THE PRIVACY COMMISSIONER AND OWN-MOTION INVESTIGATIONS INTO SERIOUS DATA BREACHES: A CASE OF GOING THROUGH THE MOTIONS?

JODIE SIGANTO* AND MARK BURDON**

I INTRODUCTION

Data breaches resulting from information security failures continue to be an issue of pressing concern.[1] The Office of the Australian Information Commissioner ('OAIC') recognises that data security is a major challenge for organisations.[2] Starting in February 2011, the OAIC commenced a series of 'high profile' investigations into alleged data breaches.[3] Each of these investigations was commenced by the Privacy Commissioner (the 'Commissioner') with reference to the OAIC's Own Motion Investigation ('OMI') powers.[4] These powers allow the Commissioner to conduct an investigation without any prior

* Dr Jodie Siganto is a collaborator on the Cyber Security Cartogaphies project led by Dr Lizzie Coles-Kemp, Royal Holloway University of London, which is part of the United Kingdom's first Cyber Security Research Institute.

** Mark Burdon is a Lecturer at the TC Beirne School of Law, University of Queensland.

1 Cyber security is referred to as a 'strategic priority for Australia's national security with the threat of cyber-attacks dramatically increasing': Nicole Brangwin, 'Cyber Security' (Briefing Book, Parliamentary Library, Parliament of Australia) <http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook44p/Cyber>. Results from a survey by the OAIC show that nearly a quarter (23 per cent) of respondents were concerned about the risk of identity fraud and theft while 16 per cent were concerned more generally by data security and the risks to financial data (11 per cent): Office of the Australian Information Commissioner, *Community Attitudes to Privacy Survey* (Research Report, 2013) 3.

2 See Office of the Australian Information Commissioner, 'Privacy Breach: 254 000 Australian Online Dating Profiles Hacked' (Media Release, 25 June 2014) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/privacy-breach-245-000-australian-online-dating-profiles-hacked>, in which the Commissioner said that 'businesses must remain vigilant about information security'.

3 The Commissioner has referred to 'high profile' investigations into data breach cases on a number of occasions: see, eg, Office of the Australian Information Commissioner, *Annual Report 2011–12* (2012) 6–7, 64 ('*OAIC 2012 Annual Report*'); Timothy Pilgrim, 'Privacy: What's Ahead in 2012' (Speech delivered at the International Association of Privacy Professionals Australia & New Zealand Annual Summit, 30 November 2011) <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-whats-ahead-in-2012>; Office of the Australian Information Commissioner, *Annual Report 2012–13* (2013) 78 ('*OAIC 2013 Annual Report*').

4 Office of the Australian Information Commissioner, *Commissioner Initiated Investigation Reports* <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/>.

complaint being made.[5] The Commissioner heralded the use of OMIs and the subsequent publication of reports as a change in its enforcement approach to 'particularly serious or high profile privacy incidents'.[6] All of these incidents related to data breaches. The new strategy was partially developed to increase the transparency of the OAIC's investigation process and to help organisations and agencies to better understand their privacy responsibilities.[7]

Surprisingly, the Commissioner's change in approach has received little scholarly attention given the heightened concern about data breaches and past criticisms of the Commissioner's failure to pursue a robust enforcement approach. Previous research has focussed on the way the OAIC has used its investigation powers generally,[8] with only limited consideration of the use of powers in

5 *Privacy Act 1988* (Cth) s 40(2) ('*Privacy Act*').

6 Timothy Pilgrim, 'Privacy Law Reform: Challenges and Opportunities' (Speech delivered at the Emerging Challenges in Privacy Law Conference, Monash University, 23 February 2012) <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-law-reform-challenges-and-opportunities>.

7 Ibid; *OAIC 2012 Annual Report*, above n 3, 64; *OAIC 2013 Annual Report*, above n 3, 78–9.

8 The Australian Law Reform Commission ('ALRC') refers to the public perception of the Commissioner as a 'toothless tiger' in its analysis of stakeholder feedback as part of its review of the *Privacy Act*: Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 109 ('*For Your Information Report*'). For other literature regarding the Commissioner's powers and the use thereof, see Lee A Bygrave, 'Where Have All the Judges Gone? Reflections on Judicial Involvement in Developing Data Protection Law' (Pt 1) (2000) 7(1) *Privacy Law and Policy Reporter* 11; Lee A Bygrave, 'Where Have All the Judges Gone? Reflections on Judicial Involvement in Developing Data Protection Law' (Pt 2) (2000) 7(2) *Privacy Law and Policy Reporter* 33; Graham Greenleaf, '"Tabula Rasa": Ten Reasons Why Australian Privacy Law Does Not Exist' (2001) 24 *University of New South Wales Law Journal* 262; Graham Greenleaf, Nigel Waters and Lee Bygrave, Cyberspace Law and Policy Centre, *Promoting and Enforcing Privacy Principles: An Analysis of ALRC Proposals for the Role of the Privacy Commissioner* (Submission to the Australian Law Reform Commission on the Review of Australian Privacy Laws Discussion Paper No 72, 19 December 2007); Nigel Waters, Abi Paramaguru and Anna Johnston, 'Enforcement of Privacy Laws – Issues Arising From Australian Experience' (Working Paper No 3, Cyberspace Law and Policy Centre, November 2007); Graham Greenleaf, *Reforming Reporting of Privacy Cases: A Proposal for Improving Accountability of Asia-Pacific Privacy Commissioners* <http://www2.austlii.edu.au/~graham/publications/2003/Reforming_reporting/#fn60>; Graham Greenleaf and Nigel Waters, *Australia's Privacy Bill 2012: Weaker Principles, Stronger Enforcement* (Privacy Laws and Business International Report, Issue 118, July 2012) 16; Anthony Bendall, *The Governance of Privacy: Speak Softly and Carry a Big Stick* (Speech delivered at the Australian Institute of Administrative Law Forum, Melbourne, 8 August 2008); Graham Greenleaf and Nigel Waters, '"Making Privacy Law Safe for Business": Australia's 2012 Privacy Bill' (2012) 8 *Privacy Law Bulletin* 266; Mark Burdon and Alissa McKillop, 'The Google Street View Wi-Fi Scandal and Its Repercussions for Privacy Regulation' (2014) 39 *Monash University Law Review* 702; Mark Hummerston, 'Sword or Shield: The Role of a Regulator' (Speech delivered at the Interpreting Privacy Principles Symposium, University of New South Wales, 3 July 2007) <http://www.cyberlaw centre.org/ipp/events/symposium07/Sword%20or%20shield.pdf>; Kevin O'Connor, 'The Federal Privacy Commissioner: Pursuing a Systemic Approach' (2001) 24 *University of New South Wales Law Journal* 255. For references to the Commissioner's new powers, see Ashley Tsacalos and Vanessa Verzi, *Civil Penalties for Breach of Privacy – Coming Soon* (Norton Rose Fulbright Public Law Report, Spring 2013) 4; Charles Alexander, Elisabeth Koster and Helen Paterson, 'Punitive Powers Guided by Ambiguity: The Australian Federal Privacy Commissioner's New Powers in the Context of a Principles-Based Privacy Regime' (2013) 9 *Privacy Law Bulletin* 66.

relation to data breach incidents.[9] This article fills a gap in the current literature and examines the actual investigatory and decision-making procedures adopted in six data breach-related OMIs undertaken between February 2011 and July 2012. They involve a range of different respondents, different types of security incidents and different findings regarding breaches of privacy principles, with a particular focus on National Privacy Principle ('NPP') 4. NPP 4 required entities covered by the *Privacy Act 1988* (Cth) ('*Privacy Act*') to implement reasonable security measures in order to protect personal information.

We examine how these investigations were conducted and the basis for the decisions made, including the publication of final investigation reports. Our framework for examination includes the OAIC's own published guidance as to how it should undertake investigations and publish reports,[10] and generally recognised principles for the exercise of regulatory powers.[11] Part II provides background to the Commissioner's investigations and interest in data breach cases and then outlines the methodology adopted. Part III details the reasoning behind the OAIC's investigatory processes including the reasons for undertaking the OMIs, the process of evidence collection, the decision-making process adopted, and the reasons for the publication of final results in OMI reports.

Our findings indicate that the investigation process followed in these six cases could be described as high-level, and lacking in both balance and vigour. Part IV then puts forward reasons for the standard of these investigations by critically questioning whether the OAIC had sufficient powers and resources to adequately conduct the OMIs. We also consider whether the Commissioner pursued these OMIs as a means to further the OAIC's policy agenda regarding the development of a mandatory data breach notification scheme.

---

9 In relation to National Privacy Principle ('NPP') 4, see Nigel Waters, Graham Greenleaf and Paul Roth, 'Interpreting the Security Principle' (Working Paper No 1, Cyberspace Law and Policy Centre, March 2007) <http://www.cyberlawcentre.org/ipp/publications.html>; Nigel Waters, 'Interpreting the Security Principle' (Speech delivered at the Interpreting Privacy Principles: Chaos or Consistency? Symposium, University of New South Wales, 17 May 2006); Nigel Waters and Graham Greenleaf, 'IPPs Examined: The Security Principle' (2004) 11 *Privacy Law and Policy Reporter* 67.

10 For an illustration of guidance issued by the OAIC, see, eg, Office of the Australian Information Commissioner, *Guide to Internal Investigations* (Privacy Fact Sheet No 9, April 2012) <http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-fact-sheets/privacy-fact-sheet-09-guide-internal-investigations.pdf>; Office of the Australian Information Commissioner, *What Will Happen to My Complaint?* (Privacy Fact Sheet No 10, June 2012) <http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-fact-sheets/privacy-fact-sheet-10-my-complaint.pdf>; Office of the Australian Information Commissioner, *How Will the OAIC Handle a Privacy Complaint against My Organisation?* (Privacy Fact Sheet No 11, June 2012) <http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-fact-sheets/privacy-fact-sheet-11-respondent-information.pdf>; Office of the Australian Information Commissioner, *Guide to Producing Case Notes* (January 2013) <http://www.oaic.gov.au/about-us/corporate-information/privacy-operational/guide-to-producing-case-notes>; Office of the Australian Information Commissioner, *Privacy Complaints and Procedures Manual*. This document is no longer published on the OAIC's website. A copy is available from the authors.

11 These principles include transparency, balance and vigour. See *For Your Information Report*, above n 8, 251 [4.74].

We conclude that the OAIC's decision to conduct these OMIs was to highlight and support its policy interests, without having the requisite resources or powers to conduct the investigations effectively. In other words, in the interests of pursuing a data breach policy agenda, the OAIC seems to have been going through the motions in its data breach investigations.

II BACKGROUND AND METHODOLOGY

A United States ('US') survey of data breaches in the first six months of 2014 reveals multiple incidents in which data, including names and addresses, credit card details and medical records, was accidently or inadvertently exposed to or compromised by attackers.[12] Many of these incidents, such as the Target attack that affected over 40 million customers[13] and the eBay compromise that involved over 145 million members,[14] have received extensive international media coverage. Similar events are occurring in Australia. In December 2012, the personal details of thousands of Australian military staff and students were illegally accessed by a hacker who breached a university database at the Australian Defence Force Academy.[15] Another successful compromise affected a number of Australian online retailers, including the popular website Catch of the Day, resulting in unauthorised access to names, delivery addresses, email addresses, encrypted passwords and credit card data.[16] The unauthorised access,

12 Martyn Williams, *The 5 Biggest Data Breaches of 2014 (So Far)* (11 July 2014) PC World <http://www.pcworld.com/article/2453400/the-biggest-data-breaches-of-2014-so-far.html>.

13 Brian Krebs, 'Target: Names, Emails, Phone Numbers on Up to 70 Million Customers Stolen' on Brian Krebs, *Krebs on Security* (10 January 2014) <http://krebsonsecurity.com/2014/01/target-names-emails-phone-numbers-on-up-to-70-million-customers-stolen/>; Grant Gross, *Update: Breach Exposes Data on 70 Million Customers, Target Now Says* (10 January 2014) Computer World <http://cwonline.computerworld.com/t/8834412/980558529/651232/17/>.

14 Denver Nicks, 'Investigators Target eBay Over Massive Data Breach', *Time* (online), 23 May 2014 <http://time.com/110210/ebay-data-breach/>; Fran Foo, 'Warning after eBay Passwords "Stolen"', *The Australian* (online), 23 May 2014 <http://www.theaustralian.com.au/technology/warning-after-ebay-passwords-stolen/story-e6frgakx-1226927542280>.

15 The stolen data, which included 'names, identification numbers, passwords, email addresses and dates of birth' of 'about 10 000 students and 1900 staff' at the Academy, was subsequently posted on several different websites: Markus Mannheim, 'Military Personnel Data Hacked for "Fun"', *The Canberra Times* (online), 11 December 2012 <http://www.canberratimes.com.au/it-pro/government-it/military-personnel-data-hacked-for-fun-20121211-2b6yp.html>.

16 Josh Taylor, *Catch of the Day Waits 3 Years To Reveal Data Breach* (18 July 2014) ZD Net <http://www.zdnet.com/au/catch-of-the-day-waits-3-years-to-reveal-data-breach-7000031759/>.

loss, misuse, or disclosure of personal information is an issue of concern often raised with the Commissioner.[17]

Despite these widely reported data breaches and concern about the compromise of personal information, there has been, to date, little regulatory response to the issue of data security in Australia. NPP 4 and its successor, Australian Privacy Principle ('APP') 11, are among the few legislative provisions regulating corporate information security practices in Australia.[18] NPP 4 required a private sector organisation covered by the Act[19] to 'take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure'.[20]

A mandatory data breach notification scheme has been a persistent regulatory initiative to remedy the problem of data breaches in Australia. Data breach notification schemes require that organisations suffering a data breach must notify those likely to be affected. Such schemes were first introduced in the US in 2002 as a response to the problem of identity theft.[21] They are now widespread

17 Inadequate data security was the most common cause of complaint to the Commissioner in 2008/09: Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2008 – 30 June 2009* (2009) 65. In 2010/11, it represented 37 out of 99 of the total number of complaints made: Office of the Australian Information Commissioner, *Annual Report 2010–11* (2011) 37 ('*OAIC 2011 Annual Report*'). It further represented the cause of complaint in over 15 per cent of cases in 2011 and 2012: *OAIC 2012 Annual Report*, above n 3. In 2012/13, the OAIC inquiries line received 9009 calls related to privacy matters within jurisdiction, 1159 of which raised issues in regard to data security: *OAIC 2013 Annual Report*, above n 3, 64–6, while 12.2 per cent of complaints related to data security: at 69. The OAIC's 2014 annual report covers the transition period between the NPPs and the Information Privacy Principles ('IPPs') to the new Australian Privacy Principles ('APPs'). In that report, only 3.8 per cent of complaints raised issues in relation to NPP 4, while 21.7 per cent raised issues in regard to IPP 4 (which applied to public sector agencies): Office of the Australian Information Commissioner, *Annual Report 2013–14* (2014) 83 ('*OAIC 2014 Annual Report*'). Further, only 0.9 per cent of complaints related to the new APP 11.

