The role of the Privacy Commissioner – an address by John Edwards

Host organisation: Crown Law / Te Tari Ture o te Karauna

Wed 9 November 2016

Introduction

- The Privacy Act in New Zealand covers “personal information”.
- "Personal information" is any information about an individual - a living natural person - as long as that individual can be identified.
- Personal information is health information, employment records, relationship details, tax status, and biometric information.

Privacy Commissioner’s role

- An independent crown entity, funded from the public purse, but with statutory independence.
- Independent investigation and inquiry functions.
- To comment and advise on policy and legislative proposals.
- Also an important communications function – to educate, inform, advise and send the right signals on relevant and topical privacy issues.
- 300 media enquiries received a year.
- Over 800 privacy complaints received a year.
- Major industry codes of practice – in health, telecommunications and credit reporting.
- Advisory opinions.
- Naming policy.

Interference with privacy

- A breach of principle 6 or 7; or a breach of any of the principles 1 - 5 or principles 8 - 12 that:
    - causes loss, detriment, damage or injury;

- adversely affects rights, benefits, privileges, obligations or interests; or
- results in significant humiliation, loss of dignity or injury to feelings.

Recent privacy-related news issues

- Police checkpoints used to collect information about attendees at a pro-euthanasia meeting – subject to an investigation by IPCA and OPC.
- Joint report into Police Vetting Service by IPCA and OPC.
- Nurses Organisation spear phishing email data breach – 47,000 members
- Education Payroll Ltd / Novopay school data breach
- Manpower collection policy statement – included sexual preference/ethnicity/political views
- Intelligence and Security Bill – OPC submission / PM's view that people had more to fear from Google and Facebook than the NZ intelligence services.

Law reform

- New Privacy Act is likely to give our Office more enforcement powers:
  1. Access determinations – Privacy Commissioner will be able to make access determinations. 60 percent of complaints are about requests for access.
  2. Enforcement notices – Privacy Commissioner to get the power to issue enforcement notices to non-compliant agencies.
  3. Mandatory breach notification – data breaches that are material and serious will have to be reported to the Privacy Commissioner.
- Other areas are being explored – e.g. fines/penalties.

Dispute resolution and investigations

- A modern faster complaints process.
- Online complaints form.
- Use of dispute resolution techniques to resolve complaints, including compulsory conferences.
- OPC closed 827 complaint files last year - an increase from 702 the previous year.

Information Sharing

- Government has signalled its intention for greater information sharing in the public sector to enable its Better Public Services vision.
- For example, a report last year found criminal justice system failings which enabled Phillip John Smith to escape overseas.
- The report's recommendations became a basis for further discussions on how agencies could work more closely together to share necessary information.
- The report said the criminal justice sector information repositories had limited interoperability with each other, and this was a wider public policy issue.
- The report authors found that a situation like Phillip John Smith's arose from multiple failings - departmental caution, ministerial direction, resource limitations, government priorities or various combinations of each.
- OPC priority to engage with government agencies in order to work through current and proposed avenues for improved information sharing.

AISAs

- Approved information sharing agreements are a mechanism in the Privacy Act that allows information sharing between and within government agencies.
- Listed in Schedule 2A of the Act – enacted in February 2013.
- AISAs are one of the recommendations by the Law Commission in its report on reforming the Privacy Act.
- AISAs authorise agencies that are parties to it to share personal information in order to provide a public service specified in the agreement.
- Potential uses include protecting vulnerable children; improving multiple services for youth with complex needs; and making tax and welfare fraud easier to detect.
- AISAs clarify and improve the rules around how agencies share personal information, while ensuring safeguards are in place to protect an individual's privacy.
- Privacy Commissioner has oversight role for AISAs.
- There are currently three AISAs in place:
- Information sharing agreement between IR and DIA.

