Auckland University
MBA and Exec MBA

Marie Shroff, Privacy Commissioner
21 and 22 February 2013

1. Introduction

- Pleased to have the chance to be here.
- Hope that I can give an insight into some of the connections between information law, technology and business – and how things are changing as more and more of our life is lived online.
- Hope too, that my reflections may resonate with you – interested to hear your insight and experience. Am aware that some of you are working in manufacturing, engineering; construction. Even in those areas – still have staff / employee information; still have information security issues. Others of you will be working more directly with personal information – in health; HR; marketing.
- One point to take away? **Information is a strategic asset for your business.**
- Upshot of that? Value it; protect it; manage it.
- Security is a business issue – not just an IT issue. Don't silo it - Do so at your peril. (Telecom/xtra / Yahoo example of that.)
- Data security – biggest concern for corporate counsel (from large US survey – Wigley article). Key points? It's a governance issue – and not something to "set-and-forget" with the techies.
- And data management is now a reputational issue. It's part of your shop front, your branding.
- Privacy is now a "need to know" regulatory and customer relations area for every business person. No easy answers or checklist – you need to understand the main features of this fast-changing landscape.
- So, against that context, wanted to give you a brief outline of my role; talk about some of the wider societal and technological changes that are shaping that role and our online identities; legal and other responses – what, if any, controls do we want and need?

What's privacy anyhow? Privacy in brief

- A basic starting point – and you may already know this: - Privacy law is concerned with information that is about a person – or can be connected to a person. (Called "personal information"). Privacy Commissioner cannot look at the use of company or official information, only information about an identifiable individual – a natural person.

- Privacy commissioners exist in most developed countries – and are often, alternatively, called 'data protection commissions' or similar. Expanding world wide. Will it be the 21st century human right?

In New Zealand – my role and functions are set out in a general way in the Privacy Act. It's a wide-ranging role - some key things:

- Independent of government. Cover both public and private sectors (but not media, courts, Parliament).
- Watchdog role – and that involves various aspects:
- Free to comment publicly about any concerns I might have about the way business or government is handling people's information.
- Have a big policy role – and comment on draft legislation, both before and as it goes through Parliament.
- I'm also a regulator – power to make industry codes of practice, eg. telecoms, health, credit reporting.
- Receive and investigate complaints (about 1,000/year) from the public.
- Freephone line service for public, business – 6/8,000 enquiries per annum
- Monitor new and changing technology.
- Also, have a significant role to communicate and educate about personal information handling (talks like today; case notes; guidance material etc).
- It's a much bigger job than I first imagined – and, because of technological change – a fast developing role.

2. Painting the digital data picture – our information revolution

In the midst of huge technological, cultural and social change. The way information about me – and you – is being collected, stored and sold, shared and re-bundled is profound. Our access to information sources is vast – and historically unparalleled.

"Big Data"

- Umbrella term that is being used to describe these developments – the age of "Big data".
- "Data analytics is becoming a driver of business innovation." (Brendan Lynch, Chief Privacy Officer at Microsoft).

There are various aspects to these changes:

- **Quantity** of information is huge – eg. the human genome has now been mapped. Think of the vast information about each of us that might be unravelled. Think of the numerous companies and government agencies that hold data about you.
- **Ease** of access – we can find detailed information with a few taps of the keyboard / Google search. What might have taken a half-day of searching through hard copies is now accessible, online, to the world in a few seconds.

- **Sensitivity** of the data – there is simply more new information being created today, eg. think of the sensitivity of DNA testing, which means that DNA information can be gathered from sweat left behind at the scene of a crime.

- **Personalised** – eg. think about your search record on Google; maybe your Facebook page.

- **Processing** of information - the suggestion is that having easy access to data is even influencing the way humans process information: - "Digital native" characteristics include: a preference for receiving information quickly – from many sources; multi-tasking; liking to network with others; liking to learn things "just in time."
- (Source:http://women.timesonline.co.uk/tol/life_and_style/women/families/article4295414.ece?)

