University of New South Wales
University of New South Wales Faculty of Law Research Series
2012

Year 2012 *Paper* 4

Privacy Enforcement Strengthens in Australia & New Zealand

Graham Greenleaf* Katrine Evans†

*University of New South Wales, g.greenleaf@unsw.edu.au

†Office of the New Zealand Privacy Commissioner, Katrine.Evans@privacy.org.nz

Privacy Enforcement Strengthens in Australia & New Zealand

Graham Greenleaf and Katrine Evans

Abstract

This article is the first of a series surveying recent Asian and Australasian examples of significant enforcement of data privacy laws. If there are current examples of where privacy laws are achieving significant outcomes in a country, this should make us cautious of the oft-voiced suspicion that 'privacy laws don't achieve anything'. On the other hand, if such examples are lacking, this raises serious questions. The main sources for such examples are court and tribunal decisions, and the databases of complaint summaries, and annual reports, of data protection authorities.

By 'significant examples of privacy enforcement actions' what we mean is as follows. Firstly, the action results from complaints to an independent authority, actions before any Court or Tribunal, or 'own motion' actions by an authority responding to a specific situation. General investigations or reform proposals by authorities are not included. Secondly, the authorities concerned could be Data Protection Authorities (DPAs) or Privacy Commissioners but they could also be telecommunications regulators, financial regulators, government agencies and so on. Independent industry self-regulatory bodies could be included. Thirdly, the result is a significant remedy for an individual or a group of people; or a significant change in (or confimation of) the interpretation of the law with potential remedial benefits; or a significant change in business or government practices.

At present there are well-established data privacy laws covering most aspects of the private sector in nine jurisdictions in Asia and Australasia. This article covers New Zealand and the three Australian jurisdictions. (An article in the next issue will cover the Asian jurisdictions.)

This survey of recent enforcement examples in New Zealand and Australia makes it clear that significant examples of enforcement of privacy laws continue to occur in all four jurisdictions considered, and some examples show the strengthening of particular remedies. However, the mechanisms through which signficant enforcement arises differs a great deal between jurisdictions. In these Australasian examples they include complainant-initiated injunctions, both awards of damages and mediations by Privacy Commissioners, orders by quasi-judicial Tribunals, and suppression orders by Tribunals. One overall factor shared by all four Australia and New Zealand jurisdictions is that payments of financial compensation to complainants are possible and do occur. A comprehensive assessment of enforcement effectiveness would also require statistical information to be considered. Such analysis of enforcement of privacy laws and its effectiveness (covering examples, statistics and mechanisms) is an important aspect of privacy research which is not yet fully developed.

Privacy enforcement strengthens in Australia & New Zealand

Graham Greenleaf and Katrine Evans

Privacy Laws & Business International Report, Issue 115, February 2012

Introduction

This article is the first of a series surveying recent Asian and Australasian examples of significant enforcement of data privacy laws. If there are current examples of where privacy laws are achieving significant outcomes in a country, this should make us cautious of the oft-voiced suspicion that 'privacy laws don't achieve anything'. On the other hand, if such examples are lacking, this raises serious questions. The main sources for such examples are court and tribunal decisions, and the databases of complaint summaries, and annual reports, of data protection authorities. Such an approach should not be confused with an analysis of the overall effectiveness of enforcement regimes in the countries concerned, or the content of their laws. A more comprehensive analysis must also consider statistical evidence of enforcement and outcomes, but this article only looks at examples where the context of the legal issues and the remedies are known.

By 'significant examples of privacy enforcement actions' what we mean is as follows. Firstly, the action results from complaints to an independent authority, actions before any Court or Tribunal, or 'own motion' actions by an authority responding to a specific situation. General investigations or reform proposals by authorities are not included. Secondly, the authorities concerned could be Data Protection Authorities (DPAs) or Privacy Commissioners but they could also be telecommunications regulators, financial regulators, government agencies and so on. Independent industry self-regulatory bodies could be included. Thirdly, the result is a significant remedy for an individual or a group of people; or a significant change in (or confimation of) the interpretation of the law with potential remedial benefits; or a significant change in business or government practices.

At present there are well-established data privacy laws covering most aspects of the private sector in nine jurisdictions in Asia and Australasia (three in Australia, Hong Kong SAR, Macau SAR, Japan, South Korea, Taiwan, and New Zealand). Malaysia also has such a law but it is not yet in force, and the laws in Vietnam and India have only been in force since mid-2011. Thailand has a law only for the public sector. These laws are surveyed by Greenleaf up to October 2011.[1] Other countries have constitutional protections or sectoral laws that also protect privacy. This article covers New Zealand and the three Australian jurisdictions. An article in the next issue will cover the Asian jurisdictions.