18 Other legislated security obligations include *Privacy (Tax File Number) Rule 2015* (Cth) r 11(1)(a), issued under *Privacy Act* s 17, which requires tax file number ('TFN') recipients to take reasonable steps to safeguard TFN information. Access controls must be established to protect electronic health records pursuant to *PCEHR Rules 2012* (Cth) pt 2, issued under *Personally Controlled Electronic Health Records Act 2012* (Cth) s 109. There are industry-specific codes which impose some security obligations. These include Australian Bankers' Association, *Code of Banking Practice* (at 1 February 2014), which is a voluntary industry scheme overseen by the Australian Bankers' Association Inc. Another important code is Communications Alliance, *Telecommunications Consumer Protections Code* (at May 2012), in particular cl 6.9.

19 There are a number of exemptions and 'carve-ins' in terms of the private organisations covered by the *Privacy Act*. Eg, s 6D(4)(b) provides that an organisation is not a 'small business' (and so will not come within the small business exemption from the Act) if it 'provides a health service to another individual and holds any health information'. See also s 7B(3), which exempts employee records from the Act.

20 The NPPs were contained in *Privacy Act* sch 3. As of 12 March 2014, the NPPs have been replaced by a new set of principles, namely the APPs: Office of the Australian Information Commissioner, *Privacy Fact Sheet 17: Australian Privacy Principles* (2014). Detailed consideration of what constitutes 'reasonable steps' for the purposes of NPP 4 is outside the scope of this article. However, it has been examined in the literature: see generally Waters and Greenleaf, above n 9.

21 Cal Civ Code §§ 1798.29, 1798.80.

throughout the US,[22] and apply to the electronic communications sector in the European Union ('EU')[23] though extensions have also been considered.[24] In 2008, the Australian Law Reform Commission ('ALRC') recommended the introduction of a mandatory data breach notification scheme referring to the increased risk that a security breach could result in identity theft and that notification of a breach would allow individuals to take remedial steps to protect themselves.[25] The ALRC also noted that data breach notification 'encourages agencies and organisations to be transparent about their information-handling practices'.[26]

The Australian Government's first stage response to the ALRC recommendations did not refer to the ALRC's recommendation regarding data breach notification.[27] Instead, a discussion paper for public consultation was issued in late 2012.[28] The OAIC supported the ALRC's proposal while noting that the introduction would require the allocation of significant additional resources to the OAIC.[29] Draft legislation was issued in June 2013,[30] and was

22 The first data breach notification law was introduced in California in 2002 (and enacted in 2003): see, eg, Gina Stevens, *Data Security Breach Notification Laws* (Congressional Research Service Report for Congress, 10 April 2012) 3. Another 46 states have since followed suit: at 4. For a full list of relevant US legislation, see National Conference of State Legislation, *Security Breach Notification Laws* (12 January 2015) <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

23 See, eg, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector: *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communication)* [2002] OJ L 105/23; *Regulation (EU) No 611/2013 of 24 June 2013 on the Measures Applicable to the Notification of Personal Data Breaches under Directive 2002/58/EC of the European Parliament and of the Council on Privacy and Electronic Communications* [2013] OJ L 173/2.

24 On 25 January 2012, the European Commission proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online data protection rights and boost Europe's digital economy, which included a broader data notification provision: see, eg, European Commission, 'Commission Proposes a Comprehensive Reform of Data Protection Rules To Increase Users' Control of Their Data and To Cut Costs for Businesses' (Press Release, 25 January 2012) <http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en>. The reform is expected to pass in 2015. For the status of the proposed reform to the EU's data protection rules, see European Commission, *Data Protection Day 2015: Concluding the EU Data Protection Reform Essential for the Digital Single Market* (Fact Sheet, 28 January 2015) <http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm>.

25 *For Your Information Report*, above n 8, ch 51.

26 Ibid [51.73].

27 Australian Government, *Enhancing National Privacy Protection* (First Stage Response to the Australian Law Reform Commission Report No 108 For Your Information: Australian Privacy Law and Practice, October 2009) 14.

28 Australian Government, 'Australian Privacy Breach Notification' (Discussion Paper, Attorney-General's Department, October 2012).

29 John McMillan and Timothy Pilgrim, Submission to Senate Legal and Constitutional Affairs Committee, *Inquiry into Privacy Amendment (Privacy Alerts) Bill 2013* <http://www.oaic.gov.au/news-and-events/submissions/privacy-submissions/inquiry-into-privacy-amendment-privacy-alerts-bill-2013>.

30 Privacy Amendment (Privacy Alerts) Bill 2013 (Cth).

referred to a parliamentary committee for consideration,[31] but then lapsed. The Attorney-General's Department consulted the OAIC regarding the drafting of the Bill,[32] which was reintroduced into the Senate in 2014. The current status of the Bill is uncertain.[33] In February 2015, the Parliamentary Joint Committee on Intelligence and Security released its report on the proposed introduction of mandatory data retention laws in Australia.[34] The Committee recommended the passing of a data breach notification law for certain telecommunication service providers,[35] a position which had been supported by the Commissioner.[36]

The OAIC and the Commissioner stepped into this contentious environment in 2011. Using the OAIC's power to commence investigations where there is no complaint, if it is deemed 'desirable that the act or practice be investigated',[37] the Commissioner embarked on a number of OMIs into data breach cases.

The *Privacy Act* provides little guidance as to how OMIs are to be conducted. It does provide that the Commissioner must inform the respondent that the matter is to be investigated before commencing the investigation,[38] but is not required to provide the respondent with an opportunity to appear before it unless it proposes to make an adverse determination pursuant to section 52.[39] The Act also specifies that the investigation shall be conducted in private but otherwise 'in such manner as the Commissioner thinks fit'.[40] Accordingly, the Commissioner can determine the process that will be used for investigations and may, for example, make decisions based on a review of relevant documentation without any hearing in person (referred to as an 'on the papers' investigation).[41] The Commissioner has

31 Parliament of Australia, *Privacy Amendment (Privacy Alerts) Bill 2013* (2013) <http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5059>.

32 McMillan and Pilgrim, above n 29.

33 For the current status of the Bill, see Parliament of Australia, *Privacy Amendment (Privacy Alerts) Bill 2014* (16 June 2014) <http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s958>.

34 Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (2015).

35 Ibid [7.128].

36 Timothy Pilgrim, Submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, January 2015, 29–30 [106]–[111] <http://www.oaic.gov.au/news-and-events/submissions/privacy-submissions/submission-on-the-inquiry-into-the-telecommunications-interception-and-access-amendment-data-retention-bill-2014>.

37 *Privacy Act* s 40(2).

38 *Privacy Act* s 43(1).

39 *Privacy Act* s 43(4).

40 *Privacy Act* s 43(2).

41 This is consistent with the general law which provides that if the relevant legislation does not prescribe how the investigation should be conducted, then the regulator may decide on what is appropriate: see generally *Kawicki v Legal Services Commissioner* [2002] NSWSC 1072. The ALRC considered the 'on the papers' approach in its 2008 report: *For Your Information Report*, above n 8, 1644–6 [49.120]–[49.128]. In this report, the ALRC recommended that the Commissioner should be able to direct that a hearing for a determination should proceed without oral submissions from the parties (ie, 'on the papers') if the Commissioner is satisfied that the 'matter could be determined fairly on the basis of written submissions by the parties': at 1646 [49.126].

issued some guidance as to how it will conduct investigations.[42] This guidance is consistent with the general principles for the exercise of regulatory powers, which include that powers should be exercised in a transparent, balanced and vigorous way.[43] It should therefore be expected that the Commissioner's investigations would be conducted in accordance with both the OAIC's published guidance and the general principles for the exercise of regulatory powers. It was on this basis that we examined the six OMIs, as detailed in the methodology below.

A Methodology

Between February 2011 and December 2014, reports from 14 OMIs conducted by the Commissioner were published.[44] This was a greater number than had been published previously over a similar period.[45] They were different to the OMI reports which had been issued previously. The respondent organisations were named for the first time.[46] The final reports were longer[47] and included more background information about the investigation, and a more detailed analysis of the application of the privacy principles. All of the reports culminated with some finding as to whether or not there had been a breach of

42 See above n 10.

43 See, eg, *For Your Information Report*, above n 8, 251 [4.74]; Information Commissioner's Office (UK), *Data Protection Regulatory Action Policy* (United Kingdom Government, Version No 2.0, August 2013) 2; Better Regulation Task Force, *Principles of Good Regulation* (Leaflet, 2003); Mandelkern Group on Better Regulation, *Final Report* (European Commission, 13 November 2001) <http://ec.europa.eu/smart-regulation/better_regulation/documents/mandelkern_report.pdf>.

44 All of the OMI reports published by the OAIC are currently available on the OAIC website: see Office of the Australian Information Commissioner, *Commissioner Initiated Investigation Reports* <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/>.

45 Between 2007 and February 2011, eight OMI reports relating to private sector organisations were published: *Own Motion Investigation v Telecommunications Company* [2010] PrivCmrA 16; *Own Motion Investigation v Information Technology Company* [2010] PrivCmrA 24; *Own Motion Investigation v Airline* [2010] PrivCmrA 12; *Own Motion Investigation v Insurance Company* [2010] PrivCmrA 1; *Own Motion Investigation v Airline* [2009] PrivCmrA 7; *Own Motion Investigation v Medical Centre* [2009] PrivCmrA 6; *Own Motion Investigation v Retailer* [2009] PrivCmrA 25; *Own Motion Investigation v Direct Marketer* [2008] PrivCmrA 23.

46 Rather than using a generic reference for the respondent, eg, *Own Motion Investigation v Medical Centre* [2009] PrivCmrA 6, reports were published naming the respondent. See, eg, Office of the Australian Information Commissioner, *Vodafone Hutchinson Australia: Own Motion Investigation Report* (16 February 2011) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/vodafone-hutchison-australia> ('*Vodafone OMI Report*').

47 Prior to February 2011, the OMI reports had averaged about 500 words. From February 2011 the reports ranged from approximately 1224 words in Office of the Australian Information Commissioner, *Telstra Corporation Limited (Telstra): Own Motion Investigation Report* (7 July 2011) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/telstra-corporation-limited-telstra> ('*Telstra Mail-Out OMI Report*'), to 2438 words in Office of the Australian Information Commissioner, *Sony PlayStation Network/Qriocity: Own Motion Investigation Report* (29 September 2011) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/sony-playstation-network-qriocity> ('*Sony OMI Report*').

privacy principles.[48] All except two reports related to incidents that were in the public domain.[49] All of the reports considered compliance with either NPP 4, or its counterpart applicable to public sector organisations, Information Privacy Principle ('IPP') 4.

Given the change in direction marked by these investigations, and their importance to a more general understanding of the Commissioner's interpretation and application of NPP 4 and IPP 4, we have examined the investigatory procedures adopted in six OMIs conducted in 2011 and 2012. These six investigations were chosen from the eight which had been completed prior to May 2013,[50] when the second of two requests for access to the OAIC's investigation files was made under the *Freedom of Information Act 1982* (Cth) ('*FOI Act*').[51] Access was not requested to all of the eight investigation files so as not to overburden the OAIC. In addition, one of the two cases not considered dealt with a government agency and IPP 4, which was then slightly different to NPP 4, the principle which applied to private sector organisations. The data used for the analysis of the six investigations selected includes the published OMI reports, media releases and statements issued by the OAIC together with information from the OAIC's investigation files obtained as a result of the access requests. The first author also conducted interviews in 2012 with the Commissioner[52] and the Acting Assistant Commissioner Compliance.[53]

Two lenses are used for analysis of these investigations: compliance with the OAIC's own issued guidance; and the transparency, balance and vigour of the use of the investigation power, being general principles for the exercise of regulatory powers. Guidance relevant to the Commissioner's investigations includes both published guidance documents, and information provided in annual reports and other general publications.

---

48 By contrast, with regard to the eight OMIs that considered NPP 4 for which reports were published prior to 2011, the Commissioner was able to conclude in most cases that the respondent was not in breach, even where this required reliance on action taken by the respondent after the incident had occurred: see, eg, *Own Motion Investigation v Medical Centre* [2009] PrivCmrA 6. For an exception to this, see *Own Motion Investigation v Telecommunications Company* [2010] PrivCmrA 16.

49 For the two reports that did not relate to incidents in the public domain, see Office of the Australian Information Commissioner, *Multicard Pty Ltd: Own Motion Investigation Report* (May 2014) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/multicard-omi>; Office of the Australian Information Commissioner, *Professional Services Review Agency: Own Motion Investigation Report* (15 December 2011) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/professional-services-review-agency>.

50 For the two investigations not considered in this article, see Office of the Australian Information Commissioner, *Professional Services Review Agency*, above n 49; Office of the Australian Information Commissioner, *First State Super Trustee Corporation: Own Motion Investigation Report* (June 2012) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/first-state-super-trustee-corporation-own-motion-investigation-report>.

51 The requests were contained in the following: Email from Jodie Siganto to OAIC, 8 September 2011; Email from Jodie Siganto to OAIC, 21 May 2013.

52 Interview with Timothy Pilgrim, Privacy Commissioner (Sydney, 14 December 2012).

53 Interview with Angelene Falk, Acting Assistant Commissioner Compliance, OAIC (Sydney, 14 December 2012).

Although the *Privacy Act* does not specify any criteria for the use of the OMI power, the OAIC has published the risk assessment criteria used by the OAIC in determining which matters to investigate on its own motion.[54] In her interview with the researcher, the Acting Assistant Commissioner Compliance confirmed these criteria, saying that the OAIC's preference is to 'open investigations where there's systemic problems, large numbers of people affected', or where the information revealed 'may have been particularly sensitive'.[55]

Once the decision to commence an investigation has been made, a short fact sheet details how investigations will be handled.[56] Although it has now been withdrawn, the Commissioner also published the *Privacy Complaints Manual*,[57] which provided more detailed information about the OAIC's investigation process, covering both complaint-based investigations and OMIs.[58] According to the fact sheet and the *Privacy Complaints Manual*, once a decision to proceed with an investigation is made, the next steps are to:

1. prepare a case plan that includes identification of the issues in the complaint and the appropriate areas of the Act that may be relevant;
2. send a letter advising the parties about the investigation (referred to in this research as the request for information ('RFI') letters);
3. collect relevant evidence, and then apply the law and relevant policy to the facts of the case; and
4. finalise the case.