So what does that really mean for you as an individual and a digital citizen?

- Against that context, we are all "digital citizens" and have to take some personal responsibility for our actions in that sphere. Life is online. We have dual responsibilities – citizens in the "real" world as well as online.

- What might that involve? Digital literacy and ethics – even morals. What you do online does have consequences.

- In relation to your identity – think about your online image and how you manage that.

- And that includes how your personal identity is being mined for cash – growth of data analytics – is it a case of 'you are what you buy'?

- But you're also part of the digital data picture: social networking, blogging, buying and banking online.

- And information about you is out there, online and being shared by others.

- **Your information has become a commodity** – with real monetary value; that is traded, sold and shared.

- Your online identity data is monetised through targeted advertising. The more you tell Google, Facebook etc, the better it is for their balance sheets.

- And for that reason, there is great pressure to create and maintain a single online "real" identity - particularly for social networking. Mark Zuckerberg has said it lacks "integrity" to have more than one online identity.

- Google's recent policy changes - remember: you're not Google's client, you're Google's product!

So what does that really mean for you in business?

- As an employer or business person, you have many options in today's marketplace. Technology is at your fingertips:
  - Keystroke monitoring
  - Drug-testing of employees
  - Monitoring of employee email / social networking
  - CCTV within the workplace / retail environment
  - Remote tracking of employees (haulage companies; couriers)
  - Biometric testing of employees: finger-printing; iris scanning
  - Auditing employee 'browsing" of client databases
  - Use and security of BYOD in the workplace (what are your company policies on that?)
  - Cloud computing more generally

- Don't have the time today to go into the specifics of these, and other, employment issues. But can draw your attention to few things:
  - You have legal obligations to be a fair employer; to communicate with your staff;
  - Legal obligations to take reasonable security measures to protect the information you are collecting.
  - You can only lawfully collect information that is necessary for your business purposes;
  - You have obligations to give notice to customers / employees about things like CCTV use:

    Example:

    As part of an employment investigation, an employer collected personal information from a man's work computer. The information collected included emails sent to and from the work computer, as well as key stroke logs for the computer.

    The employer used information collected from key stroke logging to access the man's personal web-based email account and copy several emails.

    Two separate issues:

    Information collected directly from the work computer
    Collecting the information directly from the work computer complied with the Privacy Act. This was because in both the employment agreement and employee manual the employer had clearly set out that work computers would be subject to monitoring.
    However, we thought the collection of key stroke information raised issues under principle 3 of the Privacy Act.

The policies set out in the agreement and manual were not explicit enough about that.

Information collected from the personal email account
Using the password it obtained from key stroke information, the employer accessed the man's personal email account.

Principle 1 – lawful purpose
When the employer accessed the man's personal email account, it was able to obtain information in relation to a significant number of emails sent over a period of several years.

We formed the view that the employer had breached principle 1, because the collection was unnecessary and disproportionate to the employer's needs.

Principle 3 - notification
The employer's policies were not explicit enough to make an employee aware that if they entered a password into the computer, the employer would be able to use this information to collect further information not held on the work computer.

Principle 4 – manner of collection
Principle 4 requires that personal information must not be collected by unlawful means, or means which, given the circumstances, are unfair or unreasonably intrusive.

An individual's personal email account attracts a high expectation of privacy and it would require exceptional circumstances to justify an employer directly accessing it.

We did not find that there were exceptional circumstances here, and so there was a breach of principle 4.

Outcome: The man and his employer attended mediation, were able to reach a settlement.

- **One thing to remember:** the privacy law is not “black-letter” law – it is a principles-based law (12 key principles). Why? In recognition of the fact that the law shouldn’t be tying the hand of a business / other organisation too much. Aim is to give people discretion to act as they need – within broad parameters.

- But, you can’t abuse that: need to be fair; ethical; transparent. Need to take reasonable security measures, etc. The law in this area is predicated on an expectation of fair business behaviour. If we come to investigate a complaint that is the approach we will look for.