New Zealand – Tribunal decisions and complaints

Enforcement action in New Zealand takes several common forms: investigations by the Privacy Commissioner into complaints brought by individuals; judicial decisions from the Human Rights Review Tribunal; and Privacy Commissioner-initiated

[1] Greenleaf, G 'Major Changes in Asia-Pacific Privacy Laws: 2011 Survey', *Privacy Laws & Business International Report*, Issue 113: 1, 5-14, October 2011; also available at <http://ssrn.com/author=57970>

investigations. Examples from 2010/11 are considered here. Investigations by the Privacy Commissioner into complaints can result in negotiated settlements which take many forms, including apologies to the complainant, changes in agency policies and procedures or compensation.[2] The highest compensation settlement achieved by the Commissioner in 2010/11 was $50,000 for a case involving an improper disclosure. This amount was higher than any compensation award made by the Human Rights Review Tribunal. Other results of significant investigations included:

- *Improper disclosure case:* A man had an unlisted telephone number for personal safety reasons. He moved house, and had to get a new phone number. The telecommunications company listed his new number in the telephone directory, much to his distress. After he complained to the Commissioner, the company agreed to amend its procedures to make sure that the confidential status of phone numbers was maintained despite changes of address or phone number.[3]

- *Refusal of access case:* Several health agencies refused an executor's request for access to a deceased person's health information, because the other executor had not agreed that the information should be released. New Zealand law states that an executor is a deceased person's representative and in almost all cases has a right of access to the person's health information. Health agencies cannot demand that each executor should agree to the release of the information. The health agencies accepted the Commissioner's view and released the information to the executor.[4]

- *Charging for access case:* Several lawyers complained that local authorities were charging their clients for accessing rating information about their properties. Public sector authorities are not permitted to charge for giving an individual access to their own personal information unless there is an express statutory permission to charge. The statute governing access to the register of property rating information does not expressly state that authorities can charge individuals for access to their own information, although it clearly permits charging for third party access. The local authorities amended their processes so that only third parties would be charged[5].

The Human Rights Review Tribunal has jurisdiction to hear a matter and make a judicial determination[6], provided that the Privacy Commissioner has first investigated the matter. Of the 25 new cases brought to the Tribunal in 2010/11, one of the most

---

[2] The Privacy Commissioner receives nearly 1000 complaints per year, around 30% of which result in settlement of the dispute. In 2010/11, of complaints which the Commissioner found had substance, 90% were settled. The Commissioner publishes case notes about some of the complaints she receives each year, to provide guidance about how she interprets the Privacy Act in given situations. People can subscribe through the website at www.privacy.org.nz to receive case notes automatically (no cost).

[3] Case note 225274 [2011] NZPrivCmr 10: http://tinyurl.com/7okx3s2

[4] Case note 231747 [2011] NZPrivCmr 8: http://tinyurl.com/8xhb8fp

[5] Case note 209742 [2010] NZPrivCmr 21: http://tinyurl.com/89lqlal

[6] The Tribunal's judicial determination are the source of much of the authoritative privacy jurisprudence in New Zealand. Its decisions are available at <http://www.nzlii.org/nz/cases/NZHRRT/>.

significant was *Shahroodi v Civil Aviation Authority* [2011] NZHRRT 6 (under appeal), where the Tribunal decided that the CAA had improperly refused Mr Shahroodi's request for access to information about himself. The Tribunal found that because Mr Shahroodi did not have access to the information, he did not have a proper opportunity to state his case before the Director of Civil Aviation decided to cancel his pilot's licence. The Tribunal also found that Mr Shahroodi had suffered significant distress as a result of the CAA's failure to provide him with information. It awarded compensation totalling $10,000 – half for loss of opportunity to comment and half for distress. The figure is larger than might have been expected for similar "loss of opportunity" cases a few years ago, particularly as not all the plaintiff's evidence of harm was accepted. This suggests that the Tribunal is increasing its awards of compensation for failures to provide access to personal information.