Complaint-based investigations are finalised by conciliation, by closing the case on the grounds that there has been no interference with privacy or by making a determination.[59] Fewer options are available to the Commissioner on the finalisation of OMIs.

Prior to March 2014, the Commissioner could report the findings of an OMI involving a public sector agency to the relevant Minister. However, there was no action that the Commissioner could take following an OMI involving a private sector organisation: no determination or other order could be made. This was the case even if the OAIC had determined that an egregious and continuing

54 See, eg, *OAIC 2013 Annual Report*, above n 3, 77; *OAIC 2012 Annual Report*, above n 3, 67–8; Office of the Australian Information Commissioner, *Privacy Complaints Manual*, above n 10; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (Report, March 2005) 155 ('*Getting in on the Act Report*').

55 Interview with Angelene Falk, Acting Assistant Commissioner Compliance, OAIC (Sydney, 14 December 2012).

56 Office of the Australian Information Commissioner, *How Will the OAIC Handle a Privacy Complaint*, above n 10.

57 Office of the Australian Information Commissioner, *Privacy Complaints Manual*, above n 10. No explanation seems to have been provided for the removal of the manual from the OAIC's website.

58 *Getting in on the Act Report*, above n 54, 317–20. These pages contain an information sheet entitled '2001: The Privacy Commissioner's Approach to Promoting Compliance with the *Privacy Act*, which specifies that the OAIC will use the same process in relation to OMIs as for complaint-based investigations: at 318.

59 Office of the Australian Information Commissioner, *How Will the OAIC Handle a Privacy Complaint*, above n 10, 2.

interference with the privacy of Australian citizens was occurring. Following the introduction of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth), the Commissioner was given the power to make a determination at the conclusion of an OMI in the same manner as if the investigation were based on a complaint,[60] in addition to other extended enforcement powers (such as the right to seek civil penalties).[61] The Commissioner can now find fault through an OMI against a covered private sector organisation.

We examined the four main elements of the OAIC investigations as detailed in the guidance issued by the Commission, namely the reasoning behind the decision to undertake an investigation, the collection of evidence, the decision-making process, and the selection of cases for publication of final results. We also examined the OMIs based on established regulatory principles. In its comprehensive review of the *Privacy Act*,[62] the ALRC referred to transparency, balance and vigour as important principles for the exercise of the Commissioner's powers.[63] These principles are also generally consistent with the Commissioner's own guidance in regard to the exercise of its regulatory powers[64] and principles used by the United Kingdom Information Commissioner.[65] We therefore considered the extent to which the six OMIs could also be regarded as representing a transparent, balanced and vigorous use of the OAIC's powers.

B The Six OMIs

Factual details are now provided on the six OMIs examined. They are:

1. Vodafone Hutchinson Australia Own Motion Investigation (February 2011) ('Vodafone OMI');[66]
2. Telstra Corporation Ltd Own Motion Investigation (July 2011) ('Telstra Mail-Out OMI');[67]
3. Sony PlayStation Network/Qriocity Own Motion Investigation (September 2011) ('Sony OMI');[68]

60 *Privacy Act* s 52(1A). For a discussion of the remedies and enforcement options that should be available to the Commissioner following an OMI, see *For Your Information Report*, above n 8, 1650–4 [50.2]–[50.17]. The effect of the Commissioner's lack of enforcement powers on the conduct of investigations is considered further in Part IV below.

61 The Commissioner's increased enforcement powers and their effect on the conduct of investigations is considered further in Part IV below.

62 *For Your Information Report*, above n 8.

63 Ibid [4.74].

64 Office of the Australian Information Commissioner, *Privacy Regulatory Action Policy* (November 2014) <http://www.oaic.gov.au/about-us/corporate-information/privacy-operational/privacy-regulatory-action-policy>.

65 Information Commissioner's Office (UK), *Data Protection Regulatory Action Policy*, above n 43.

66 *Vodafone OMI Report*, above n 46.

67 *Telstra Mail-Out OMI Report*, above n 47.

68 *Sony OMI Report*, above n 47.

4. Telstra Corporation Ltd Own Motion Investigation (June 2012) ('Telstra Bundles OMI');[69]
5. Dell Australia and Epsilon Own Motion Investigation (June 2012) ('Dell/Epsilon OMI');[70] and
6. Medvet Science Pty Ltd Own Motion Investigation (July 2012) ('Medvet OMI').[71]

1 Vodafone OMI

Media reports appeared on 9 January 2011 suggesting that personal details of millions of Vodafone customers (including names, home addresses, drivers' licence numbers and credit card details) were available on the web and 'criminal groups have paid for the private details of some Vodafone customers to blackmail them'.[72] In response to the significant media interest in the incident,[73] the Commissioner commenced an OMI in early January 2011.[74] This investigation was completed in around five weeks. The Commissioner found that the information was not part of a public website as had been reported,[75] and found no evidence of any unauthorised disclosure. Accordingly, Vodafone was found not to have breached NPP 2[76] – which applied to how organisations might use or disclose personal information – but to have breached NPP 4 by failing to take reasonable steps to protect information.[77]

---

69 Office of the Australian Information Commissioner, *Telstra Corporation Limited: Own Motion Investigation Report* (June 2012) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/telstra-corporation-limited> ('*Telstra Bundles OMI Report*').

70 Office of the Australian Information Commissioner, *Dell Australia and Epsilon: Own Motion Investigation Report* (June 2012) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/dell-australia-and-epsilon> ('*Dell/Epsilon OMI Report*').

71 Office of the Australian Information Commissioner, *Medvet Science Pty Ltd: Own Motion Investigation Report* (July 2012) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/medvet-science-pty-ltd-own-motion-investigation-report> ('*Medvet OMI Report*').

72 AAP, 'Vodafone Mobile Records Leaked onto the Internet', *The Courier Mail* (Brisbane), 9 January 2011 <http://www.couriermail.com.au/business/vodafone-mobile-records-leaked-onto-the-internet/story-e6freonx-1225984387960>; Natalie O'Brien, 'Mobile Security Outrage: Private Details Accessible on Net', *The Sydney Morning Herald* (online), 9 January 2011 <http://www.smh.com.au/technology/security/mobile-security-outrage-private-details-accessible-on-net-20110108-19j9j.html>.

73 See, eg, Peter Martin and Lucy Battersby, 'Vodafone May Be Liable on Privacy Breach', *The Sydney Morning Herald* (online), 10 January 2011 <http://www.smh.com.au/technology/security/vodafone-may-be-liable-on-privacy-breach-20110109-19jup.html>.

74 The OMI report states that the Commissioner opened the investigation 'in response to media reports that the personal information of Vodafone Hutchison Australia (Vodafone) customers had been compromised': *Vodafone OMI Report*, above n 46.

75 Ibid.

76 NPP 2 provided, among other things, that 'an organisation must not use or disclose personal information … for a purpose … other than the primary purpose of collection' other than in certain specified circumstances.

77 *Vodafone OMI Report*, above n 46.

2 *Telstra Mail-Out OMI*

In October 2011, an incorrect mail merge resulted in 220 000 letters explaining upcoming price changes being sent to Telstra customers, which contained the names, phone numbers and telephone plans of customers other than the recipients of the letters.[78] The OMI report noted that the Commissioner opened the case following receipt of a notification letter from Telstra.[79] However, the incident was already in the media at the time,[80] and Telstra had earlier reported the incident to the Australian Communications and Media Authority ('ACMA'), which also notified the OAIC.[81] The OAIC opened its investigation in late October 2010[82] and closed it by a letter to Telstra on 16 May 2011, confirming the OAIC's view that there had been a breach of NPP 2 but no breach of NPP 4.[83] An OMI report that was published in July 2011 concluded the breach was a one-off human error, and as such did not mean that Telstra had failed to comply with its obligations under NPP 4.[84]

3 *Sony OMI*

Following extensive media reporting of an attack on the Sony PlayStation Network ('PSN') resulting in the compromise of information in relation to approximately 77 million PSN customers around the world,[85] the OAIC commenced an investigation in April 2011.[86] The investigation was effectively concluded in late June when the OAIC sent a draft closing letter and OMI report

78 *Telstra Mail-Out OMI Report*, above n 47.

79 Ibid.

80 See Asher Moses, 'Telstra Botched Mail-Out Exposes 220 000 Customers', *The Sydney Morning Herald* (online), 27 October 2010 <http://www.smh.com.au/technology/security/telstra-botched-mailout-exposes-220000-customers-20101027-173du.html#ixzz2hC0Ak7np>; 'Massive Telstra Bungle a Privacy Breach', *News.com.au* (online), 27 October 2010 <http://www.news.com.au/business/massive-telstra-bungle-a-privacy-breach/story-e6frfm1i-1225944346111>.

81 Letter from Jane van Beelen to Olya Booyar, ACMA, 27 October 2010, which refers to 'your letter of 26 October 2010 … requesting further information about this matter'.

82 Letter from Timothy Pilgrim to Helen Lewin, 28 October 2010 ('*Telstra Mail-Out RFI Letter*').

83 Letter from Mark Hummerston to Helen Lewin, 16 May 2011 ('*Telstra Mail-Out Close Letter*').

84 *Telstra Mail-Out OMI Report*, above n 47.

85 See, eg, Chris Griffith, 'Breach Sparks Security Alert: Call for Laws To Protect against PlayStation-Style Attacks', *The Australian* (online), 3 May 2011 <http://www.theaustralian.com.au/business/technology/breach-sparks-security-alert-call-for-laws-to-protect-against-playstation-style-attacks/story-e6frgakx-1226048705602>; 'Sony Bows Head over PlayStation Security Breach' *The Sydney Morning Herald* (online), 2 May 2011 <http://www.smh.com.au/technology/security/sony-bows-head-over-playstation-security-breach-20110502-1e3m5.html#ixzz2g95KsFNE>.

86 Letter from Timothy Pilgrim to Managing Director, Sony, 27 April 2011 ('*Sony RFI Letter*'). *Sony OMI Report*, above n 47, refers to the investigation being commenced 'following media reports'. The investigation also included copies of two media reports: Asher Moses, 'PlayStation Hacking Scandal: Police Chief Says Contact Your Bank Now', *The Sydney Morning Herald* (online), 27 April 2001 <http://www.smh.com.au/digital-life/games/playstation-hacking-scandal-police-chief-says-contact-your-bank-now-20110427-1dvts.html>; 'PlayStation Privacy Breach: 77 Million Customer Accounts Exposed', *The Sydney Morning Herald* (online), 27 April 2011 <http://www.smh.com.au/digital-life/games/playstation-privacy-breach-77-million-customer-accounts-exposed-20110426-1dvhf.html>.

to Sony Australia for their review.[87] Further communication ensued regarding the application of the *Privacy Act*, in particular whether the Sony Australian entity had collected or held any personal information.[88] These issues were finalised by the end of September 2011,[89] when the OAIC issued a report together with a media release.[90] No evidence of any unauthorised disclosure was found, because there was no positive act of disclosure by Sony.[91] The report also found that Sony had taken reasonable steps to secure the personal information for the purposes of NPP 4 and therefore did not breach the security principle.

4 Telstra Bundles OMI

On 9 December 2011, a user of the popular Australian internet forum, Whirlpool, discovered that he could access an internal Telstra tool (called the 'visibility tool')[92] that enabled access to information including billing account numbers, first and last names, and notes about accounts such as usernames and passwords for over 734 000 Telstra account holders.[93] The Commissioner opened an OMI on 12 December 2011. An exchange of letters between the OAIC and Telstra followed regarding the incident and the remediation steps undertaken.[94] The OAIC closed the investigation in April 2012.[95] In the final OMI report issued in July 2012 together with a media release,[96] Telstra was found to have breached both NPP 2 and NPP 4. The OAIC concluded that although Telstra had existing policies and procedures in place that, if followed, would have prevented the

87 Email from OAIC to Sony, 29 June 2011. This email enclosed a draft OMI report, and had as its header 'FINAL Sony 1 Own Motion Investigation Report June 2011'.

88 Email from Sony to OAIC staff, 8 July 2011. This email came with attachments, including an OAIC draft report and draft close letter from the Commissioner with amendments suggested by Sony Computer Entertainment Europe ('SCEE'). According to the published *Sony OMI Report*, above n 47, SCEE is the data controller for the PSN/Qriocity personal data, and is the entity that had collected the personal information of Australians.

89 Letter from Timothy Pilgrim to Managing Director, Sony, 29 September 2011 ('*Sony Close Letter*').

90 *Sony OMI Report*, above n 47; Office of the Australian Information Commissioner, 'Australian Privacy Commissioner Concludes Sony Investigation' (Media Release, 29 September 2011) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/australian-privacy-commissioner-concludes-sony-investigation>.

91 *Sony OMI Report*, above n 47.

92 See, eg, Asher Moses and Ben Grubb, 'Telstra Customer Database Exposed', *The Sydney Morning Herald* (online), 9 December 2011 <http://www.smh.com.au/it-pro/security-it/telstra-customer-database-exposed-20111209-1on60.html>.

93 WireFire, 'Our Best Ever Cable Broadband Deal' on *Whirlpool Forum* (9 December 2011) <http://forums.whirlpool.net.au/forum-replies.cfm?t=1801978&p=27#r533>; Asher Moses, 'Telstra's 734 000 Account Privacy Blunder Breached Multiple Laws: Regulators', *The Age* (online), 29 June 2012 <http://www.theage.com.au/it-pro/security-it/telstras-734000-account-privacy-blunder-breached-multiple-laws-regulators-20120629-2165z.html>.

94 Email from Telstra to Timothy Pilgrim, OAIC, 9 December 2011; Letter from Mark Hummerston, Assistant Commissioner Compliance, OAIC, to Telstra, 12 December 2011 ('*Telstra Bundles RFI Letter*'); Office of the Australian Information Commissioner, *File Note* (29 March 2012).

95 Email thread from TJ, OAIC, to Telstra, 30 April 2012 ('*Telstra Bundles Close Letter*').

96 Office of the Australian Privacy Commissioner, 'Telstra Breaches *Privacy Act*' (Media Release, 29 June 2012) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/telstra-breaches-privacy-act>.

errors which led to this incident, there was evidence of behaviours not consistent with those policies and procedures.[97]

5 Dell/Epsilon OMI

Epsilon, a US company, provided email marketing services for Dell Australia. In March 2011, the names and email addresses of customers of over 60 Epsilon client companies including Dell Australia were accessed following a malware attack.[98] Following receipt of notice of the breach from Epsilon, Dell Australia notified its customers and the Commissioner.[99] In April 2011, the OAIC opened separate investigations into Dell Australia and Epsilon.[100] Dell Australia advised that it had completed a 'high level offsite security assessment' of some part of Epsilon's infrastructure but had not been able to undertake any other audit as 'the incident [was] still under investigation by law enforcement authorities in the United States'.[101] In response to its separate RFI letter,[102] Epsilon provided a copy of the investigative report prepared for it by Verizon Business Services/Cybertrust in mid-November 2011.[103] Both the Dell Australia and Epsilon investigations were closed in January 2012,[104] and drafts of the OMI report were sent in July 2012.[105] The final OMI report published in July 2012 only considers whether there was a breach of NPP 4 (and not of NPP 2), concluding that both Dell and Epsilon had taken sufficient security measures for the purposes of NPP 4.[106]

6 Medvet OMI

The final OMI involved Medvet, a private company owned by the South Australian ('SA') Government,[107] which offered a range of testing services including online ordering of drug and DNA self-testing kits which could be

97 *Telstra Bundles OMI Report*, above n 69.