- Apart from technology-related scenarios, there are perennial questions around appointment processes; information on other job applicants (recent Massey University - Wrigley decision); and reference checking.

- And here's an underutilised right: we all have the legal right to have access to information held about us. Your customers might come asking from time to time.

- **Example:**

  A man asked his bank for copies of loan documents that had been completed by his former wife. The loans had been taken out using a house owned jointly by the man and his former wife as security, but without the man's knowledge or agreement.

  The bank initially refused to provide the loan documents on the basis that they were not 'personal information' about the man.

  *After looking at the documents, it was our view that the loan documents were in fact personal information about **both** the man and his former wife, and that the man should be enabled to access them.*

- **Example:**

  Christchurch earthquake – requests to EQC for property valuation information. Upshot? Valuations had to be released.

  Privacy at Work – a guide that covers most of these areas and is freely available online: www.privacy.org.nz (Also contains case examples. More case notes available on our website.)

  Requirement for privacy officers.
  OPC helpline: 0800 803 909; enquiries@privacy.org.nz

Global information flows

- Information now moves freely on a global scale. Smaller countries like New Zealand are inevitably 'takers' of global technology and services from big players such as Microsoft, Facebook and Google. We need to be a part of international moves to protect our consumer data in the global digital world – and to give a level playing field for business.

  Outline two aspects that may affect you in business:

  (1) Cloud computing
  (2) EU Adequacy

Cloud computing

- **Starting point:** if a business operating in NZ holds personal information, it needs to comply with the (NZ) Privacy Act.

- **Why does privacy matter when your data is in the cloud?** Whether personal information is held on in-house computers; in a shared datacentre in New Zealand, or offshore, you've still got legal obligations to protect it.

- **Impact of using a cloud provider?** With cloud providers, there is a third-party relationship to manage, and that can be more challenging if they are based overseas. Clients trust businesses to have things sorted – and a loss of trust is very likely a loss of business.

- **What does cloud mean for New Zealanders?** Your information increasingly does not stay in New Zealand. As individuals, we send our own information offshore all the time – for example when we buy goods, use smartphones or social media. And our government and businesses also act internationally as well as locally.

- **The cloud is not inherently bad or good**. It's just different and requires people to think differently about IT than they have in the past. The bottom line is – work out where your information is going and who's got their hands on it – and make sure whatever arrangements you use stand up when assessed against NZ legal standards.

- **Our survey** (2011) showed that many agencies don't let individuals know they are sending their personal information, so people frequently have no idea their information is being stored or processed overseas.

- **New developments in this area:** The Institute of IT Professionals (IITP [formerly NZ Computer Society]) has led work on developing a voluntary industry code of practice: the Cloud Computing Code of Practice. This is for cloud providers operating in NZ, and is essentially a list of things that cloud providers should be telling their customers. The IITP code is also expected to be launched in early 2013.

- IITP code complements our own cloud guidance for SMEs, which was released on 12 February, and gives people a checklist of questions to ask, and guidance on what to look out for (available at www.privacy.org.nz)

Business opportunities: EU adequacy

- Recently, thanks to work by OPC, NZ attained "EU Adequacy". What does this mean? The European Commission has formally recognised NZ's Privacy Act as offering an adequate standard of data protection for the purposes of EU law.

- Establishes NZ, in the eyes of our trading partners, as a safe place to process personal information.

- Why does this matter? Few countries outside Europe have achieved that status.

- Practical effect? Helpful to NZ businesses that trade with Europe. Expect that is will open up opportunities for more data processing here. **Example:** have spoken to SME IT owner who lost a contract through NZ law not being deemed "adequate" at the time.

- Also signifies a step towards consistent privacy laws throughout the world, creating a trustworthy platform internationally from which to trade.

3. Regulatory responses

So, against this fast changing landscape, from a regulator's perspective, the question becomes two-fold: Do you want or need to regulate this? and if so,
How on earth do you do it?