New Zealand – The Street View and Buzz investigations

The Commissioner does not have to receive a complaint to investigate an incident, and Privacy Commissioner-initiated investigations (or "CIIs") sometimes involve an in-depth investigation culminating in a public report or statement. The most significant recent CII report is the Commissioner's December 2010 report into Google's collection of information from wi-fi networks in New Zealand during its "Street View" filming operations.[7] The Commissioner found that Google had breached its obligations to tell people that it was collecting MAC addresses and other information about wi-fi networks. Some of that information could be classified as 'personal information' under NZ law as it was capable of identifying individuals. Google had a legitimate reason to collect the information (to improve the performance of its location based services), but it could and should have expressly told people that this was part of its Street View operation: Street View was doing more than taking photographs.

The Commissioner also found that Google had no legitimate reason to collect payload information from unsecured wi-fi networks and that the collection was seriously intrusive. From a privacy perspective, it did not matter that Google had collected the information inadvertently. The investigation resulted in Google providing various undertakings to the Commissioner, including to delete the payload information; apologise to consumers; change its internal review processes for products with a significant effect on personal information; undertake privacy impact assessments for any future Street View filming in New Zealand; and regularly consult with the Commissioner about significant product launches that could affect the privacy of New Zealanders.

The investigation had two additional notable features. First, the Commissioner referred the collection of payload data to the NZ Police, in case the collection breached the law on interception of communications. While the Police ultimately decided not to proceed, this shows that the Commissioner will work closely with other relevant agencies if she believes there may have been evidence of significant misconduct or breach of other laws. Secondly, the Commissioner to some extent co-ordinated the investigation with similar investigations in other jurisdictions overseas.[8]

---

[7] http://privacy.org.nz/google-s-collection-of-wifi-information-during-street-view-filming/)

[8] Linkomes, L 'Google, Facebook face increased pressure from the regulators' *Privacy Laws & Business International Report*, Issue 110, May 2011, 17-18

Co-ordinated enforcement action – where an agency is given a similar message by a variety of privacy commissioners – can maximise the impact that a small jurisdiction is able to have. Another example in 2010 was the joint letter that ten privacy commissioners, including New Zealand, sent to Google in the wake of its faulty launch of Google Buzz, which exposed contact lists without people's consent.[9] Joint enforcement action is going to increase and improve in the coming years, in the wake of initiatives such as the Global Privacy Enforcement Network and the APEC cross-border privacy enforcement work. New Zealand is an active member of both initiatives.

Australia – Federal law

Two largely unprecedented developments in the enforcement of Australia's *Privacy Act 1988* occurred in 2011.

The Federal Court decision in *Smallbone v New South Wales Bar Association* [2011] FCA 1145 resulted in only the second injunction in 20 years being issued under under the Act. An unusual provision in the Act (s98) allows any party to go directly to the Federal Court (bypassing the Privacy Commissioner), but only to obtain an injunction against breach of one of the data privacy Principles. Here, an applicant for 'silk' (appointment as Senior Counsel) successfully obtained an injunction to prevent the NSW Bar Association from announcing the results of his application until he was able to access the information on which the decision was to be made (while preserving the anonymity of those commenting on his application) in order for him to see whether any of it was erroneous and if so to decide whether he would further challenge it under the Act. The Bar Association did not appeal.

The Privacy Commissioner has power under s52 of the Act to award compensation and other remedies for breaches of the privacy principles (called 'determinations'). However, the Commissioner has only once before considered a claim for compensation in making a determination, and in that case (*Rummery*[10]) there was a successful appeal against inadquacy of the Commissioner's award of damages. In *'D' and Wentworthville Leagues Club* [2011] AICmr 9 the Commissioner held that the Club had interfered with the complainant's privacy by disclosing the complainant's membership details and gaming information to the complainant's ex-partner, in breach of National Privacy Principle 2. The Commissioner ordered that the Club apologise, undertake staff training, and pay the complainant A$7,500 (US$8,084) for non-economic loss but was not satisfied that the complainant suffered economic loss. The Commissioner's reasoning appears to endorse the view of the Tribunal in *Rummery* that it would '... not go so far as deciding that we must award compensation once a loss is established. However … once loss is proved, there would need to be good reason shown … as to why compensation for that loss should not be awarded', but whether this approach will be followed remains to be seen. Consistent with the few other s52 determinations issued by the Commissioner, the respondent was named.