98 Taken from the facts referred to in *Dell/Epsilon OMI Report*, above n 70. See also Prepared Statement to House Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing and Trade, US House of Representatives, 2 June 2011, 13 (Jeanette Fitzgerald, General Counsel, Epsilon Data Management LLC).

99 Email from Dell to OAIC, 6 April 2011; Letter from Dell to Timothy Pilgrim, 6 April 2011.

100 Letter from Mark Hummerston, OAIC, to Dell, 19 April 2011 ('*Dell RFI Letter*'). Email from MS, OAIC, to Epsilon; Letter from OAIC staff to Epsilon, 29 April 2011 ('*Epsilon RFI Letter*').

101 Email from Dell to MS, OAIC, 19 July 2011.

102 *Epsilon RFI Letter*, above n 100.

103 Email thread from Epsilon to AM, OAIC, 15 November 2011.

104 Letter from OAIC staff to Dell, 11 January 2012 ('*Dell Close Letter*'); Email thread from AM, OAIC, to Epsilon, 11 January 2012 ('*Epsilon Close Letter*').

105 Letter from OAIC staff to Dell, July 2012. Letter from OAIC staff to Epsilon, 2 July 2012.

106 As in the Sony investigation, jurisdictional issues were raised in *Dell/Epsilon OMI Report*, above n 70. In this case, the issues were in regard to the application of the *Privacy Act* to Epsilon (being a US incorporated organisation, and arguably not carrying on business in Australia). As in the Sony investigation, because the Commissioner was satisfied that Epsilon had met its obligations under the NPPs, the Commissioner was not required to reach a formal view on this matter.

107 Medvet, *About Us* <http://www.medvet.com.au/about-us>.

delivered directly to a nominated shipping address.[108] In July 2011, it was reported that information relating to orders received by Medvet was available online.[109] An OMI investigation was opened on 18 July 2011.[110] In response to the Commissioner's request for information,[111] Medvet provided a copy of a report into the incident prepared by Deloitte on behalf of SA Health.[112] A further report on the implementation of corrective actions recommended by Deloitte was also provided to the OAIC around 5 December 2011.[113]

A closing letter was sent to Medvet on 19 December 2011, in which Medvet was found to be in breach of NPP 4.[114] Medvet was also advised that, in light of the security measures being implemented, the OAIC would cease the investigation and the file on this matter was 'now closed'. Nearly five months later, in May 2012, a draft OMI report was prepared and sent to Medvet for comment.[115] Although there is no reference to any further interaction between the OAIC and Medvet in the investigation file, in July 2012 the Commissioner advised Medvet that, 'as it was aware,' the Commissioner had reviewed the file and as part of that review had now determined that there was a breach of NPP 2, as well as NPP 4.[116] The reasons for this change in position are redacted in full. The findings of breach of both NPP 4 and NPP 2 are reflected in the OMI report published on the OAIC website on 26 July 2012 (which are quite different to the findings first communicated in the closing letter sent to Medvet in December 2011, and probably included in the draft OMI report sent in May 2012).[117]

---

108 For consideration of the Commissioner's approach in medical privacy cases, see Bruce Arnold, 'Open Doors: Recent Medical Privacy Incidents' (2011) 8 *Privacy Law Bulletin* 26.

109 See, eg, Hedley Thomas, 'DNA Test Names Exposed Online', *The Australian* (online), 16 July 2011 <http://www.theaustralian.com.au/news/health-science/dna-test-names-exposed-online/story-e6frg8y6-1226095576596>; Sarah Martin 'Investigation into South Australia's Medvet Lab after Serious Privacy Breach', *News.com.au* (online), 18 July 2011 <http://www.news.com.au/national-old/south-australias-medvet-blood-lab-publishes-details-of-paternity-and-drug-test-applicants/story-e6frfkx9-1226096476780>; 'Online Medical Privacy Breach To Be Probed', *ABC News* (online), 18 July 2011 <http://www.abc.net.au/news/2011-07-18/medvet-privacy-breach-online/2798650>.

110 Office of the Australian Information Commissioner, 'Case Management Summary: Medvet Laboratories' (20 June 2013) ('*Medvet Case Management Summary*'), attached to Letter from OAIC staff to Jodie Siganto, 30 August 2013.

111 Letter from Timothy Pilgrim to Medvet, 20 July 2011 ('*Medvet RFI Letter*').

112 Email from Medvet to AM, OAIC, 21 September 2011. The Deloitte report is not included as an attachment to this email thread (and was not disclosed). The report is not referred to in any other correspondence.

113 The records refer to Letter from Managing Director, Medvet, to OAIC, 28 November 2011, which may have included the implementation report, but this has been redacted.

114 Letter from OAIC staff, Assistant Commissioner, OAIC, to CEO, Medvet, 19 December 2011 ('*Medvet Close Letter 1*').

115 Email from KO, OAIC, to Medvet, 15 May 2012 (with attachments including a covering letter and a draft Medvet OMI investigation report); Letter from Mark Hummerston, Assistance Commissioner Compliance, OAIC, to Medvet, 15 May 2012.

116 Letter from Timothy Pilgrim, Privacy Commissioner to CEO, Medvet, 10 July 2012 ('*Medvet Close Letter 2*').

117 *Medvet OMI Report*, above n 71.

III ANALYSIS OF INVESTIGATORY PROCEDURES

In this Part, we detail our examination of the six OMIs with particular focus on the reasoning behind the decision to undertake an investigation, the process of evidence collection, the decision-making process adopted and the reasoning for publication of final results in an OMI report.

A Decision To Undertake Investigation

The OAIC's guidance indicates that the criteria to be used for the selection of OMIs include consideration of systemic problems, whether large numbers of people are affected, and whether particularly sensitive information might have been revealed.[118] However, none of the files for the OMIs contain any record of or reference to consideration of these elements as the basis for opening the investigation.[119]

The Acting Assistant Commissioner Compliance referred to another two reasons for commencing an OMI.[120]

The first reason was where the OAIC was notified of a data breach. In that case, the office would determine if the organisation had a strategy in place to address the breach. If satisfied that appropriate steps were being taken, then the OAIC would not take any further action, although it would seek to have the organisation report on the remedial steps taken. However, 'if the report falls short in [their] view then at that point [they would] open an Own Motion Investigation and ask some formal questions under [their] Own Motion Investigation power'.[121]

Telstra Mail-Out, Sony, Dell/Epsilon and Telstra Bundles were OMIs where the organisation notified the OAIC of a breach.[122] However, there is no indication in any of the files or the reports that the Commissioner was concerned that the organisations might not take appropriate remedial steps to recover from the breach. To the contrary, each report refers approvingly to the post-breach actions taken by the respondent. For example, the conclusion to the *Sony OMI Report* provides: 'The Privacy Commissioner was also satisfied with how the incident was dealt with following the breach in terms of the extra security measures that have been implemented to help protect personal information'.[123]

The second reason for instigating an OMI was in response to media interest. This seems to have been the most likely reason for the commencement of

118 See, eg, *OAIC 2012 Annual Report*, above n 3, 62–3; *OAIC 2013 Annual Report*, above n 3.

119 The Telstra Mail-Out investigation was in part the result of a referral from ACMA: Letter from Telstra to Olya Booyar, ACMA, 27 October 2010, a copy of which was included in the OAIC's investigation file.

120 Interview with Angelene Falk, Acting Assistant Commissioner Compliance, OAIC (Sydney, 14 December 2012).

121 Ibid.

122 See Letter from Telstra to Timothy Pilgrim, 27 October 2010; Letter from Dell Australia to Timothy Pilgrim, 6 April 2011; Email from Sony to Enquiries, OAIC, 27 April 2011; Email from Telstra to OAIC, 9 December 2011.

123 *Sony OMI Report*, above n 47.

investigations in all six cases as each incident received media attention.[124] Furthermore, all six investigation files contain media clippings about the incident being investigated, which certainly demonstrates that the OAIC was acutely aware of media attention.[125] The Vodafone, Sony and Medvet OMI reports all identify media as the reason for opening the investigations.[126] By way of example, the first paragraph of the *Vodafone OMI Report* provides: 'The Australian Privacy Commissioner, Timothy Pilgrim opened an own motion investigation … in response to media reports that the personal information of Vodafone Hutchison Australia (Vodafone) customers had been compromised'.[127]

Unlike previous OMIs, the Commissioner elected to respond to the media reports, not only by opening an investigation, but also in a number of cases by issuing its own media release. This approach was adopted on the commencement of the Vodafone, Sony and Telstra Bundles OMIs.[128] Even in those cases where no media release was issued, the fact that the Commissioner was undertaking an

124 See, eg, Moses, 'Telstra Botched Mail-Out Exposes 220 000 Customers', above n 80; 'Massive Telstra Bungle a Privacy Breach', above n 80; O'Brien, above n 72; Peter Martin and Lucy Battersby, 'Vodafone May Be Liable on Privacy Breach', *The Sydney Morning Herald* (online), 10 January 2011 <http://www.smh.com.au/technology/security/vodafone-may-be-liable-on-privacy-breach-20110109-19jup.html>; Liana Baker, 'Sony PlayStation Suffers Massive Data Breach', *Reuters* (online), 26 April 2011 <http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426>; Thomas, 'DNA Test Names Exposed Online', above n 109.

125 See, eg, the Dell investigation file which included excerpts from the following: Fahmida Y Rashid, *Epsilon Data Breach Highlights Cloud-Computing Security Concerns* (6 April 2011) eWEEK <http://www.eweek.com/c/a/Security/Epsilon-Data-Breach-Highlights-Cloud-Computing-Security-Concerns-637161>; Karen Dearne, 'Epsilon Email Security Breach Widens', *The Australian* (online), 7 April 2011 <http://www.theaustralian.com.au/business/technology/epsilon-email-security-breach-widens/story-e6frgakx-1226035279855>; Asher Moses, 'Dell Australia Customer Details Stolen in Major Global Data Breach', *Technology*, *The Sydney Morning Herald* (online), 7 April 2011 <http://www.smh.com.au/technology/security/dell-australia-customer-details-stolen-in-major-global-data-breach-20110407-1d4yd.html>. These were attached to Letter from OAIC staff to Jodie Siganto, 30 August 2013. The Telstra Bundles investigation file included an excerpt from Asher Moses and Ben Grubb, 'Telstra Customer Database Exposed', *The Age* (online), 9 December 2011 <http://www.theage.com.au/it-pro/security-it/telstra-customer-database-exposed-20111209-1on60.html>. This was attached to Letter from OAIC staff to Jodie Siganto, 30 August 2013.

126 *Vodafone OMI Report*, above n 46; *Sony OMI Report*, above n 47; *Medvet OMI Report*, above n 71.

127 Office of the Australian Information Commissioner, *Vodafone OMI Report*, above n 46.

128 Timothy Pilgrim, 'Privacy Commissioner Opens Investigation into Telstra Customer Accounts Data Breach' (Statement, 12 December 2011) <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/telstra-data-breach/privacy-commissioner-opens-investigation-into-telstra-customer-accounts-data-breach-statement-from-australian-privacy-commissioner-tim>; Office of the Australian Information Commissioner, 'Australian Privacy Commissioner To Investigate Vodafone Allegations' (Media Release, 10 January 2011) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/australian-privacy-commissioner-to-investigate-vodafone-allegations>; Timothy Pilgrim, 'Investigation into Sony Data Breach (Statement, 4 May 2011) <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/sony-playstation-network/investigation-into-sony-data-breach-4-may-2011>.

investigation seemed to find its way into the public domain.[129] The Commissioner also responded to media queries about whether an investigation was being undertaken[130] and to further queries as the investigation proceeded.[131] The OAIC's continuing awareness of the ongoing media interest in the investigations is confirmed by copies of news articles held in the investigation files.[132] Specific reference to media interest was made in correspondence between the OAIC and the respondents in the Telstra Mail-Out, Vodafone and Sony investigations.[133] The OAIC also issued media releases[134] or a statement[135] on the publication of each of the OMI reports other than Dell/Epsilon.

The relationship between media coverage and the conduct of an OMI is an important consideration as it provides an insight into why these investigations were undertaken. We contend that the combination of a notification about a significant data breach and subsequent media interest appears to be the main determinant of whether an OMI was conducted in these six incidents. In fact, none of the investigation files or reports of the six OMIs contain any record of or reference to consideration of systemic issues, or any of the other criteria which the OAIC has publicly advised that it refers to when determining whether or not

129 See, eg, Hedley Thomas, 'Privacy Data Still Online 24 Hours after Alert', *The Australian* (online), 18 July 2011 <http://www.theaustralian.com.au/national-affairs/private-data-still-online-24-hours-after-alert/story-fn59niix-1226096403027#sthash.aUOZR0cJ.dpuf>, which provides that the 'Privacy Commissioner Timothy Pilgrim will investigate Medvet's original internet security breach and the subsequent failure of the company to immediately remove the hundreds of customers' orders that it knew were cached by Google and online'.

130 See, eg, Karen Dearne, 'Privacy Czar To Investigate Epsilon Email Breach', *The Australian* (online), 7 April 2011 <http://www.theaustralian.com.au/technology/privacy-czar-to-investigate-epsilon-email-breach/story-e6frgakx-1226035569602#sthash.w4iypq2o.dpuf>; Moses, 'Telstra Botched Mail-Out Exposes 220 000 Customers', above n 80.

131 See, eg, Internal email thread, OAIC, 5 May 2011.

132 See, eg, excerpts from articles dated 2–3 May 2011 on *The Sydney Morning Herald*'s website, which were attached to Letter from OAIC staff to Jodie Siganto, 30 August 2013.

133 See, eg, Email from OAIC to Timothy Pilgrim, 24 May 2011, which states: 'spoke to [redacted] yesterday. I confirmed we would be making a media statement accompanied by a short report upon closing the investigation'.

