Privacy Commissioner John Edwards' speech to the In-House Lawyers Association (ILANZ)

on Thursday 17 May 2018 in Hamilton

to In-house counsel for public and private organisations

Introduction

- The theme of this conference – "No. 8 Wire" – encourages creativity, innovation and reinvention.
- Both the current Privacy Act and the new Bill are enabling pieces of legislation – there is room for flexibility and creativity
- But you must be aware of the privacy risks – laws are about to change, and recent litigation has made some risks much clearer

Law reform

- Privacy Bill is now before select committee.
- Select committee submissions from my office
- But your input is important – keep compliance costs down, prevent the erosion of privacy rights, help create a Privacy Act that is good for the challenges of the next 25 years.
- Submissions close 24 May

Privacy Act 1993

- Privacy Act is now 25 years old - passed by Parliament on 5 May 1993.
- At the time, the first national information privacy law outside Europe to apply to both the public and private sectors.
- It did not, as some had predicted, paralyse business or curtail the news media in reporting news.
- Gave New Zealanders the right to access their own medical records outside the public health system.
- Enabled New Zealanders to seek the correction of information held on credit reporting agencies' files, if it happened to be inaccurate or wrong.

- New Zealanders also given the right to access information about them on their employer's personnel files – only a right for public sector employees at the time.
- The Act gave people a clear avenue for a privacy complaint.
- The Privacy Commissioner provided a simple mechanism with an ombudsman-like investigation into complaints and a non-adversarial approach.

Years in between

- Privacy Act – from world leading to behind the times.
- Two significant reviews:
    - Necessary and Desirable – Privacy Act 1993 Review by Assistant Privacy Commissioner Blair Stewart in 1998.
    - Law Commission 2011 review – completed a major review of the Privacy Act which began in 2006.
- Delays in adopting Law Commission recommendations meant Act fell further behind overseas trends.
- Section 26 report to Government in 2017 intended to introduce further changes beyond those made by the Law Commission.
- Six years since Law Commission report mean new developments in technology and privacy and data protection regulation have yet to be reflected in the Bill.
- Developments in the interim - rapid changes in information and digital technology, data science, and changes in international data protection frameworks.
- Reflect on Edward Snowdon's revelations, the right to be forgotten, artificial intelligence, predictive risk modelling, algorithmic transparency, smart phones, Internet of Things, mobile apps, GDPR, drones, and now, Cambridge Analytica data mining.

Current Privacy Bill

What are the key changes in the Privacy Bill?

- Mandatory data breach notification – an agency must notify my office of privacy breaches (defined as unauthorised or accidental access to, or disclosure of, personal information) that pose a risk of harm to people, and to affected individuals.
- Compliance notices – I will be able to issue compliance notices that require an agency to do something, or stop doing something, in order to comply with the law.
- New criminal offences – it will be an offence to mislead an agency in a way that affects someone else's information and to knowingly destroy documents containing personal information where a request has been made for it. The penalty is a fine up to $10,000.

- Binding decisions on access requests – and I will be able to make decisions on complaints relating to access to information, rather than the Human Rights Review Tribunal.

Section 26 recommendations

In 2017, I proposed six new recommendations to the Privacy Bill. These are:

- Penalty Power - empowering the Commissioner to apply to the High Court for a civil fines to be imposed in cases of serious breaches (up to $100,000 for an individual and up to $1 million for a body corporate)
- Accountability - a power to require an agency to demonstrate its ongoing compliance with the Act
- Portability - introducing data portability as a consumer right.
- In addition:
    - Protection against the risk that individuals can be unexpectedly identified from data that had been purportedly anonymised;
    - Narrowing the defences available to agencies that obstruct the Commissioner or fail to comply with a lawful requirement of the Commissioner
    - Reforming the public register principles in the Act and providing for the suppression of personal information in public registers where there is a safety risk.