---

[9] http://privacy.org.nz/media-release-privacy-guardians-warn-multinationals-to-respect-laws/

[10] *Rummery and Federal Privacy Commissioner and Anor* [2004] AATA 1221

There were 19 case notes in 2011 of complaints under the *Privacy Act 1988* published by the Office of the Australian Information Commissioner[11], of which four resulted in changes to the practices of the organisations complained about:

- *Disclosure of debt information*: The complainant contracted with a buyer to sell his car over which a financial institution had previously held a security.. The prospective buyer obtained a letter from that financial institution confirming that the loan had been fully repaid and the security discharged.. The letter did not contain details such as the complainant's name, address or date of birth.Nevertheless the Commissioner considered that the information in the letter related to the complainant's account with the financial institution and as such was a disclosure of personal information about the complainant. The fact that the prospective buyer had previous knowledge of these details did not lessen the financial institution's obligation under NPP 2.1 to only disclose an individual's personal information for the primary purpose of its collection, or for a secondary purpose where it can rely on one of the statutory exceptions (which did not apply here). The financial institution immediately ceased its practice of sending such letters to third parties without the written consent of the account holder. It also apologised and offered a goodwill payment. (*Q and Financial Institution* [2011] AICmrCN 11)

- *Recording of outbound calls:* The complainants alleged that a retail company recorded outbound calls it made to them without providing sufficient notification.. When the complainants became aware their calls were being recorded they objected, claiming that they had not been notified or asked for their consent as required by the *Privacy Act*. The retail company argued that the complainants had been notified about the recording of calls by the interactive voice response system when they made their first inbound call to the company. The Commissioner considered that the recording of calls for training, coaching and monitoring purposes was necessary for one of the company's functions (as the Act requires) However under the *Telecommunications (Interception and Access) Act 1979* (Cth) all parties in the telephone conversation must have actual knowledge that the conversation will be monitored prior to both inbound and outbound calls. Notification can be by pre-recorded message, verbal or written notification. Neither the notification prior to the original incoming call nor the the company's privacy policy gave sufficient notice or constituted obtaining of consent. Therefore, the collection of personal information during such calls was by unfair and unlawful means, and in breach of National Privacy Principle 1.2. The Commissioner did not accept that the subsequent calls were a continuation of the original incoming call where notification had been provided. Subsequently, the company changed its procedures so that a standard script is read by the staff member when making every outbound call to advise the individual the call is being monitored and recorded for training purposes. (*P and Retail Company* [2011] AICmrCN 10)

- *Inaccurate personal data:* In the course of a fraud investigation an insurance company collected the complainant's personal information from a third party

[11] Available at <http://www.oaic.gov.au/publications/case_notes.html>

insurance industry database,. The complainant discovered that the insurance company had made multiple enquiries about them, stating different purposes for each and with no common reference number. The Commissioner found that the insurance company had recorded incorrect descriptors and was unable to verify why it had made the enquiries, or to find the various entries when it needed to correct the information and had not taken reasonable steps to ensure the personal information it disclosed was accurate and complete, as required by the Act. Consequently the insurance company changed its procedures to ensure its staff used a unique reference number for enquiries, and retrained staff on the appropriate use of descriptors. The company also amended the complainant's personal information so it was accurate, and offered an unconditional apology, which was accepted. (*I and Insurance Company* [2011] AICmrCN 3)

- *Excessive collection by a club:* A registered club insisted on scanning the driver's licences of visitors to the club as a condition of entry. The complainant conceded that the club was required to collect their name, address and signature, but considered the collection of the other information on the licence (including date of birth, driver's licence number, driver's licence type and photograph) to be unnecessary. The club would not agree to cease or alter its identity scanning practices, and claimed it did offer its patrons the alternate option of manually completing and signing the register. It offered to delete the scanned licence details if the complainant provided a statutory declaration concerning dates of their visits to the club. The Commissioner decided that the offer of deletion coupled with the alternative option of manual sign-in adequately dealt with the collection issues. The Commissioner did not proceed further to consider whether the general practice of scanning licences was excessive collection of information. (*H and Registered Club* [2011] AICmrCN 2).[12]

Australia – Victorian public sector

The Victorian Privacy Commissioner investigates complaints against Victorian public sector agencies, and in 2011 published case notes[13] on four such investigations, of which two are significant:

- *Excessive disclosure in workplace investigation:* The complainant complained to her employer (the respondent) of bullying by various co-workers. The complaint was by a letter which included a chronological list of all of the alleged bullying incidents and set out the complainant's state of mind, emotional responses to the incidents, and outcomes sought. The employer advised that full copies of the letter would be provided to each of the alleged bullies. Reluctantly the complainant agreed to this and the copies were distributed. The Privacy Commissioner decided that the full disclosure of the document to all of the alleged bullies appeared to be far more than what they needed to respond to the complaint about their own alleged behaviour.