134 Office of the Australian Information Commissioner, 'OAIC Finalises Investigation into Telstra Mailing List Error' (Media Release, 11 October 2011) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/oaic-finalises-investigation-into-telstra-mailing-list-error>; Office of the Australian Information Commissioner, 'Privacy Commissioner Releases Vodafone Findings' (Media Release, 16 February 2011) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/privacy-commissioner-releases-vodafone-findings>; Office of the Australian Information Commissioner, 'Australian Privacy Commissioner Concludes Sony Investigation' (Media Release, 29 September 2011) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/australian-privacy-commissioner-concludes-sony-investigation>; Office of the Australian Information Commissioner, 'Telstra Breaches *Privacy Act*', above n 96.

135 In the Medvet investigation, a statement was released following negative coverage of the report in the press: Office of the Australian Information Commissioner, 'Privacy Commissioner Responds to Media Claims about Medvet Investigation – Letter to the Editor of *The Australian* Newspaper from Australian Privacy Commissioner, Timothy Pilgrim' (Statement, 26 July 2012) <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/medvet-investigation/privacy-commissioner-responds-to-media-claims-about-medvet-investigation>.

to commence an OMI.[136] It would therefore seem that the decision to commence an OMI in the period under examination was heavily influenced by media coverage rather than other stated regulatory aims of the OAIC.

B Collection of Evidence

Once the decision was made to commence an OMI, a file was set up and a pro forma complaint assessment sheet completed.[137] According to the *Privacy Complaints Manual*, a case plan should also be prepared.[138] That case plan should identify the issues raised by the complaint, the relevant privacy principles that may have been breached and the information or evidence needed to establish whether there has been a breach of privacy.[139]

We question whether the OAIC is following its own procedures in relation to investigations. Our research revealed that there was no evidence of any case plan in any of the six investigation files. It could be that the case plan was not included in the disclosed papers following the freedom of information ('FOI') process. However, if that is the case it would be difficult to see why, given that the case plan is unlikely to be relevant to the exemptions put forward by the OAIC for redacting information.[140]

It would seem that the first step adopted in each of the OMIs was to issue a letter in a fairly standard form to each of the respondents. This letter advised the

---

136 There is a single reference to systemic issues in a letter sent to Telstra asking for more information about the breach, which states that the incident 'indicates that there may be systemic issues within the Telstra systems with regard to data security': Letter from OAIC staff to Telstra, 8 March 2012. No further reference is made to systemic issues in the files or in any of the reports. However, following the release of the *Telstra Bundles OMI Report*, the Commissioner was reported to be watching for systemic privacy weaknesses in Telstra's operational culture: see Andrew Colley, 'Privacy Commissioner Timothy Pilgrim Will Probe Telstra's Culture in Light of Privacy Breach', *The Australian* (online), 29 June 2012 <http://www.theaustralian.com.au/australian-it/telecommunications/privacy-commissioner-timothy-pilgrim-will-probe-telstras-culture-in-light-of-privacy-breach/story-fn4iyzsr-1226412092746>. It is not clear what this reference to the Commissioner's interest in possible systemic issues in the media report was based on. The media release accompanying the release of the *Telstra Bundles OMI Report* contains no reference to systemic issues.

137 Complaint assessment sheets were disclosed for all of the OMIs except the Epsilon and Telstra Mail-Out OMIs. See the attachments to Letter from Caren Whip to Jodie Siganto, 30 August 2013: Office of the Australian Information Commissioner, *Complaint Assessment Sheet* (10 January 2011); Office of the Australian Information Commissioner, *Complaint Assessment Sheet* (27 April 2011); Office of the Australian Information Commissioner, *Complaint Assessment Sheet – OMI* (6 April 2011); Office of the Australian Information Commissioner *Complaint Assessment Sheet* (12 December 2011); Office of the Australian Information Commissioner, *Complaint Assessment Sheet* (19 July 2011).

138 Office of the Australian Information Commissioner, *Privacy Complaints Manual*, above n 10, 33.

139 In determining what information or evidence may be required, the *Privacy Complaints Manual* provides that consideration should be given to any evidence to hand in relation to the allegations, which identifies what information or evidence is still needed: Office of the Australian Information Commissioner, *Privacy Complaints Manual*, above n 10, 33.

140 The reasons for exempting records from disclosure pursuant to the authors' request for access included that the records formed part of the deliberative process pursuant to *FOI Act* s 47C(1) would have a substantial adverse effect on the operations of the agency pursuant to s 47E(d), or would unreasonably affect the organisation in respect of its lawful business, commercial or financial affairs or prejudice the future supply of information to the agency pursuant to s 47G(1).

respondents of the allegations, the possible outcome of the OMI and asked for a response to a series of questions related to the allegations within a specified period of time.[141] Almost identical RFI letters were used in the Telstra Mail-Out, Vodafone, Sony and Medvet OMIs.[142] This is notwithstanding that the incidents being investigated were very different in terms of the source of the compromise, the way the compromise had been effected, the risk profile of the organisations under consideration, the type of information compromised and the extent of and potential harm resulting from the possible breach. If consideration had been given to some of these relevant contextual issues, it might be expected that different questions would have been posed directed towards seeking different information that would have been pertinent to a particular breach. Instead, a standard form letter was used which seems to demonstrate a failure to appreciate the contextual complexities of data breach incidents.

In contrast, the Dell Australia, Epsilon and Telstra Bundles RFI letters indicated some customisation of questions in view of the particular issues raised by those incidents, although in different ways. Of the three,[143] Dell Australia's RFI letter was perhaps the most problematic as it asked only two questions of the respondents. First, it asked what steps Dell Australia had taken to protect information in order to comply with NPP 4.1.[144] Secondly, whether Dell Australia had protected personal information it provided to third parties and asked for 'full details of any contractual measures in place to ensure that third parties also take reasonable steps to comply with NPP 4.1 and reference any relevant industry standards'.[145] The fact that Dell Australia had entered into a contract with Epsilon and was pursuing an investigation to determine whether Epsilon had complied with relevant standards, presumably in accordance with its contractual commitments, was likely communicated by Dell to the OAIC in its initial contact on 6 April 2011.[146] Dell's provision of contractual information then seems to have been used by the OAIC as the investigatory framework for the RFI letter. In essence, Dell's initial contact appears to have shaped the nature of the OAIC's

141 RFI letters for all of the investigations were disclosed*: Telstra Mail-Out RFI Letter*, above n 82; Letter from Timothy Pilgrim to Vodafone, 10 January 2011 ('*Vodafone RFI Letter*'); *Sony RFI Letter*, above n 86; *Dell RFI Letter*, above n 100; *Epsilon RFI Letter*, above n 100; *Telstra Bundles RFI Letter*, above n 94; *Medvet RFI Letter*, above n 111.

142 *Telstra Mail-Out RFI Letter*, above n 82; *Vodafone RFI Letter*, above n 141; *Sony RFI Letter*, above n 86; *Medvet RFI Letter*, above n 111.

143 The *Epsilon RFI Letter*, above n 100, contained questions similar to the *Dell RFI Letter*, above n 100, and the earlier RFI letters. The *Telstra Bundles RFI Letter*, above n 94, raised similar questions to the earlier letters although in different terms and was specifically directed to the database which had been accessible.

144 *Dell RFI Letter*, above n 100.

145 Ibid.

146 Although this is not clear from the file, an internal OAIC email refers to a phone conversation in which Dell had advised the OAIC that 'Epsilon … holds customer data for Dell [words exempted on basis of *FOI Act* ss 47C, 47G] … Epsilon has engaged [words exempted on basis of *FOI* ss 47C, 47G] to investigate the breach. … Dell indicated it would provide a final report': Email from OAIC to Timothy Pilgrim, 6 April 2011. It is likely that the first redaction referred to the contractual terms between the organisations: see Email thread from Dell to OAIC, 6 April 2011.

investigation which is of particular relevance given the absence of any second round of questioning by the OAIC considered further below.

The files reveal that once RFI letters are responded to, the OAIC considers the adequacy and weight of the evidence provided, and whether any additional evidence is required to support the OAIC's decision-making process. This assessment of the processes adopted in the files is consistent with the interview conducted with the Acting Assistant Commissioner Compliance, who confirmed that the investigation process is 'primarily a paper based investigation … in terms of asking a series of questions and then analysing the information that's returned to us'.[147]

An analysis of the different types of records disclosed from the OAIC's investigation files supports the proposition that each investigation is conducted 'on the papers' and largely via email and letter. There are few phone calls or meetings recorded between the OAIC and the respondents.[148] There is no evidence of the Commissioner requesting that any respondent provide verbal evidence. Investigators from the OAIC do not appear to have visited the offices or any other premises of the respondents or even met with respondents in person; the exception being a visit by the OAIC to the Vodafone office after the conclusion of the OMI to watch a demonstration of Vodafone's new online learning system.[149] Moreover, there is no indication that the OAIC provided any respondent or party with the opportunity to appear before it, or that any party requested to do so.[150]

The adoption of this pure 'on the papers' approach is important here because the OAIC does actually have powers under sections 43 and 44 of the *Privacy Act* to 'obtain information from such persons, and make such inquiries, as he or she thinks fit',[151] to require the production of any 'information or a document [the Commissioner has reason to believe is] relevant to an investigation'[152] and to require a person to 'attend before the Commissioner at a time and place specified in the notice to answer questions relevant to the investigation'.[153] During an interview, the Commissioner confirmed that these investigatory powers had been used 'frequently and for various reasons' although mostly as a consequence of internal governance requirements applicable where respondents have been being asked to provide information.[154] If not statutorily required, those respondents may

147 Interview with Angelene Falk, Acting Assistant Commissioner Compliance, OAIC (Sydney, 14 December 2012).

148 There is reference to a teleconference with Telstra, but that appears to have been limited to discussion of Telstra's report on the Telstra Bundles investigation, rather than separate testing of the assertions from that report.

149 Internal email thread, OAIC, 7 September 2011.

150 In the Telstra Mail-Out investigation, Telstra objected to the findings in *Telstra Mail-Out Close Letter*, above n 83, on the basis, inter alia, that it had not be given the opportunity to be heard: Email from Telstra to OAIC, 26 May 2011. It is not clear what happened to this objection.

151 *Privacy Act* s 43(3).

152 *Privacy Act* s 44(1).

153 *Privacy Act* s 44(3).

154 Interview with Timothy Pilgrim, Privacy Commissioner (Sydney, 14 December 2012).

be in breach of other laws if they provided information without a formal statute-based request.[155]

However, we can find no evidence in any of the six OMIs regarding the use by the OAIC of its powers under sections 43 and 44 of the *Privacy Act*. The use of these powers was considered in the Telstra Bundles investigation during an email exchange between the OAIC and Telstra. The OAIC advised Telstra that if it did not provide a report by 30 March 2013 (Telstra having previously said that it would be able to report on the incident that occurred in mid-December by late January), then the Commissioner would 'issue a notice compelling Telstra to respond by way of a senior executive being required to appear before the Commissioner and answer questions'.[156] This is the only situation where the threat of such powers, rather than the use of these powers, was adopted.

We contend that the Dell/Epsilon investigation was an incident where the OAIC may have used its powers to secure evidence that the respondent was unwilling to provide. In that case, Dell had advised that it would undertake a security audit in response to the incident.[157] The OAIC followed this up in July, requesting a copy of that audit report.[158] Dell declined and responded that it had 'recently completed a high-level off-site security risk assessment' and confirmed that the assessment indicated that Epsilon had 'met relevant industry and data security standards'.[159] Dell argued that the report 'contains confidential information that relates to Epsilon's information security systems that contractually Dell cannot disclose to the OAIC'.[160] Dell further suggested that the OAIC should contact Epsilon itself because 'Epsilon will have detailed information on its own internal information security systems and procedures'.[161]

It seems unlikely that Dell's confidentiality obligations would have sufficed to avoid compliance with lawful requests by local regulators for the provision of documents or information. In any case, the OAIC could have entered into some sort of confidentiality arrangement with Dell to reassure it that it would not have been in breach of its contractual obligations to Epsilon.[162] It is quite astonishing to us that a corporation can claim confidentiality founded on a pre-existing contractual obligation and that is sufficient to deter a regulatory investigation into a serious and significant data breach. Yet, there is no evidence from the Dell/Epsilon investigation file that the OAIC considered issuing Dell with a request to produce the information pursuant to the section 43 or 44 powers. In fact, it does not appear that the OAIC pressed Dell for the disclosure of Dell's

155 Ibid.
156 Email from OAIC to Telstra, 15 March 2012.
157 This is apparent from the reference to the security audit to be undertaken in the Email from OAIC to Dell, 1 July 2011.
158 Email thread between OAIC and Dell, 5 July 2011.
159 Email from Dell to OAIC, 19 July 2011.
160 Email from Dell to MS, OAIC, 19 July 2011.
161 Ibid.
162 In regard to the release of Epsilon's own investigation report, Epsilon secured appropriate confidentiality undertakings from the OAIC prior to providing a copy of that report.

report in any way whatsoever. It also does not appear that the OAIC asked for or obtained a copy of Dell's assessment from Epsilon.

Similarly, with reference to a pure 'on the papers' approach, there is also no indication of the OAIC seeking evidence from independent, third-party experts. In some of the six OMIs, respondents retained their own third-party experts, a practice which appears to have been generally accepted by the OAIC. This reliance on information provided by the respondent rather than on any independent investigation or third-party evidence gathering by the OAIC on its own behalf is supported by the OMI reports. Each report includes a statement to the effect that the information relied on by the OAIC in forming its decision is that provided by the respondent. For example, the Dell/Epsilon report provides:

> On the basis of information received from Epsilon, the Privacy Commissioner considers that at the time of the incident Epsilon had reasonable steps in place to protect the personal information it held and in his view Epsilon has met its obligations under NPP 4.1 of the *Privacy Act*.[163]

The *Privacy Complaints Manual* provides that, to ensure procedural fairness, the 'OAIC needs to take account of all relevant considerations and needs to support its position with evidence or other material'.[164] The manual refers to different types of evidence that might be available, including copies of audit trails from computer systems and 'corroborative evidence from third parties, often by way of a statutory declaration'.[165] However, the *Privacy Complaints Manual* does not distinguish between the evidence requirements in complaint-based investigations (where two parties provide evidence) versus OMIs (which typically only involve a respondent).[166] In 2007, the Administrative Review Council released a series of best practice guides designed for agencies with decision-making authority, which would include the OAIC. These include an evidence guide,[167] which states that information provided by applicants (or respondents in the case of OMIs) may be used as evidence but only for 'establishing facts that are likely to be true or that are not material'.[168] Notwithstanding this advice, it seems that in each of the six OMIs considered, the Commissioner relied almost entirely on evidence provided by the respondents, without independent corroboration (other than reports commissioned by the respondents) to establish material facts.

