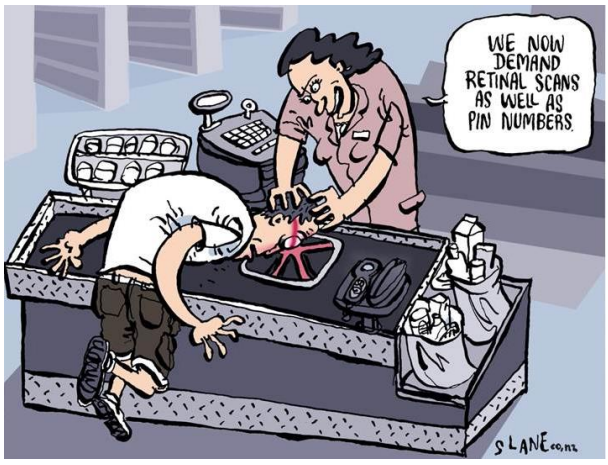
The real estate company said that it gathered information for its mailing database through another company. This company gathered information from publicly available sources such as Quotable Value NZ and newspaper advertising.

The real estate company said it had removed the couple's name from its internal database, but had failed to inform the other company of the couple's request. The real estate company gave the couple the contact details for the other company and suggested they write to it directly and ask to be removed from its database. They were willing to do this.

We were satisfied the real estate company had removed the couple's names from its internal database as they had requested.

We also provided the couple with contact details for the New Zealand Marketing Association which operates a Do Not Call list for personal home contact details. The couple were happy with the result and we closed the file.

Recognising the limits of information



In each of these cases, the one common theme is customer alienation. That's the obvious conclusion because all three resulted in complaints to my office. Customer alienation is an important factor in how you find a balance between inaccurate broad spectrum marketing, like email spam, and targeted marketing that becomes so accurate that people complain about it being too creepy and intrusive.

It is also important to recognise the limits of big data. As data sets increase and grow, thanks to the multiplying capacity of computers to collect and interpret data, there are very real dangers that you could be making the wrong assumptions about your potential customers.

Predictive analysis is not fool proof and the use of big data can lead to over-confidence, leading to mistakes. That's because personal information needs to be updated and corrected frequently because it becomes obsolete very quickly.

Make sure you audit your lists for quality and use the services of trusted and responsible marketing advisers.

You might also want to consider adding privacy to the value of your brand. If you let your customers know that you protect and use personal information about them to the highest of privacy standards, it can only help you gain the trust and confidence of your customers, and attract more.

The Marketing Association's has made positive steps by establishing a Code of Practice for direct marketing and telemarketing. The association also has a Do Not Call register and its Data Warranty Register. Consumers want confidence that organisations will treat their personal information with respect for their privacy. Industry self regulation is a crucial part of any regulatory framework but for it to work well, all marketing practitioners need to be aware of their responsibilities and obligations. Otherwise, external regulation and enforcement will have a bigger role to play in improving universal compliance.

Control

Think also about putting the power of choice in the hands of the customers. Let them decide whether they want to "opt in" to your marketing and advertising. Opt in is a more privacy friendly strategy which would be more likely to bring a "buy in".

Consider the alternative. Why should consumers have to bear the burden of refusal? It sets up a potentially negative engagement with an existing or potential customer right from the start and makes them more inclined to reject the product or service. Isn't marketing about giving consumers more choice?

As I mentioned in the earlier quote by Danah Boyd, people want to feel like they have personal control over their information. So why not give them that choice?

More teeth for the Privacy Commissioner

You may be aware that the Privacy Act has been reviewed by the Law Commission which has made comprehensive and well-founded recommendations on changing the 20-year-old law and bringing it up-to-date.

Most of those changes are now being included in draft legislation that is likely to go before Parliament

next year. One of the proposed changes is to give my Office the authority to order that information be given to people. This is a very significant one because over 60 percent of the complaints that come to my office deal with requests for access.

This is not a "nice to have" for individuals; it's a "have to have". Providing access is a key part of your business, a key part of the relationship you have with your clients - not some legal compliance exercise.

Another significant change on the horizon is a shift to mandatory breach notification. The Privacy Commissioner currently depends on voluntary breach notification and on the willingness of agencies to alert us if there's been a data breach.

We have started to track breach notifications more formally because this is a matter of external interest and importance. There has been a noticeable pick up in compliance in the business sector, particularly among large businesses.

The change to mandatory breach notification will bring us in line with many other jurisdictions with well developed privacy protection laws. New Zealand has been lagging internationally by having a voluntary system.

Under the proposed changes, actions such as failing to notify me of a privacy breach or impersonating someone to obtain their personal information will be an offence and will 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.

My office will also provide more guidance about how to comply with privacy laws and technical improvements to the Privacy Act will make it clearer and easier to understand.

And in rounding up, I want to highlight a couple of new guidance resources we've produced which may be of interest to you.

Our *Data Safety Toolkit* is a free online resource on preventing and dealing with data breaches. This is available on our website, as is our *Need to Have or Nice to Know* guidance for mobile app developers and businesses on their responsibilities under the Privacy Act when designing new apps.

Both are available at www.privacy.org.nz.

Thank you.