[12] For a similar case note from New Zealand in 2011, see case note 221786 [2011] NZPrivCmr 2: **http://tinyurl.com/7jrkgc7**

[13] http://www.privacy.vic.gov.au/privacy/web2.nsf/pages/case-notes

Disclosure of information in this context should have been kept to the minimum necessary to investigate the matter. The document should have been edited in order to protect the complainant's privacy. The complainant's consent could not be relied on, because the Act requires that individuals must be provided with a real choice about what will happen with their personal information. The excessive disclosure also meant that the respondent had not taken reasonable steps to protect the personal information it held. The complaint was successfully conciliated with the organisation apologising, agreeing to change its policies relating to bullying investigations and paying compensation. (*Complainant AU v Public Sector Agency* [2011] VPrivCmr 3)

- *Inadequate notice of website publication:* The complainant's submission to a local council included comments about the complainant's neighbours, in response to a request for submissions about a local law. The submission identified both the neighbours and the complainant. The complainant knew the submission would be discussed at a meeting of the local council, but was surprised to find it included in full in the minutes of the meeting which were then published on the Internet and searchable via search engines. The Commissioner held that the notice given by the council when soliciting submissions failed to adequately inform the complainant that such submissions would be placed on the Local Council's website, and therefore did not ensure that the individual knows for what purpose the information is collected and in what way the organisation may disclose that information as required by Privacy Principle 1.3. The complaint was resolved by conciliation with the council agreeing to remove the letter from its website, offering a statement of regret, commiting to additional privacy training for its staff, and agreed to amend its privacy policy and notices concerning publication of submissions. (*Complainant AT v Local Council* [2011] VPrivCmr 2)

Where complaints cannot be resolved by the Victorian Privacy Commissioner, they can be referred to the Victorian Civil and Administrative Tribunal (VCAT). During 2011 VCAT did not deliver decisions on any such cases, and nor were there any decisions of the Victorian Supreme Court concerning the *Information Privacy Act 2000*.

Australia – NSW public sector

There were 38 court or tribunal decisions in 2011 considering the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIPA), which covers the New South Wales (NSW) state public sector including local government. Local Area Health Services account for a high percentage of cases going to the Tribunal. The *Health Records and Information Privacy Act 2002* (HRIPA) contains similar principles applying to health service providers in both the public and private sectors in NSW. Unless noted otherwise the decisions discussed below are by the Administrative Decisions Tribunals (ADT) of NSW. The examples following illustrate the wide range of remedies available from the ADT.

- The most significant remedy awarded by the ADT required the respondent Area Health Service to pay the applicant compensation totalling A$40,000 (US$43,115) in respect of breaches of both the Act and the *Health Records and Information Privacy Act 2002* (NSW). This is the maximum amount of

compensation payable under the Act. The willingness of the Tribunal to make awards of the maximum allowable compensation must send a strong signal to government agencies concerning settlements with compensation when they are conducting their own internal investigations, which are required before a case can go the Tribunal. (*NK v Northern Sydney Central Coast Area Health Service (No.2)* [2011] NSWADT 81)

- An Area Health Service was required by the ADT to correct its records by destroying one file on the applicant patient's medical record; by deleting the name and contact details of his son from his clinical form; and by annotating his form to state that the patient requests that his son not be contacted. (*TB v South Eastern Sydney Illawarra Area Health Service [2011] NSWADT 165*)

- Another Area Health Service was found to have disclosed patient informaton to two doctors, in breach of an Information Privacy Principle. It was ordered to apologise in writing for each of the breaches found; to write to the two doctors seeking to recover the health information wrongly disclosed to them; to ensure that any recovered information was stored with proper security, and to advise the patient of the outcomes of this process. The ADT obviously can and does give detailed instructions to agencies on how to carry out remedial actions. (*QB v Greater Southern Area Health Service* [2011] NSWADT 90)

- The same Area Health Service was also required by the ADT to undertake wide-ranging policy review and staff training, as a result of the above complaint. It was required to review and reissue within 90 days its Health Intake and Triage Policy so that it complies with the Health Privacy Principles (HPPs) on a lengthy and specific list of matters; and to introduce within six months, training for mental health workers that it employs in the proper implemenaton and observance of the HPPs. (*QB v Greater Southern Area Health Service No 2* [2011] NSWADT 162)