The *Privacy Complaints Manual* suggests that, following the initial request for information, further evidence-collecting steps might be considered, depending on the response to the initial request.[169] These steps might include requesting further information or documents from the respondent or complainant or seeking

163 *Dell/Epsilon OMI Report*, above n 70.
164 Office of the Australian Information Commissioner, *Privacy Complaints Manual*, above n 10, 34.
165 Ibid.
166 This possibly reflects the focus of the *Privacy Complaints Manual* on complaint-based investigations.
167 Administrative Review Council, *Decision Making: Evidence, Facts and Findings* (Best Practice Guide No 3, August 2007) <http://www.arc.ag.gov.au/Documents/ARC+Best+Practice+Guide+3+Evidence+Facts+and+Findings.pdf>.
168 Ibid 4.
169 Office of the Australian Information Commissioner, *Privacy Complaints Manual*, above n 10, 34.

independent corroboration from another source, for example, a website, government body or third party.[170] There is little evidence of any second round of questioning by the OAIC of the respondents following receipt of the response to the initial RFI letters, certainly in regard to data security issues, and other than in regard to the provisions of reports where the respondent had indicated it was investigating the incident.[171] In particular, other than the Telstra Bundles investigation,[172] it does not appear that the OAIC sought to elicit further information about how the incident occurred, what security measures were in place, how those measures were determined to be adequate, or what the organisational response to the incidents was in any of the OMIs following the respondents' replies to the initial RFI letters or the receipt of investigation reports.[173]

One result of the limited follow-up is that responses to the RFI letters, together with any reports provided, comprise almost the entirety of evidence regarding the incident obtained by the OAIC and relied on in making its decisions. In effect, the questions posed in the RFI letters set the parameters for the investigation. This makes the fact that those questions are largely generic, high-level and open-ended or, as in the case of the Dell investigation, framed by the information provided by the respondent, even more problematic.

In summary, it appears that the OAIC is overly willing to rely on the written information voluntarily provided by the respondent being investigated. There is virtually no questioning of interested parties and no indication of any independent verification of information provided by respondents or third-party experts engaged by respondents. There is no evidence of the use of available powers under sections 43 and 44 of the *Privacy Act* to require production of further information or of any detailed further questioning by the Commissioner following receipt of the response to the RFI letters. In effect, we argue that the 'on the papers' approach adopted by the OAIC is insufficient and unlikely to provide adequate and reliable evidence in the context of the complex contextual realities of serious data breaches.

C Decision-Making

According to the *Privacy Complaints Manual*, the OAIC must take steps to advise entities being investigated of three pieces of information before closing an investigation:

- firstly, that it proposes to close the complaint
- secondly, why it intends to close the complaint

170 Ibid.

171 The Sony and Dell/Epsilon investigations included some discussion between the parties around the application of the *Privacy Act* to the entities involved, as demonstrated by the references to the jurisdiction issues in the respective reports.

172 Letter from OAIC staff to Telstra, 8 March 2012.

173 Email from OAIC to Telstra, 15 March 2012.

- thirdly, that it is offering the complainant a reasonable opportunity to make a submission before it closes the complaint.[174]

Letters advising each of the respondents of the outcome of the investigations ('close letters') were disclosed for all of the OMIs.[175] Each of these close letters followed a similar format and generally met the above requirements.[176]

However, the investigation files provide very little indication as to how the OAIC arrived at the decision as to whether there has been an interference with privacy as contained in the close letters. This is not surprising given that one of the main grounds for redaction of records was that they related to the OAIC's decision-making process. Broadly, any record that might have provided information relevant to decision-making was redacted, including all draft OMI reports as well as most of the substantive parts of the close letters sent to the different respondents.

However, each of the six investigation files also contained a summary sheet that listed all of the actions undertaken in each investigation. These summary sheets do not reveal any discernible process about how decisions were made by the OAIC.[177] For instance, there are no references to any internal meetings to determine outcomes, or of briefing notes being drafted or sent to case supervisors for consideration and decision on outcomes.

Although the files do not reveal the process by which decisions were made in any of the investigations, they do indicate that in most cases the decision regarding whether there had been an interference with privacy was arrived at quite quickly. In the Sony investigation for example, a file note records that, at an internal OAIC meeting occurring the day after Sony's response to the RFI letter was received, it was decided that there was no breach of NPP 4.[178] This is notwithstanding that details of how the attack had succeeded were not publicly

174 Office of the Australian Information Commissioner, *Privacy Complaints Manual*, above n 10, 25.

175 See, eg, *Telstra Mail-Out Close Letter*, above n 83; *Sony Close Letter*, above n 89.

176 It should be noted that large sections of all the close letters, other than *Telstra Mail-Out Close Letter*, above n 83, have been significantly redacted on the basis that the contents went to the OAIC's decision-making process or contained information confidential to the respondent.

177 See, eg, Office of the Australian Information Commissioner, *Case Management Summary: Sony Computers Entertainment Australia Pty Ltd* (18 June 2013) ('*Sony Case Management Summary*'), attached to Letter from OAIC to Jodie Siganto, 30 August 2013; *Medvet Case Management Summary*, above n 110.

178 *Sony Case Management Summary*, above n 177, refers to this meeting on 12 May 2011. No record of the meeting was produced by the OAIC pursuant to the FOI request.

available, raising the question of how the Commissioner was able to determine that Sony had taken appropriate steps to protect the personal information.[179]

The Medvet investigation tends to support the contention that the OAIC did not have a consistent process for decision-making in OMIs, and that in some investigations, the case may have been closed too quickly. A note from the case officer in the Medvet investigation file states 'we received a response from Medvet on 21 September and I have assessed the response and it appears that [the respondent] has taken reasonable steps and we are in a position to finalise'.

Even though the decision was made to formally close the Medvet OMI, it was later reopened, resulting in two very different close letters being sent to Medvet. In the reopening of the Medvet OMI, there is no reference to any new evidence being received or further internal meetings being held to discuss the case after the first close letter was sent in December 2012.[180] However, nearly seven months after that first close letter, in July 2012, a second and different close letter was sent to Medvet advising of a new finding of breach of NPP 2 (in addition to the previous finding of breach of NPP 4).[181] The basis for this change is difficult to understand. It may be that the different decision was due to an alternative view being taken of the facts by the Commissioner, who, according to the new close letter, conducted a review of the file as part of finalising the draft OMI report.[182] Unfortunately, we were unable to confirm this point, as almost the entirety of the second close letter was redacted. The fact that the Commissioner felt it appropriate to change the communicated findings of an investigation suggests, at the very least, a problem with the initial decision-making process.

D Publication of Findings

There are two aspects to the publishing of OMI reports. The first is the selection of the investigation as one on which to report. The second is the process of the preparation of the report. The *Guide to Producing Case Notes* sets out a process for the selection of cases from which to publish a report. The process

179 In May 2011, at the same time as the OAIC was concluding its investigation, Sony submitted a written statement to a US Congressional Hearing to the effect that the incident was still being investigated and the cause of the incident was not clear: Letter from Kazuo Haria, Chairman, Sony Computer America LLC, to Fred Upton Chairman, US House of Representatives, Committee on Energy and Commerce, 26 May 2011. The United Kingdom Information Commissioner's Office's ('UK ICO') report into the same incident was not issued until early 2013, over 12 months after the finalisation of the Commissioner's investigation: Information Commissioner's Office (UK), *Data Protection Act 1988 Monetary Penalty Notice: Sony Computer Entertainment Europe Limited* (14 January 2013) <http://www.ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Notices/sony_monetary_penalty_notice.ashx>. That report benefited from detailed information from Sony about the vulnerabilities in the Sony systems that enabled the attack. By reference to those vulnerabilities, and the failure to implement fairly rudimentary measures such as software patching, the UK ICO decided that Sony had failed to take reasonable steps, referring to Sony's out-of-date software patching (which was one of the contributors to the success of the attack according to the UK ICO's report). This was not referred to as a relevant consideration by the OAIC in its report.

180 *Medvet Close Letter 1*, above n 114.

181 *Medvet Close Letter 2*, above n 116.

182 Ibid.

entails a case officer flagging potential cases for publication which are then given further consideration by a project manager in consultation with the compliance unit where appropriate.[183] The same process applies to the publication of OMI reports.[184]

Our review of the six OMIs indicates that this preparation process was largely followed by the OAIC. However, in terms of the selection of cases for reporting, the investigation files indicate that the Deputy Commissioner for Compliance and the Commissioner personally played a significant role. The Commissioner or Deputy Commissioner determined whether a report should be published, reviewed the proposed OMI reports and negotiated their terms with the respondent in at least five of the six investigations.[185] The Commissioner seems to have been particularly active in decision-making around whether a report should be published. For example, a note in the Medvet file records '[d]iscussed possibility of report with MH. … MH said we will wait for TP [*FOI Act* section 22(1)(a)(ii) exemption] to see if he wants to issue public report'.[186]

Once a decision to publish a report is made, a draft OMI report is prepared and sent to the respondent for comments and, subject to that, published on the OAIC website.[187] As no draft OMI Reports were disclosed, it is difficult to ascertain any changes agreed to as part of this review process. However, the published reports appear to reflect the terms of the close letters sent out in each investigation, which suggests that any issues are largely resolved when the close letters are sent out (other than in the Medvet investigation).

E Summary of Findings

Our examination of the six OMI investigation files reveals a number of key findings. It appears that the OAIC did not follow its own criteria in deciding which incidents should be the subject of an OMI. In particular, none of the six investigations reviewed were overtly undertaken on the basis that they involved any systemic issue or that they were responsive to a perceived risk of significant harm. The main reason for commencing the investigations appears to have been the media attention that had been given to the cases, and the Commissioner's own decision to investigate high-profile data breach cases.

As regards the process adopted, no case plan was prepared to guide any of the investigations. There is no indication from the files of any pre-planning to

183 Office of the Australian Information Commissioner, *Guide to Producing Case Notes*, above n 10, specifically the information under subheading 'Selecting a Suitable Case for a Case Note'.

184 Ibid.

185 See, eg, the Sony investigation, where the Commissioner was involved in settling the final close letter and attached OMI report: Email from Timothy Pilgrim to OAIC staff, 24 May 2011. The OAIC email, sending a draft of close letter and the OMI report to Sony, refers to the Commissioner's clearance being obtained to sending out those documents: Email from Linda King to Sony, 29 June 2011.

186 Office of the Australian Information Commissioner, *File Note* (19 December 2011). The reference to 'TP' is to Timothy Pilgrim, the Privacy Commissioner.

187 Although correspondence on the investigation files indicated that draft OMI reports were sent to each of the respondents, no draft OMI report was disclosed on the basis that the drafts went to the OAIC's decision-making process. The drafting of the OMI reports is discussed further below.

identify the evidence that should have been obtained in each case in order to determine whether there had been an interference with privacy. Moreover, rather than specific questioning based on the details of the case, generic and non-specific questions were typically posed in the RFI letters sent to the respondents. It should also be noted that these letters were the principal device for gathering evidence about the incidents.

Regarding evidence, the investigatory processes adopted in the six OMIs did not appear to involve any vigorous pursuit of information. However, there was in one case an apparent willingness to at least threaten to use more coercive powers in the face of lack of cooperation, as demonstrated by the OAIC's response to Telstra's delay in the Telstra Bundles OMI. Communication between the OAIC and the respondents is almost entirely by exchange of emails and letters, with little evidence of any physical meetings or site inspections taking place.

The evidence relied on by the OAIC in reaching its decisions is provided by the respondents either directly or via third-party reports commissioned by the respondents. There is no independent testing or verification of the information that is obtained from or at the direction of the organisation being investigated in response to the questions raised in those RFI letters.

The investigation files provide little information to indicate the process used by the OAIC to arrive at a decision regarding the outcome of an investigation. However, it does appear that the decision is made quite quickly following receipt of information from the respondent, with the change in the findings in the Medvet case suggesting that perhaps decisions may be made without appropriate consultation within the Commission. While the production of reports is largely consistent with the relevant guidance, the decision to publish the six OMI reports appears to have been influenced by the Commissioner. The decision does not seem to have been made on the basis of the criteria stated in the guidance on publishing case notes.

All of these points raise significant questions about both the validity and purpose of the six OMIs. We conclude our article by considering the further implications of these findings, in particular possible reasons for the identified shortcomings in these investigations.

IV IS THE PRIVACY COMMISSIONER GOING THROUGH THE MOTIONS?

In this Part, we consider the possible reasons for some of the problems identified in the OAIC's investigatory approach. Those reasons include the OAIC's lack of powers, lack of resources and whether there was another policy imperative at work. We conclude the article by going back to what can be learned from the six OMIs in order to look forward to the further development of data breach policy formulation.

A A Lack of Powers?

The OAIC's investigatory approach in the six OMIs may have been influenced by the limited powers available, at that time, for OMIs.

As of March 2014, the Commissioner has the benefit of additional investigation and enforcement powers. These powers include the power to:

- make a determination following an OMI;[188]
- seek civil penalties for a serious or repeated interference with the privacy of an individual;[189] and
- accept written enforceable undertakings by entities to take, or refrain from taking, specified actions to ensure compliance with the *Privacy Act*.[190]

The Acting Assistant Commissioner Compliance referred to these additional powers in our interview, commenting that they bring a 'heightened deterrent and educative element to those matters'.[191] The OAIC supported this extension of its powers, saying that the new powers 'would have significant implications for privacy compliance in Australia',[192] including the provision of 'credibility for enforcement of privacy law' and 'an even greater incentive' for privacy responsibilities to be taken 'seriously'.[193] This is a long held point by the OAIC, particularly in regard to powers when undertaking an OMI. In 2007, the Office of the Privacy Commissioner, the predecessor of the OAIC, also supported the introduction of enforceable remedies following OMIs, noting that it had 'experienced some difficulties' in dealing with potential privacy breaches where there was no individual complainant and where the respondent was not cooperative.[194]

Prior to March 2014, and at the time the six OMIs were undertaken, the Commissioner did not have any determination enforcement powers when conducting an OMI, and was largely reliant on the voluntary cooperation of respondents. This is one of the factors thought to have influenced the conciliatory approach taken to investigations by the Commissioner and the interest shown by the Commissioner in concluding investigations on the basis of outcomes agreed

188 *Privacy Act* s 52(1A).
189 *Privacy Act* pt VIB deals specifically with civil penalty orders.
190 *Privacy Act* s 33E.
191 Interview with Angelene Falk, Acting Assistant Commissioner Compliance, OAIC (Sydney, 14 December 2012).
192 Pilgrim, 'Privacy Law Reform', above n 6.
193 Ibid.
194 *For Your Information Report*, above n 8, 1651 [50.7].

with the respondent.[195] Without recourse to more punitive powers, such as the ability to issue a determination with adverse findings, there has been little that the OAIC could do if confronted by an uncooperative or recalcitrant respondent.[196]

While the Commissioner has acknowledged the effect of the lack of powers on OMIs,[197] he has also been careful to state – certainly in regard to the recent data breach investigations – that the respondents have been cooperative and that the OAIC had been 'very lucky' in the investigations conducted because 'organisations have been very willing to provide us with relevant information to undertake these investigations'.[198] In our interview, the Assistant Commissioner Compliance referred to the 'difficulty' of not having an attached enforcement power while noting that in all the OMIs completed to date, 'the respondents have been very cooperative' and 'accept the views that we come to in general and … see the benefit from their point of view in complying with the findings that are given'.[199] Ensuring this cooperation does seem to have some consequences. The findings from the review in Part III suggest that the investigation process has not been vigorously pursued, that the Commissioner has not used its powers to require the production of documents or the appearance of witnesses and that the OAIC has been concerned to arrive at an agreed outcome with the respondents in each of the investigations.