GDPR

- This brings us to Europe, where the GDPR is set to introduce much stronger privacy and personal data protections
- The European Union's General Data Protection Regulation (GDPR) is a data protection framework that requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states:
    - Adopted by the European Parliament in April 2016
    - Takes effect on 25 May 2018
    - Provisions are consistent across all 28 EU member states
    - It means all companies doing business in the EU have just one standard to meet
    - A harmonisation of disparate data protection and privacy laws and regulations across the region
- GDPR defines several roles that are responsible for ensuring compliance

  - data controller
  - data processor
  - data protection officer
- Some of the features of the GDPR are in New Zealand's Privacy Bill, but not all

What types of data does the GDPR protect?

The GDPR protects all personal information, including;

- Basic identity information such as name, address and ID numbers
- Web data such as location, IP address, cookie data and RFID tags
- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation

Which types of agencies are covered?

- Any company that stores or processes personal information about EU citizens within EU states must comply with the GDPR, even if they do not have a business presence within the EU
- Specific criteria for companies required to comply are:
  - A presence in an EU country
  - No presence in the EU, but it processes personal data of European residents
  - More than 250 employees
  - Fewer than 250 employees but its data-processing impacts the rights and freedoms of data subjects, is not occasional, or includes certain types of sensitive personal data

How does it affect third-party contractors?

- GDPR places equal liability on data controllers (the organisation that owns the data) and data processors (outside organisations that help manage that data)
- A third-party processor that is not compliant means your organisation is not compliant
- The new regulation also has strict rules for reporting breaches that everyone in the chain must be able to comply with

- More on reporting breaches later

What are the penalties for non-compliance?

- Up to €20 million or 4 percent of global annual turnover - whichever is higher
- Management consulting firm Oliver Wyman predicts the EU could collect as much as $US6 billion in fines and penalties in its first year
- The fines are big news to US businesses – estimates vary but the consensus is that half of the American companies that should be compliant will not be by 25 May
- Commentators are predicting EU regulators will act quickly on a few non-compliant companies to send a message to everyone

So how does the GDPR affect New Zealand?

- We've seen a lot of confusion about how New Zealand businesses will be affected as the build-up to the GDPR comes in
- I think partly the issue is that anxiety is being promoted by people who are talking up the extra territorial elements of the GDPR
- Laws have extra territorial effect only in quite limited circumstances.
- The GDPR says you may be subject to this law if you are effectively operating in Europe
- If you are selling Manuka honey from a website in Northland and somebody in The Netherlands has ordered it and shipped it, and you have their data in your data base, that does not make you subject to the GDPR
- Do you have a base in Europe?
- Are you advertising on your website in European languages?
- These are some of the tests that will be used to indicate whether you also have to comply with that legal framework
- Compliance with the New Zealand Privacy Act takes you quite a long way in terms of the GDPR and keeps you pretty safe
- It doesn't get you all the way - which we can talk about - but I think some elements of that concern about companies around the world having to comply is a bit overstated.

Litigation

R v Alsford [2017] NZSC 42

- In this significant decision, the Supreme Court has clarified the law in relation to **voluntary** requests for personal information by law enforcement agencies
- It also affirms the obligations and responsibilities of both the law enforcement requester and the responding agency
- We've previously found confusion in the private sector about the legal basis for law enforcement agencies to request personal information.
- Alsford presented an opportunity for judicial clarification – I sought and was given leave to intervene in the hearing.
- The decision has been subject to suppression orders until recently.
- Police made requests to three electricity providers for power consumption data from the defendant's properties. All three companies disclosed the information sought under privacy principle 11(e)(i) of the Privacy Act.
- Police's method of collecting the information, and how they then used the information to support production order and search warrant applications, was one of the grounds of appeal.
- The majority of the Supreme Court (4:1) affirmed the Police's ability, in the circumstances and in the absence of a production order, to ask for power consumption information in the form of monthly aggregated data, despite finding that one of the three requests did not provide sufficient information to justify the resulting disclosure.
- That particular disclosure was therefore not justified in terms of principle 11(e) and to that extent; there was a breach of the Privacy Act.
- The decision also affirms that where the Police obtain information from service providers about customers on a **voluntary** basis, they must not infringe section 21 of the New Zealand Bill of Rights Act (the right to be secure against unreasonable search and seizure).