    - This agreement authorises the disclosure of passport information to Inland Revenue to enable it to make contact with overseas based student loan borrowers and liable parents who are in default of their obligations.
- Information sharing agreement between IR and NZ Police.
    - Authorises the disclosure of information by IR to Police to assist in the reduction the rate of serious criminal offending by tracing criminal proceeds.
- Information sharing agreement for improving public services to vulnerable children.
    - This agreement authorises the disclosure of information by the MSD, Justice, Health and Education and Police for assessing referrals to children's action groups.
- Perceived roadblocks in the AISA process – since 2014, only three have been completed.
- Public sector heads perceive it as a long and arduous process to create an AISA.

Harmful Digital Communications Act

- HDCA makes some changes to the scope of the Privacy Act.
- One change is to close the 'revenge porn' loophole, where complainants' ex-partners could distribute intimate photographs or videos without breaching the Privacy Act.
- Previously, any information gathered during the course of an individual's domestic or family affairs was not covered - section 56 of the Privacy Act.
- HDCA amendment eliminates this exemption in situations where it would be 'highly offensive to an ordinary reasonable person' to collect, use or disclose the information in question.
- Test for OPC is to establish a line as to what objectively qualifies as 'highly offensive'.
- The HDCA also places some new limits on the way publicly available information can be used or disclosed.

- Using or disclosing publicly available information is now limited to circumstances where it would not be unfair or unreasonable to do so.

HRRT privacy decisions

- HRRT is increasing the awards of damages in privacy cases.
- Awards for breaches of the right of access are often around $10,000, increasing to $20,000 where the circumstances are aggravated.
- Equally, awards are lower if the breach is not particularly damaging or substantial.
- A departure from previous awards of approximately $2000 to $5000
- Tribunal appears to be recognising the importance of being able to get access to information and the uncertainty and harm that is caused if the information is not provided.
- Privacy Commissioner's role as the gate keeper to the Tribunal.
- Privacy Act only requires that "investigation has been conducted" into the particular interference with privacy allegation for the aggrieved person to bring proceedings (s 82(1)(a)).
- OPC's threshold for investigating complaints are in sections 69 and 71 of the Act.
- The 'proceeding' provisions are in sections 73-80.
- Note the informality of these processes (i.e. few formal steps) with the focus on settlement and that Commissioner doesn't necessarily issue a decision.
- Section 75 requires only for the Commissioner to inform of the result and that it may be an investigation is not progressed for variety of reasons (although complainants can take their case to Tribunal by themselves).
- Most of the work happens at the Commissioner level - very few cases go to the Tribunal.
- Referrals to the Director of Human Rights Proceedings and number of cases taken to Tribunal each year are a very small percentage of the Office's case load.
- Beyond the Tribunal, there are very few appeals to the High Court, nor other cases involving the interpretation or application of the Privacy Act that reach the general courts.

- This results in the general courts having very little exposure to the Privacy Act and therefore limited knowledge.

Some Tribunal decisions

1. ***Taylor vs Orcon***:
    - $25,000 in damages over a $300 disputed bill passed on to a debt collection agency.
    - Tribunal decision makes it clear agencies must take adequate steps to check the accuracy of the information before referring it to a debt agency.
2. ***Watson vs Capital Coast DHB***
    - $15,000 in damages after the Tribunal decided that an investigation into a workplace harassment complaint failed to follow workplace policies.
    - Complainant had been refused information gathered during the course of the investigation – damages awarded for humiliation, loss of dignity and injury to feeling.
3. ***Hammond vs NZCU Baywide***
    - $168,000 in damages exceeded the previous highest award of $40,000 (Hamilton v The Deanery in 2003).
    - A woman complained after her former employer distributed copies of a photo she posted on Facebook to harm her future employment prospects.
    - It has become the new benchmark for compensating harm caused by a breach of the Privacy Act.
4. ***Tan vs Police***
    - Police disclosed sensitive personal information about the woman's brother to the woman's employer. The brother was a convicted child sex offender.
    - The woman complained to OPC, and subsequently took the case to the Tribunal.
    - Police did not have enough information to obtain a search warrant or a production order so relied on principle 11 to request evidence from the employer.
    - OPC found no breach and the Tribunal agreed.
    - Tribunal said where there was insufficient evidence to obtain a compulsory order, it would be absurd Police would be precluded from using the

Privacy Act because the Act's principles specifically contemplate that a request of this kind would be made by law enforcement agencies.