There are also consequences in terms of the accountability of the OAIC. One of the reasons for refusing access to the investigation files pursuant to the FOI requests referred to in Part II included that disclosure would 'have a very real impact on the Commissioner's own motion investigations as the OAIC depends on the goodwill and cooperation of OMI respondents to provide information', and ensuring the confidentiality of the information supplied was critical to maintaining that cooperation.[200]

Part of the purpose of the *FOI Act* is to support government accountability and transparency of regulatory action.[201] The OAIC decided that non-disclosure of records in the interests of ensuring the cooperation of respondents in future

195 O'Connor, above n 8, 258–60. See also Interview with Angelene Falk, Acting Assistant Commissioner Compliance, OAIC (Sydney, 14 December 2012), where the Acting Assistant Commissioner referred to the OMI decisions as 'recommendatory only', but noted that that would change under the reforms of the *Privacy Act* with the ability for the Commissioner to make a determination (which if not complied with can be enforced in the Federal Court) and seek undertakings as an alternative to a determination (which can also be enforced in the Federal Court), saying 'so I think that will give a heightened deterrent and educative element to those matters'.

196 The Office of the Privacy Commissioner acknowledged that it had 'experienced some difficulties' in dealing with potential privacy breaches where there was no individual complainant and where the respondent was not cooperative: see *Getting in on the Act Report*, above n 54, 155; *For Your Information Report*, above n 8, 1651 [50.7].

197 In the interview with the researcher, the Commissioner referred to the OAIC's lack of powers, saying 'I have no remedy powers to force [respondents] to do anything': Interview with Timothy Pilgrim, Privacy Commissioner (Sydney, 14 December 2012).

198 Ibid.

199 Interview with Angelene Falk, Acting Assistant Commissioner Compliance, OAIC (Sydney, 14 December 2012).

200 Letter from OAIC to Jodie Siganto, 30 August 2013.

201 *FOI Act* s 3.

investigations overrode the public interest in transparency and accountability. This indicates the level of concern within the OAIC about its ability to conduct investigations without the cooperation of respondents.

On its face, the extension of the determination power to investigations commenced on the Commissioner's own motion and the ability to seek civil penalties would seem to be significant additions to the OAIC's armoury. Those additional powers may well herald a change in the investigation process, and in particular a less conciliatory approach, given that the OAIC now has enforcement options in the case of a recalcitrant or unresponsive respondent.

A more vigorous investigatory approach may also be influenced by another change effective as of March 2014. Determinations will now be subject to merit reviews by the Administrative Appeals Tribunal (not limited to grounds of procedural fairness or a question of law).[202] The possibility of an OMI culminating in the making of a reviewable determination may change the nature of the investigation undertaken and the content of any report issued, bearing in mind the potential appeal and review rights.[203] In any case, where the OAIC does make a determination, the respondent has the right to be provided with the reasons for the decision, which should include findings on material questions of fact that refer to the evidence or other material on which those findings were based.[204] Where this occurs, it is likely to improve both the balance and vigour of the investigation process and the transparency of the Commissioner's reporting.

However, it is not clear that the Commissioner will use this new power to make a determination following an OMI. Prior to 2011, the OAIC had issued few determinations, the most recent being in 2004.[205] Since then it has referred to its intention to issue more determinations, referring specifically to the value of determinations to explain the OAIC's interpretation of the privacy principles.[206] Eight new determinations have been issued since 2011, making it 16 determinations issued in total.[207] This heightened recent activity may indicate a

202 *Privacy Act* s 96(1)(c).

203 *Privacy Act* s 96(1)(c). See also Office of the Australian Information Commissioner, *Privacy Review Rights* (1 September 2009) <http://www.oaic.gov.au/privacy/privacy-review-rights>. The same reasoning may apply to the potential use by the Commissioner of the power to seek a civil penalty, by application to the Federal Court: *Privacy Act* pt VIB.

204 *Privacy Act* s 52(1B)(2). See also *Administrative Appeals Tribunal Act 1975* (Cth) s 28.

205 Office of the Privacy Commissioner, *Complaint Determination No 5 of 2004* (April 2004) <http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-determinations/complaint-determination-no-5-of-2004>.

206 See, eg, Pilgrim, 'Privacy Law Reform', above n 6.

207 The eight determinations issued after 2004 are '*EQ*' *and Great Barrier Reef Marine Park Authority* [2015] AICmr 11 (Unreported, Commissioner Pilgrim, 2 February 2015); '*DO*' *and Department of Veterans*' *Affairs* [2014] AICmr 124 (Unreported, Commissioner Pilgrim, 13 November 2014); '*DK*' *and Telstra Corporation Ltd* [2014] AICmr 118 (Unreported, Commissioner Pilgrim, 30 October 2014); '*CP*' *and Department of Defence* [2014] AICmr 88 (Unreported, Commissioner Pilgrim, 2 September 2014); *'CM' and Corporation of the Synod of the Diocese of Brisbane* [2014] AICmr 86 (Unreported, Commissioner Pilgrim, 2 September 2014); '*BO*' *and AeroCare Pty Ltd* [2014] AICmr 32 (Unreported, Commissioner Pilgrim, 8 April 2014); '*S*' *and Veda Advantage Information Services & Solutions Ltd* [2012] AICmr 33 (Unreported, Commissioner Pilgrim, 20 December 2012); '*D*' *and Wentworthville Leagues Club* [2011] AICmr 9 (Unreported, Commissioner Pilgrim, 9 December 2011).

new resolve to make determinations, including as an outcome of OMIs. However, at least one other issue regarded as impacting on the OAIC's use of the determination power remains.[208] The Commissioner will still struggle to enforce compliance with a determination without the matter being heard de novo by the Federal Court.[209] In addition, respondents have no right to require the Commissioner to make a determination. Without a determination, the only judicial review available will be in regard to questions of law and the Federal Court so far has been reluctant to entertain any such review.[210]

Given the Commissioner's historical reluctance to make determinations, and its continued inability to enforce a determination without there being a full hearing, it seems more likely that the OAIC will elect to take an alternative approach to concluding OMIs and, instead of making a determination, will seek to secure an enforceable undertaking from respondents.[211] As the Commissioner has previously indicated, concluding investigations based on undertakings made by the respondent may be a more attractive resolution than making a determination.[212]

If this is the avenue pursued by the Commissioner, it is unlikely to contribute greatly to the rigour of the investigation process or the jurisprudence around the Commissioner's interpretation and application of the privacy principles. Enforceable undertakings are, by their nature, enforceable without any judicial review or other consideration of the merits of the undertaking. This means that the conduct and outcome of those investigations which culminate in an enforceable undertaking will not be subject to any form of judicial review. Enforceable undertakings can also be compared to conciliated outcomes. They are the agreement reached between the regulator and the respondent as to the appropriate remediation action to be taken to enable the regulator to close an investigation. Although they are of some use, in terms of providing reassurance that identified problems may be addressed, the contents of enforceable undertakings will not have any significant weight in terms of the interpretation or application of the privacy principles, nor will they support increased

208 See, eg, O'Connor, above n 8, 256–7, which suggests that the lack of determinations is because most investigations are resolved successfully. O'Connor further attributes this to the high chance of differences in interpretation between the Commissioner and the Federal Court which means that there is 'always a reasonable prospect of Federal Court over-rule, with the result that the authority of the Privacy Commissioner and the Commissioner's Office might be diminished in the process': at 259–60.

209 *Privacy Act* s 55A(5).

210 To date, most applications for review have been dismissed without consideration of the privacy principles: see, eg, *A v Australian Information Commissioner* [2011] FCA 520; *Wijayaweera v Australian Information Commissioner* [2012] FCA 99; *Hammond v Australian Information Commissioner* [2013] FCA 802. There have been only two cases where the Court considered the Commissioner's interpretation of the privacy principles as part of its decision as to whether or not there had been a mistake in law: *Smallbone v New South Wales Bar Association* (2011) 198 FCR 17; *Jones v Office of the Australian Information Commissioner* [2014] FCA 285.

211 *Privacy Act* s 33E.

212 In both the Vodafone and the Telstra Bundles investigations, the respondents gave undertakings to the Commissioner to take agreed remediation steps and report back to the Commissioner on the action that had been taken.

accountability of the Commissioner for its investigations and findings.[213] Future OMIs that culminate in enforceable undertakings are unlikely to be significantly different to the investigations considered in this research, with the attendant issues of transparency, balance and vigour.

B Appropriate Skills and Resources?

The eschewing of any vigorous independent inquiry into the facts of the six OMIs may be a consequence of the limited resources and skills available to the OAIC, particularly when faced with investigating highly complex data security incidents. The OAIC's resource issues have been recognised for some time. The ALRC referred to the significant expansion of the responsibilities of the OAIC, which 'resulted in more functions and powers for the Commissioner, although not always a commensurate increase in resources'.[214]

More recently, the Commissioner has publicly acknowledged the resource pressures facing the OAIC, noting a decrease in staffing numbers 'in line with the [office's] need to meet efficiency dividends imposed by Government'.[215] In the last two years, the OAIC's resource issues have been exacerbated by the 'daunting task' of developing guidance to assist with the new APPs, 'given that it has received no additional resourcing for this implementation work'.[216]

One of the most obvious consequences of the OAIC's resourcing constraints is the long waiting period before a privacy complaint is allocated to an investigating officer. It is presently taking about 19 weeks longer than the usual four-week period.[217] In a 2013 Senate Estimates Hearing, the Australian Information Commissioner, Professor John McMillan, was asked directly whether the OAIC's work is being compromised because of the lack of resources.[218] Professor McMillan did not think that 'the quality of the work has been compromised', but thought the OAIC was 'unable to meet the performance standards' it set for itself.[219] It is difficult to see how the Australian Information

213 Cf the approach of the Federal Trade Commission in the US, which has relied on undertakings to resolve data breach cases: see, eg, Travis D Breaux and David L Baumer, 'Legally "Reasonable" Security Requirements: A 10-Year FTC Retrospective' (2011) 30 *Computers & Security* 178; Andrew Serwin, 'The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices' (2011) 48 *San Diego Law Review* 809.

214 *For Your Information Report*, above n 8, 1515–16 [45.2].

215 Ben Grubb, 'Long Delays before Privacy Complaints Assessed', *The Sydney Morning Herald* (online), 13 September 2013 <http://www.smh.com.au/digital-life/consumer-security/long-delays-before-privacy-complaints-assessed-20130912-2tn72.html#ixzz2yY0zIYho>.

216 Message from the Privacy Commissioner, Timothy Pilgrim, quoted in *OAIC 2013 Annual Report*, above n 3, xiv.

217 Grubb, above n 215.

218 Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, *Estimates* (2013) 64–5 ('*Estimates 2013*'). In the Senate Committee hearings the previous year, the Commissioner had said that he considered that the OAIC's level of activity in all areas of its compliance work, complaints and national investigations, would be affected by the number of resources the office had and that there was potential for the Office's ability to respond to high profile data breach cases to be impacted: see Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, *Estimates* (2012) 41–3.

219 *Estimates 2013*, above n 218, 64.

Commissioner can make that assertion in regard to the use of its OMI power given the steady decline in the number of OMIs undertaken,[220] the use of the 'on the papers' approach to OMIs and the questions raised in this research in regard to the balance and vigour of the investigative process itself. In any case, given the proposed restructuring of the OAIC[221] (which has not progressed since the September 2014 sitting of Parliament),[222] it seems likely that the Commissioner's current resource issues will become more acute.[223]

In addition to the number of staff available to conduct investigations, the OAIC may also have issues in terms of the skills of its staff. In our interview, the Assistant Commissioner Compliance said: '[O]ne of the things that is a challenge for us is ensuring that we've got sufficient expertise to be able to analyse the information that is provided back to us particularly if it's very technical'.[224]

The Commissioner also acknowledged the skills issues regarding NPP 4 investigations saying:

> [This] is an area that is going to be increasingly hard for us to determine because of the nature and complexity of systems and we are already finding that. … Because as you can appreciate you need to start having some fairly well developed technical skills to be able to start assessing at a very forensic level sometimes what is going on in organisations.[225]

Later in the interview, when discussing the skills required to carry out investigations, the Commissioner said it was hard for the OAIC to attract the sort of people who had the requisite skill levels and, once in the OAIC, for those people to maintain that skill level.[226]

Although acknowledging the difficulty with appropriate skills, the Commissioner did not believe that it had impacted upon the investigation process. While conceding that the OAIC was very reliant on the information provided by respondents and the skills of individual staff members, the

---

220 In 2013/14, six matters were considered and five matters proceeded to an OMI: *OAIC 2014 Annual Report*, above n 17, 91; 13 OMIs were conducted in 2012/13: *OAIC 2013 Annual Report*, above n 3, 77; 37 were conducted in 2011/12: *OAIC 2012 Annual Report*, above n 3, 62; and 59 were conducted in 2010/11: *OAIC 2011 Annual Report*, above n 17, 36.

221 John McMillan, James Popple and Timothy Pilgrim, 'Australian Government's Budget Decision To Disband OAIC' (Statement, 13 May 2014) <http://www.oaic.gov.au/news-and-events/statements/australian-governments-budget-decision-to-disband-oaic/australian-government-s-budget-decision-to-disband-oaic>. The restructuring was proposed in the Freedom of Information Amendment (New Arrangements) Bill 2014 (Cth) which was introduced into the Senate but not considered before the end of the 2014 sitting period: Parliament of Australia, *Freedom of Information Amendment (New Arrangements) Bill 2014* (2014) <http://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r5350>.

222 'The OAIC will therefore remain operational until further notice': Office of the Australian Information Commissioner, *OAIC To Remain Operational until Further Notice* (Statement, December 2014) <http://www.oaic.gov.au/news-and-events/statements/australian-governments-budget-decision-to-disband-oaic/oaic-to-remain-operational>.