- This case demonstrates the need for better information to be made available to companies and individuals about the circumstances in which personal information can be released and used for law enforcement purposes
- My Office has created a comprehensive suite of resources relating to this issue, including:
    - Guidance for releasing personal information to Police and law enforcement agencies
    - A Transparency Reporting Summary Report and Appendix

Dotcom v Crown Law Office [2018] NZHRRT 7

- In July 2015 Kim Dotcom's lawyers made 52 near-identical requests for personal information urgently as it was required for "pending legal action" (the September 2015 extradition eligibility hearing in the District Court).
- Nearly all the various Crown agencies transferred their requests under s 39 of the Privacy Act to the Attorney-General (in practice the Crown Law Office).
- The Solicitor General responded on the Attorney-General's behalf, declining all the requests under s 29(1)(j) of the Privacy Act on the basis that they:
- were vexatious
- included information that was trivial
- were not genuine and were intended to disrupt the extradition hearing.
- Dotcom complained to my office and we investigated, finding no interference with privacy. Dotcom then went to the Tribunal.
- The Tribunal had to determine whether the transfer of requests to the Attorney-General was legal, and if s 29(1)(j) was a proper basis to decline the request.
- Dotcom firmly denied the allegations in the Crown's refusal letter. The Tribunal was satisfied by his evidence that the requests "were genuine and based on an honest belief that in the unique circumstances of a truly exceptional case".

Transfer issue

- Section 39 of the Act lets an agency can transfer a request if it doesn't hold the information (s 39(b)(i)) or they believe the information is more closely connected with the functions of another agency (s 39(b)(ii)).

- In this case the Crown relied on s 39(b)(ii) to transfer the requests. Crown Law had been leading the Crown's litigation against Dotcom and make a decision and provide a consistent response to the requests.

- The Tribunal found that the transfers were not made in accordance with the Act and the Attorney was not the lawful transferee under s 39(b)(ii). Just because Crown Law was giving legal advice to the agencies doesn't mean the requested information was more closely connected to them.

- Because of this, the Tribunal found that the Attorney had no authority as transferee to refuse to disclose the requested information. Dotcom had established an interference with privacy in terms of s 66(2))b) of the Act – no proper basis for the refusal.

- The Tribunal rejected the Crown's submission that whether transferred or not, the decision was going to be to refuse to release the information.

Whether the requests were vexatious

- The Tribunal also considered whether, if the transfer was lawful, there was a proper basis to decline them as vexatious under s 29(1)(i) of the Act.

- The Tribunal found Dotcom had amply satisfied them that, contrary to the assertion by the Crown, he had no ulterior motive in making the information privacy requests and that these were entirely genuine and not intended to disrupt the extradition hearing.

Remedies

- The Tribunal granted:

- a declaration that there was an interference with Dotcom's privacy

- an order that the Crown agencies now comply with the access requests

- damages of $90,000 ($30,000 of loss of benefit and $60,000 for loss of dignity or injury to feelings).

- Although these were exceptional circumstances, it demonstrates the risks of getting privacy wrong – financial costs and reputational damage

"No. 8 wire"

- All this talk of new laws and litigation is not meant to scare you away from the "No. 8 Wire" mindset
- Once you're aware of the risks and have mitigated them, you can experiment and innovate while handling personal data safely
- If you want to try something new with personal information, do a privacy impact assessment to find out the potential risks
- Recent example from the news; facial recognition technology
- Search "privacy impact assessment" on our website to find our PIA toolkit
- Recently I launched the Privacy Trust Mark.
- The Trust Mark identifies products and services that I consider to be outstanding in the way they manage personal information.
- If you put in the work and take account of privacy values in the design of your product or service, the Trust Mark gives people more confidence to engage with it
- You can find out more about the Trust Mark and how to apply for one on our website.