Higher Courts and the Privacy Act

1. Christopher Harder

- In 2000, the barrister Christopher Harder recorded two conversations with a client's ex-partner, Ms C, without her being aware he was doing so.
- Ms C complained to the Privacy Commissioner, both about the taping, and about the use Mr Harder made of the tapes.
- The issue is whether Mr Harder's conduct in taping the two conversations without Ms C's knowledge, constituted interference with her privacy in terms of s66 of the Privacy Act.
- The Complaints Review Tribunal (now the Human Rights Review Tribunal) brought a claim for damages on behalf of Ms C
- Tribunal held that Mr Harder had been guilty of an interference with her privacy, and awarded her damages of $7,500 pursuant to s88(1)(c) of the Act.
- Mr Harder appealed to the High Court which upheld the Tribunal.
- Mr Harder then appealed to the Court of Appeal on four points of law.
- He did so pursuant to s124(1) of the Human Rights Act 1993 which applies to cases arising under the Privacy Act by dint of s89 of that Act.
- Privacy experts have argued Harder should have taken reasonable steps to warn the woman.
- A majority of the five judges said at the time there was nothing unfair about wanting to make sure the lawyer had an accurate record of the call.

2. Justice Winkelman and Kim Dotcom

- Former Privacy Commissioner Sir Bruce Slane: "Privacy Act is not the right 'pathway' for the courts.
- In 2014, Justice Winkelmann ordered Kim Dotcom to apply under the Privacy Act for his personal information held by journalist David Fisher, who wrote a book about him.
- Mr Fisher had declined to voluntarily hand over the information to the Crown.

- Justice Winkelman required Mr Dotcom to make an access request for his personal information and then to make available the information that would be required by the court.
- Mr Dotcom's personal information was the subject of a case brought by him and others against the Police and the GCSB.
- The judge interpreted the media exemption in the Privacy Act as not applying to Mr Fisher as the author of a book.
- This resulted in calls to widen the Privacy Act exemption to journalists who are authors producing investigative reporting in the form of a book, rather than in a news medium as defined in the Act.

3. Cameron Slater v Nicky Hager

- Investigative journalist Nicky Hager received a hard drive from an unnamed source with a significant amount of personal correspondence to and from blogger Cameron Slater.
- The information was source material for Hager's 2014 book, Dirty Politics.
- Mr Slater made a complaint to my office that the means by which Mr Hager obtained his private emails and published them, breached his privacy.
- In determining whether Mr Hager was 'news media' for the purposes of the publication of a book, my office decided the facts of the complaint were quite different from those in the Dotcom case.
- s14 of the Privacy Act requires that in performing functions under the Act, we have to have due regard for the protection of important human rights and social interests that compete with privacy.
- We decided Dirty Politics was the collection and dissemination of news by a journalist and we had no jurisdiction to consider if it was a breach of the Privacy Act.

4. Roughan vs Prime Minister John Key

- In 2015, NZ Herald journalist John Roughan wrote a book about Prime Minister John Key.
- Lawyers for Bradley Ambrose, the cameraman suing Mr Key for defamation as a result of the "teapot tapes" events, asked the Prime Minister for discovery, including material held by Mr Roughan, his biographer.

- They were asking the PM to exercise his right under the Privacy Act to access personal information about him, so it could be produced to the Court.
- Prime Minister's lawyers obliged and made the request of Mr Roughan who refused on the basis that he was a journalist.
- We had a case that had identical legal issues to Kim Dotcom decision by Justice Winkelmann.
- A journalist working for NZ Herald writes a book about a well known individual who is a party to legal proceedings.
- As a statutory officer faced with a case with identical facts to those directly ruled on by a senior judicial officer, I was bound by that precedent.
- Simply no "wiggle room".

ENDS