What are you trying to solve?

- Are you trying to curb individual anti-social behaviour?
- Or is it because you want to trim the wings of hungry multi-national companies?
- Or, alternatively, should we just let people figure things out for themselves – and maybe get their fingers (and wallets!) burnt in the process.

And what tools can you use?

- Privacy law reform – filling some regulatory gaps
- International cooperation – filling some of the jurisdictional gaps
- Industry developments and self-regulation

Privacy law reform – Law Commission Privacy review – filling some of the regulatory gaps

- Law Commission major 4 ½ year project – particularly assessing the impact of technology changes for privacy.
- Found NZ privacy law to be flexible and technology-neutral.
- But found that new risks have emerged from the way today's businesses use personal information.

Recommendations – essentially – you need some new tools.

- Compliance notices to be issued to stop a business or government agency continuing to flout the law (similar to Resource Mgmt Act enforcement notice);
- Streamlining privacy complaint processes;
- Privacy Commissioner should be able to direct a business or organisation to release information;
- Better processes to tackle systemic problems that affect many people, eg. group or "class action" complaints;
- Narrow the "domestic affairs" exemption in the Privacy Act to better protect people from publication of offensive or harmful material online;
- Regulating surveillance, interception and electronic tracking through a new **Surveillance Devices Act**;
- Making companies in New Zealand more clearly accountable if sending information off-shore;
- Currently Privacy Commissioner can't investigate actions of a business based offshore: eg Google, Facebook. So increasingly there are moves to coordinate regulatory efforts internationally. Example: ***GPEN – Global Privacy Enforcement Network -*** Effectively operates as a referral system. Relies on cooperation between regulators. eg. in the US, the Federal Trade Commission.

4. Concluding Comments

- OPC on Twitter and Facebook.

- Has the data-driven economy yet reached its fullest bloom? All our indications would have to say 'no'. 'The data-centred economy is just nascent' (Craig Mundie, head of research and strategy at Microsoft).

- Regulatory developments aplenty. Emerging trends of co-regulation. Industry initiatives (IITP cloud code; OPC Cloud guidance). Lots of international cooperation.

- Business is now in a time where **the way you manage your data is a reputational issue.** A shop-front issue. Need to manage your risk in these areas.

- And at the individual level - Digital citizenship needed – personal control and responsibility.

- "To err is human, but to really foul things up you need a computer." (Ehrlich)

- "It takes less time to do a thing right than explain why did it wrong." (Longfellow)

EXTRA MATERIAL

LAW COMMISSION RECOMMENDATIONS

Overall? NZ privacy law is flexible and technology-neutral. The review endorsed that approach. But the Law Commission has also recognised that new risks have emerged from the way today's businesses use personal information.

Technology change has thrown down some challenges – particularly when it comes to keeping confidential data secure. Businesses are now well aware information is a valuable asset to be protected. Personal information is at the heart of many new business opportunities, so getting the fundamentals right is important.

Key recommendations include:

- Requiring that people be notified of serious security breaches, so that they can take steps to protect themselves;
- Enabling compliance notices to be issued to stop a business or government agency continuing to flout the law (similar to Resource Mgmt Act enforcement notice);
- A national "Do Not Call" register to put a stop to unwanted telemarketing;
- Regulating surveillance, interception and electronic tracking through a new **Surveillance Devices Act**.;
- Streamlining privacy complaint processes to get fast results;
- The Privacy Commissioner could direct an agency to release the information that they cannot legally withhold;
- Better processes to tackle systemic problems that affect many people, for instance by using group or "class action" complaints;
- Narrowing the "domestic affairs" exemption in the Privacy Act to better protect people from publication of offensive or harmful material online;
- Making companies in New Zealand more clearly accountable if sending information off-shore;
- Better regulating the way personal information is shared between government agencies through approved information sharing programmes.