223 See, eg, Bruce Baer Arnold, 'Ending the OAIC and New Frameworks for Privacy Law' (2014) 11 *Privacy Law Bulletin* 66.

224 Interview with Angelene Falk, Acting Assistant Commissioner Compliance, OAIC (Sydney, 14 December 2012).

225 Interview with Timothy Pilgrim, Privacy Commissioner (Sydney, 14 December 2012).

226 Ibid.

Commissioner said that he believed those skills were sufficient 'to put [him] in a position where [he could] make a sound decision on what [had] been presented to [him]'.[227] However, there is some evidence from the investigation files that the investigators may not have sufficient technical skills.

In the Medvet investigation, two third-party reports were prepared. The first was a Deloitte report which provided an analysis of the breach and the system flaws that led to that breach occurring.[228] The second was a consultant's report containing an update on the implementation of remedies to the issues raised in the Deloitte report.[229] When considering whether to pursue a copy of this second report, an internal OAIC email states: 'Let's pursue the 2nd report then … If the first report is highly technical it may not assist us anyway'.[230]

The implication from this email exchange is that technical reports may present difficulties for the OAIC. There is also some suggestion from the investigation files that the OAIC may not have been conversant with the two international standards relevant to information security: ISO 27001[231] and ISO 27002.[232] An email chain from the Sony investigation file includes the following: 'We have got a licenced copy of the ISO IT Security Standard to assess Vodafone's NPP4 compliance, I expect that standard is going to come in handy again and can be relevantly be applied to the Sony issues as it is an international standard'.[233]

It is likely that this is a reference to ISO 27002, as that was the standard referred to in the *Vodafone OMI Report*.[234] The wording of the comment suggests that, at least at the time of writing, the OAIC regarded ISO 27002 as the only ISO IT Security Standard. There is no reference to ISO 27001 or to the fact that ISO 27002 is designed as a code of practice supporting ISO 27001. The proposition that at the time the OAIC compliance team was not aware of ISO 27001 or its relationship to ISO 27002 is supported by the subsequent note in the Epsilon file which provides: 'File discussed with supervisor (LK). Issues for follow up standards and investigation report. … LK to contact Standards Australia to

227 Ibid.

228 A copy of the Deloitte report was provided under cover of the Letter from Medvet to OAIC, 21 September 2011. However, the contents of that report were redacted in full: Letter from OAIC staff to Jodie Siganto, 7 April 2014; Email thread from Medvet to OAIC staff, 21 September 2011, document CMS 3.

229 The contents of these reports were redacted in full. An internal OAIC email contains the following statement: 'there has been a second Consultant's Report showing what had been recommended and what has been implemented': Internal email thread, OAIC, 9 November 2011.

230 Internal email thread, OAIC, 10 November 2011.

231 International Organisation for Standardisation, *ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements* (2013).

232 International Organisation for Standardisation, *ISO/IEC 27002:2013 Information Technology – Security Techniques – Code of Practice for Information Security Controls* (2013).

233 Internal email, OAIC, 6 May 2011.

234 *Vodafone OMI Report*, above n 46.

clarify the content of ISO 27001 (as we haveAS/NZS ISO 27002 only under licence)'.[235]

If the OAIC does not have the technical knowledge or skills to analyse the causes or methods for prevention of security breaches, or to assess technical details about how security breaches occurred, then it is not clear how the OAIC is able to conduct these investigations or assure itself that third-party expert reports are accurate, complete and based on the use of an appropriate standard of care. It is therefore difficult to determine how the OAIC can adequately say whether there has been any failure to properly protect personal information.

Third-party investigation reports were provided by the respondents in the Medvet, Sony and Epsilon investigations.[236] The OAIC's reliance on the Deloitte report in the Medvet case in particular was somewhat controversial with one media commentator suggesting that that report may not have been independent.[237] On that point, the Commissioner expressed confidence that he would be able to identify any lack of independence and that the OAIC had the skills to assess whether or not it would be appropriate to rely on a third-party report.[238] The Commissioner appeared to consider the fact that the Deloitte report found a lot of failings in the system as evidence of the report's independence.[239] The Commissioner also commented that he did not think it appropriate for the OAIC to replicate the work done by Deloitte and to 'expend the office's resources to repeat an exercise that had been done, in [his] view, quite independently and with a reasonable outcome'.[240]

This point is potentially concerning. If this statement is indeed a foreshadowing of OAIC policy on the future reliance on third-party reports, then it is possible that the use of existing formal powers will once again be eschewed. Moreover, an overt and under-critical reliance on respondent third-party reports could lead to the situation where deep-pocketed respondents with existing relationships with legal and information security experts, who are likely to be engaged to prepare 'independent' investigation reports, may be able to secure more favourable investigation outcomes.

C A Data Breach Policy Imperative?

In view of the Commissioner's limited resources and lack of powers, the OAIC's decision to pursue investigations into data breach cases in the 2011/12 period is of interest. As discussed, the stated reasons for the Commissioner's

235 Office of the Australian Information Commissioner, *Complaint Management System Report Epsilon Investigation File* (File No C15085, 9 September 2013) 2.

236 Medvet provided a report from Deloitte: see Email thread from Medvet to OAIC staff, 21 September 2011, document CMS 3; Sony provided a third-party investigation report; Epsilon provided a report from Verizon.

237 Letter from Timothy Pilgrim to the Editor of *The Australian* newspaper, 26 July 2012 <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/medvet-investigation/privacy-commissioner-responds-to-media-claims-about-medvet-investigation>.

238 Ibid.

239 Interview with Timothy Pilgrim, Privacy Commissioner (Sydney, 14 December 2012).

240 Ibid.

acknowledged change in enforcement approach were to increase transparency in the OAIC's investigation process, and to help organisations and agencies to better understand their privacy responsibilities.[241] However, it seems likely that these investigations were, at least in part, a consequence of the Commissioner's interest in supporting the notification of data breaches in Australia.

The Commissioner has long supported the introduction of a mandatory data breach notification requirement. This stance is reflected in public submissions,[242] media releases,[243] reports[244] and speeches.[245] The Commissioner believes that mandatory data breach notification 'helps to manage the risk to individuals in the case of a data breach' and 'also helps organisations … deal with this risk, and respond to a breach'.[246] The Commissioner has also consistently made the point that breaches seem to be under-reported: 'It is not a secret that we don't see the levels of data breach notification that we would like to see, given how many organisations experience a breach'.[247]

The OAIC first published a voluntary data breach notification guide in August 2008,[248] updating it in July 2011 and again in August 2014,[249] as a means of encouraging organisations to 'voluntarily put in place reasonable measures to deal with data breaches', while legislative change is considered by the

241 Ibid.

242 See, eg, Timothy Pilgrim, Submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, January 2015; Office of the Privacy Commissioner, Submission to the Australian Law Reform Commission, *Review of Privacy – Issues Paper 31*, February 2007; Office of the Privacy Commissioner, Submission to the Australian Law Reform Commission, *Review of Privacy – Discussion Paper 72*, December 2007; Timothy Pilgrim, Submission to Attorney General's Department, *Discussion Paper: Australian Privacy Breach Notification*, November 2012.

243 Office of the Australian Information Commissioner, *Australians Better Protected with Mandatory Data Breach Notification* (Media Release, 28 May 2013) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/australians-better-protected-with-mandatory-data-breach-notification>.

244 *OAIC 2012 Annual Report*, above n 3, xv; *OAIC 2013 Annual Report*, above n 3, xv.

245 See, eg, Timothy Pilgrim, 'The Importance of Information Security in Protecting Privacy' (Speech delivered at the Australian Information Security Association Conference, Melbourne, 17 October 2014) <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/the-importance-of-information-security-in-protecting-privacy>; Timothy Pilgrim, 'Mapping Data Breach Notification' (Speech delivered at the iappANZ Data Breach Panel Discussion, Sydney, 6 May 2013) <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/mapping-data-breach-notification>; Timothy Pilgrim, 'Privacy Reform – Act Three' (Speech delivered at the iappANZ 'Privacy Unbound' Summit, Sydney, 25 November 2013) <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-reform-act-three>.

246 Pilgrim, 'The Importance of Information Security', above n 245.

247 Ibid.

248 Office of the Australian Information Commissioner, *Data Breach Notification: A Guide to Handling Personal Information Security Breaches* (August 2008).

249 Office of the Australian Information Commissioner, *Data Breach Notification: A Guide to Handling Personal Information Security Breaches* (July 2011); Office of the Australian Information Commissioner, *Data Breach Notification: A Guide to Handling Personal Information Security Breaches* (August 2014) <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches>.

government.[250] The Commissioner has drawn attention to its 2011 data breach notification guide, stating that it outlines steps businesses and agencies can take to respond to and mitigate the results of data breaches.[251]

In addition to these speeches, submissions and reports and the issuance of guidance, data breach notification has been raised in 8 of the 14 data breach investigations conducted by the Commissioner between February 2011 and December 2014.[252]

The *Telstra Mail-Out OMI Report* refers approvingly to Telstra's notification to its customers, providing that 'by notifying affected customers, these individuals had an opportunity to take appropriate action, if necessary, to mitigate any harm they may suffer'.[253] By contrast, in the *Sony OMI Report* the Commissioner indicated concern 'about the time that elapsed – seven days – between Sony becoming aware of the incident and notifying customers and the OAIC'.[254] The Commissioner referred to the benefits of immediate or early notification[255] and recommended that 'Sony review how it applies' the OAIC's data breach notification guide.[256]

Other published investigation reports also support the Commissioner's position that the OAIC, as well as affected persons, should be notified of breaches. In its OMI report in relation to Cupid, the Commissioner referred to the fact that Cupid had notified all affected users and developed a data breach response plan after the incident, but also referred to the fact that Cupid had not notified the OAIC of the breach. The report stated: 'Notifying the OAIC can be a useful step in responding to a data breach, and the Commissioner encourages voluntary notification'.[257] Similar support for proactively notifying the OAIC of data breaches was included in the most recent report of an investigation into Telstra.[258]

---

250 John McMillan, 'Launch of Data Breach Notification Guide' (Speech delivered at the OAIC Privacy Awareness Week Corporate Breakfast, Sydney, 30 April 2012) <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/launch-of-data-breach-notification-guide>.

251 Office of the Australian Information Commissioner, 'Privacy Breach: 254 000 Australian Online Dating Profiles Hacked', above n 2.

252 Data breach notification has not been referred to in the reports published in regard to the Vodafone, Telstra Bundles, Medvet, Multicard and Department of Immigration and Border Protection investigations. The reference in the *Dell/Epsilon OMI Report* is only to Epsilon's notification of its customers in the description of the actions taken following the incident: *Dell/Epsilon OMI Report*, above n 70.

253 *Telstra Mail-Out OMI Report*, above n 47.

254 Pilgrim, 'Privacy Law Reform', above n 6. See also *Sony OMI Report*, above n 47.

255 Pilgrim, 'Privacy Law Reform', above n 6.

256 Ibid.

257 Office of the Australian Information Commissioner, *Cupid Media Pty Ltd: Own Motion Investigation Report* (June 2014) 10 <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/cupid-omi> (citations omitted).

258 Office of the Australian Information Commissioner, *Telstra Corporation Limited: Own Motion Investigation Report* (March 2014) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/telstra-omi-march-2014>. See also Office of the Australian Information Commissioner, 'Privacy Breach: 254 000 Australian Online Dating Profiles Hacked', above n 2, where the Commissioner said: 'I encourage organisations to proactively notify the OAIC of a data breach so that we can work with them and assist with appropriate remediation if necessary'.

In terms of the six OMIs reviewed, the selection of the particular cases to investigate (all involving a data breach), the ongoing media engagement highlighting both the investigations being undertaken and the investigation results once available, and the Commissioner's personal involvement in the decision to publish reports, all suggest that these OMIs were part of a policy imperative to focus on investigating data breach cases. The Commissioner drew the specific link between these investigations and data breach notification in our interview, saying that 'we are seeing breaches on a large scale' and that a mandatory reporting scheme was required 'to give people the ability to know they need to take steps to protect [their personal] information when something goes wrong'.[259]

Based on the above, it could be argued that one of the motivations for undertaking these OMIs and publishing investigation reports might have been to provide further support for the introduction of a mandatory data breach notification scheme, or at the very least, to highlight the issue of data breaches in Australia. This would be consistent with the Commissioner's stated policy position and may explain why the Commissioner has elected to dedicate increasingly scarce resources to the pursuit of these investigations, in preference to other regulatory activity. It may also explain why the investigations themselves lack the rigour that might otherwise be expected. It is possible that the real purpose for these investigations was to raise the profile of data breaches and to highlight the role of the Commissioner in resolving issues as part of a more general policy imperative. If that is indeed the case, then it is not so important that the investigations themselves be conducted in line with the OAIC's own guidance or in accordance with general principles for the use of regulatory powers, including the principles of transparency, balance and vigour.

V CONCLUSION

Our investigation of the six OMIs suggests that the OAIC's decisions to commence the investigations were in response to media and were perhaps motivated by an interest in raising the profile of data breaches in Australia to support the introduction of a mandatory notification scheme. Whether this is in fact correct or not, there are clearly issues with the process followed in each investigation. In all of the OMIs, an 'on the papers' approach was used, based on written responses to largely generic requests for information. There was virtually no second-round questioning, independent evidence gathering or confirmation of the facts as asserted by the respondents, whether directly or via third-party investigation reports commissioned by the respondents. The decision-making process used is also not clear. The change in the outcome of the Medvet investigation, after the initial outcome was communicated to the respondent, in

259 Interview with Timothy Pilgrim, Privacy Commissioner (Sydney, 14 December 2012).

particular raises issues as to the basis for the OAIC's decision-making in these cases.

We assert that these issues arise, in part, as a consequence of the limited powers, skills and resources available to the OAIC at the time. Given the OAIC's new powers and increased accountability, these issues may be addressed in future Commissioner-initiated investigations. However, without the allocation of significant additional resources, it seems unlikely that there would be any significant change in process. Reliance on third-party investigation reports commissioned by the respondent in a future investigation may not be an appropriate resolution.

The OAIC is right to emphasise that the problem of data breaches is likely to remain. However, the examination of the six OMIs reveals that the investigatory approach adopted can lead to the situation where the OAIC investigators are simply going through the motions. On that note, given the issues we highlight in this article, the OAIC's data breach investigations as a body of work are unlikely to be of assistance in regulatory efforts to prevent data breaches, unless significant changes are undertaken. Such changes would herald a major policy shift regarding the role of the OAIC, characterised by the need for a supported, adequately resourced and thus proactive Australian privacy regulator. In that regard, our examination of six relatively recent OMIs sounds a warning not just as to what has happened, but also for the future.