- The pseudonymisation of a court decision previously published on the Internet was the remedy provided by the ADT in one decision. The Tribunal had published its decision on the applicant's claim in a discrimination matter, and according to its usual practice, its reasons for decision were published on the internet identifying the applicant. During a subsequent hearing of an application for costs, the applicant sought orders under s75 of the *Administrative Decisions Tribunal Act 1997 (NSW)* to amend the Tribunal's published reasons so as to anonymise her name, the name of her daughter who was a witness, the names of her parents and the name of her business, on the grounds that identifying any of them would also identify her. The Tribunal noted that its decision referred to the fact that the applicant had been diagnosed as suffering from serious mental disorder, to the various symptoms of mental disorder, their effects, and their treatment, because these were matters central to the issues in dispute. The Tribunal accepted the applicant's submission that the names ought be suppressed for three reasons: (i) mental health informaton has the potential to be used in prejudicial ways against her in future, with or without her knowledge, given the persistence of considerable prejudice in the community against persons with mental health conditions; (ii) the provisions of the *HRIPA* demonstrate that that NSW public policy accords increasing importance to the privacy of health information; and (iii) the

published decisions of the Tribunal remain unaltered, even after information they contain about a party's health is out of date, in sharp contrast with the provisions of the this Act for the updating of health information. (*ACE v State of NSW (TAFE Commission and DET (No 2)* [2011] NSWADT 77)

- In an industrial dispute before the NSW Industrial Relations Commission, privacy considerations resulted in the reduction of what might have otherwise been a remedy of reinstatement for an employee dismissed from a government position to a payment of six month's salary. This was because the Commission found that the employee had used 'data downloads, correspondence and other material that contained sensitive client information' to assist his industrial claim, in breach of ss17 and 18 of the *PPIPA*. 'As a public servant he seriously and knowingly breached client confidentiality for his own private purposes in circumstances where it was completely unjustified', said the Commission, and this 'added to our lack of confidence in reinstatement or re-employment in the Public Service being appropriate remedies'. (*Raeburne v Department of Justice and Attorney General* [2011] NSWIRComm 48)

- The continuing inability of the *PPIPA* to provide any remedy in some clear situations of privacy breaches was demonstrated again in 2011. The Tribunal found that it was probable that a Council employee provided a third party with details of the applicant's correspondence with the Council, without consent of either the applicant or the Council. However, the Tribunal followed the precedent established in the NSW Court of Appeal in *Director General, Department of Education and Training v MT* [2006] NSWCA 270 and found there was no breach of the *PPIPA*. In *MT's Case* the Court of Appeal held that where 'the "use" or "disclosure" of information was for a purpose extraneous to any purpose of the Department, it should not be characterised as "use" or "disclosure" by the Department or conduct of the Department' under s18, and the Department was not vicariously liable for such conduct. Here, although the employee 'sent the correspondence to the Council for a purpose that was directly related to the Council's functions', this 'was for a purpose extraneous to the business of Council' namely the employee's own purposes in assisting the third party in its dealings with the Council. The Tribunal considered that 'she embarked upon a frolic of her own that was unrelated to her duties or the Council's functions'. (*NY v Lake Macquarie City Council* [2011] NSWADT 13)

Conclusions

From this survey of recent enforcement examples in New Zealand and Australia it is clear that significant examples of enforcement of privacy laws continue to occur in all four jurisdictions considered, and some examples show the strengthening of particular remedies. However, the mechanisms through which signficant enforcement arises differs a great deal between jurisdictions. In these Australasian examples they include complainant-initiated injunctions, both awards of damages and mediations by Privacy Commissioners, orders by quasi-judicial Tribunals, and suppression orders by Tribunals. One overall factor shared by all four Australia and New Zealand jurisdictions is that payments of financial compensation to complainants are possible and do occur. A comprehensive assessment of enforcement effectiveness would also require statistical information to be considered. Such analysis of enforcement of

privacy laws and its effectiveness (covering examples, statistics and mechanisms) is an important aspect of privacy research which is not yet fully developed.

An article in the next issue will consider recent enforcement examples in Asian jurisdictions with established laws (Hong Kong, Japan, South Korea, Macau and Taiwan), and some other jurisdictions such as Indonesia where there are new examples of enforcement. It will also consider whether any trends in enforcement are apparent across the whole region.