Overall effect? - Law Commission recommends modern tools to fix modern problems. Proposed package of reforms:

  - creates a modern and effective privacy law
  - has targeted changes
  - introduces opportunity for efficiencies in the current dispute resolution system.
- Next steps – Government response (soon!) – and hopefully, putting some changes into law.

Recent privacy related developments and media stories

Media trends

Our media enquiries are a good reflection of where things are at for us. We get about 200-300 calls from media each year. The vast majority of those are technology related. To give you a picture – the sort of enquiries we got in the last year included:

- Telecom – Yahoo/xtra hacking incident – February 2013
- ACC data breach – spreadsheet listing details of 6,000 ACC claimants emailed to a client
- MSD security breach – member of public accessed MSD's server at WINZ job seeker kiosk
- IRD breach – release of personal details of clients to another client by post
- Corrections breach: ex-inmate posted muster sheet on Facebook
- WINZ employee browsing – to help family and friends find jobs
- Immigration employee browsing – using confidential client database "like a dating site" and looking at information on wealthy and interesting clients "just for fun"
- Kim Dotcom surveillance by GCSB
- LC's recommendations to give the PC more powers
- Privacy Commission's Annual report – complaint numbers
- Sharing information with third parties – elderly man filled out PO redirection form forgot to tick the "don't pass on my details box" then started getting marketing material posted to him
- Google – new privacy policy
- Google – destruction of Google's WiFi payload data
- Facebook – can employers check profiles
- Facebook – graph search
- IT trends in healthcare – privacy issues GPs need to be aware of
- Cloud computing – industry code of practice initiative / risks to Government?
- KPMG report on global hacking and data loss figures
- Cyber stalking apps on cell phones – NZ's situation
- Phone app so parents can spy on kids (Life360)
- Drones – concerns about their use
- Auckland bars using ID scanners
- Terralink 3D street filming – privacy implications
- Automatic number plate recognition technology
- Facial recognition CCTV – is it being used in NZ?
- CCTV being installed in school and restaurant toilets – is this legal?
- Banks releasing information to Police without warrant in suspected money laundering case
- District Councils selling personal information from building consent applications to third parties
- Brendan Horan – phone leaks
- Kate Middleton in hospital - privacy breach/Australian radio prank

Google's 2012 privacy policy changes

Privacy Commissioner's comment:

"Google's aim of making their privacy policies simpler and clearer is a move in the right direction. We have encouraged Google to go down that track and have said how important it is for privacy policies to be readily understandable and as clear as possible. If these changes do that, then that is a good thing for Google users.

Google's plans for increased linkages in user identity data across Google products and services to provide a seamless user experience do raise concerns and it means the ground is shifting for Google account holders.

Users need to be aware that Google's business model relies on being able to deliver targeted advertising and that user demographic data provides the raw fuel. That exists under the current model and is extended by the new plans.

Google account holders might want to look again at their privacy settings in tools like Google Dashboard and change those if they want more privacy. Some users may choose to create pseudonymous, separate, online profiles. I will continue to keep track of these changes and the impact that they may have on user privacy.

For people who don't have Google accounts (eg Google+, Reader, Gmail etc) there is probably little difference."

Cloud computing survey – May 2011

- Information is global – and passes instantaneously across national or state boundaries. As you well know, the law doesn't work that way!
- Carried out a survey of the way businesses and government agencies were using offshore information and communication technologies services.
- Found that both the private and public sectors need guidance in this area. While most of the organisations have controls to protect the security of personal information in transit, some have no control over what happens once the information is sent overseas or don't know if they have controls.
- Survey will help us to develop guidance on how to mitigate ICT risks that will enable businesses and government agencies to get the most out of cloud services.
- If New Zealand businesses and government agencies are going to take advantage of the benefits the cloud can offer, it is imperative that privacy issues are tackled and got right.

Public opinion poll - Key points:

- We regularly commission public opinion surveys to get an idea of how attitudes to privacy are developing. April 2012 latest. Pretty consistent results over the years.

- General concern about privacy has risen to 67% in 2012, up from 47% when first measured in 2001.

- Overall, 54% of respondents surveyed said they used a social networking site - compared with 43% in 2012, 32% in 2009 and just 14% in 2007.

- 88% of those under 30 used social networking; 20% of over 60's.

- But - surprisingly, ***more than half of users (55%) believed social networking sites were mainly private spaces*** where people shared information with their friends.

- Information that children put on the internet about themselves is the privacy issue that most worries New Zealanders. Eighty-four (84) percent of people surveyed said they were concerned about the issue, including 73% who said they were "very concerned".

- A new and somewhat surprising finding was 88% of people are concerned that businesses should tell them how they use pi; and that business should be punished if they misuse pi; 97% felt PC should be able to stop breaches of PA.

MORE DETAIL ON LC PROPOSALS

LC – proposed new power: Compliance Notice

- **New power** - The Law Commission has put forward the low-cost, low-resource suggestion of a **compliance notice** to target those agencies that persistently flout the law.
- Privacy Commissioner could order agencies to fix business practices that breach the law.
- Targeted tool - would address those rare occasions when no other solution has worked and people are at risk of harm from misused information or inadequate business practices.
- **Why needed?** Some agencies may poorly protect, unwisely disclose or even exploit or on-sell individual information.
- **Example?**: Professional man who refused to take content down from his website that named young women who had made allegations of sexual abuse against him – in his professional capacity.
- **Effect:** We could fix problems quickly, and protect people's personal details from loss or misuse;

LC – Privacy Breach Notification

- Reality is that occasionally things do go wrong and personal data is lost or hacked into. At the moment, people are not necessarily told, and so are put at risk of identity theft or other harms.
- Voluntary scheme in place at the moment.
- **Proposal** – The voluntary scheme would become mandatory so that people would be told when there was a serious data breach that affected them – so that they could take steps to protect themselves, like cancelling a credit card. Recommendation is for a "risk-based" approach, to avoid notification overload.
- **Eg.?** Sony breach as it affected NZers; bank sends bank statement to estranged partner.

LC – Class Actions to Tackle Systemic Harm

- **Proposal -** groups of people would be able to bring "class actions" / representative complaints.
- This recommendation reflects the reality of many privacy breaches nowadays.
- We see plenty of instances, such the Sony Playstation customer data breach recently, when one systemic problem affects thousands of people.

LC – Faster Dispute Resolution

- **Major changes** (2) to privacy dispute resolution proposed
- Privacy Commissioner could **determine access complaints** (where a person seeks their own information), and would be able to direct an agency to release the information. Effect: Quicker, streamlined dispute resolution. Appeal through the HRRT.
- **Role of Director of Human Rights Proceedings (DHRP) abolished -** OPC would be able to take cases directly to the Human Rights Review Tribunal to hear all types of privacy complaints.
- Also proposed that businesses could refuse a request if the same information had already been released to the requester.

LC – Cross-border

- Internationally New Zealand business has opportunities in technology and data processing – partly due to our time zone, and developments in 'cloud computing'.
- Recommendations would bring our law up to date with international best practice, and would enable NZ to opt into the APEC cross-border privacy rules in the future.
- Clearer rules would mean businesses sending data overseas could be certain where responsibility for the information would lie.

LC – Closing off Offensive Internet Postings

- **Closing legal loopholes -** loophole at the moment around the publication of highly offensive material online. New proposal would mean in future people could complain and potentially get offensive material taken down from the internet.
- We know of cases where people have posted intimate photographs of former partners online, for instance, and as the law currently stand there is very little we can do about that.

New media review

The Law Commission has also recently stepped up its efforts to review a particular aspect of privacy in New Zealand – the regulation of the news media in the new digital era. The Commission is looking specifically at:

- The definition of "news media": what should fall outside this definition? Blogs?

- The jurisdiction of the BSA and the Press Council. If the Privacy Act does not cover new media, should the BSA or PC?

- The adequacy of existing criminal and civil remedies for wrongs such as defamation, harassment or breach of confidence.