Australian Government
Office of the Australian Information Commissioner

'LU' and Department of Defence (Privacy) [2017] AICmr 61 (26 June 2017)

Decision and reasons for decision of
Australian Privacy Commissioner, Timothy Pilgrim

Complainant:	**'LU'**
Respondent:	**Department of Defence**
Decision date:	**26 June 2017**
Application number:	**CP14/03264**
Catchwords:	**Privacy — Privacy Act — Information Privacy Principles — *Privacy Act 1988* (Cth) s52 — IPP 4 — Data security failure — IPP 10 — Unauthorised use of sensitive personal information — Compensation awarded – Non-economic loss – Section 52(3) expenses awarded**

Table of Contents

Determination

1. The Department of Defence interfered with the complainant's privacy in breach of the *Privacy Act 1988* (Cth) (**Privacy Act**) by:

    - failing to take such security safeguards as is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse, contrary to Information Privacy Principle (**IPP**) 4.
    - using the complainant's personal and sensitive health information contrary to IPP 10.

2. The Department of Defence shall:

    - review its procedures in relation to the internal handling and dissemination of personal information, particularly sensitive information and report the review findings and implementation to the Commissioner within nine (9) months
    - within 60 days;
        - issue a written apology to the complainant acknowledging its interference with the complainant's privacy and the distress it has caused
        - pay the complainant $10,000 for non-economic loss caused by the interference with the complainant's privacy, and
        - pay the complainant $3,000 to reimburse reasonably incurred expenses in connection with the making of the complaint and the investigation of the complaint.

The Complaint

3. At the time of the alleged breach, the complainant was employed by the respondent, the Department of Defence (**Defence**) in its Land Systems Division (**LSD**).

4. Australian Government employees, including employees of Defence, may make claims under the Safety Rehabilitation and Compensation Act 1988 (Cth) (SRC Act) for compensation for injuries suffered in the course of their employment, subject to various conditions.

5. On 12 October 2009 solicitors engaged by the complainant requested Comcare, the agency responsible for workplace compensation in most Australian Government agencies, investigate whether the complainant's employment with Defence had caused or contributed to her contraction of a form of cancer. It was also alleged that a number of the complainant's colleagues, had become seriously ill or died, from cancer related illnesses. Following its investigation, Comcare produced an investigation report, which contained the personal information of the complainant, including her health information (**Comcare Report**).

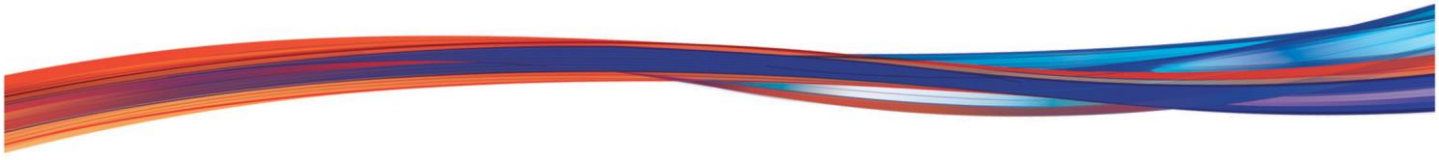
6. In July 2011, the complainant requested from Comcare a copy of the Comcare Report under the Freedom of Information Act 1982 (Cth) (FOI Act). The Comcare Report was provided to the complainant and a redacted version of the Comcare Report (redacted Comcare Report) was made publicly available through the freedom of information (FOI) disclosure log on Comcare's website.[1] However, the redacted Comcare Report did not properly de-identify the complainant, revealing:

    - the complainant's name, postal address and date of birth;
    - the complainant's Personnel Management Key Solution (PMKeyS) number, a unique employee number allocated to Defence personnel, which provides access to phone number and personal email address information; and
    - the complainant's health information.

7. On 9 August 2012, in response to an 8 August 2012 email sent by a LSD employee raising concerns about a 'cancer cluster', accommodation issues and bullying and harassment, a senior officer in Defence sent an email to approximately one thousand, two hundred and seventy (1270) LSD staff, which included a link to the redacted Comcare Report on Comcare's website. On reading the email, the complainant learned the redacted Comcare Report had been published on Comcare's website, and contained her personal information, including sensitive health information.

8. On 10 August 2012 the complainant wrote to the senior officer's Chief of Staff complaining that her personal information was included in the redacted Comcare Report, which had been sent via an email link to Defence staff, and demanded that the email be withdrawn. The senior officer subsequently emailed staff asking that any downloaded copies of the redacted Comcare Report from the Comcare website be deleted and destroyed.

[1] All Australian Government agencies that are subject to the FOI Act are required under section 11C of that Act to publish an FOI disclosure log on their website. The FOI disclosure log lists information that has been released in response to an access request under the FOI Act and the information released must either be made available on the website or through some other means. The information released that must be published is subject to certain exceptions including; personal information about any person, if it would be unreasonable to publish the information.



9. On the same date, Defence contacted Comcare and advised that that the complainant's personal information was included in the publicly available redacted Comcare Report.

10. On or about 13 August 2012, Comcare removed the redacted Comcare Report from its website.

11. On 22 August 2012 the complainant was referred by Defence for psychological and psychiatric assessment.

12. In August 2012 Defence engaged a consulting firm to investigate allegations concerning workplace practices outlined in an email dated 13 August 2012, which was further to the one sent on 8 August 2012 by the same LSD employee. The 13 August 2012 email was a response to and specifically referred to the 9 August 2012 email containing the link to the redacted Comcare Report. Defence provided a consultant from the firm (**Consultant)** with a copy of the redacted Comcare Report for its investigation.

13. After October 2012 the complainant became aware that a copy of the redacted Comcare Report had been saved on the Defence Records Management System (DRMS) without access restrictions or controls.

14. The complainant lodged a complaint with the Office of the Australian Information Commissioner (OAIC) under s 36 of the Privacy Act on 22 July 2012, complaining of Defence's actions. On 11 September 2012, the OAIC declined to investigate this complaint on the ground that the complainant had not first complained to Defence about the matter.

15. On 7 July 2014, the complainant's representatives notified the OAIC that attempts by the complainant to resolve her complaint with the Defence were unsuccessful, and that the complainant now wished to resolve her complaint through the OAIC.

16. The complainant alleges that Defence unlawfully interfered with her privacy, contrary to the Information Privacy Principles (**IPPs**) by:

    - inappropriately collecting the complainant's personal information including sensitive information (Issue 1)
    - failing to protect her personal information, including health information as was reasonable in the circumstances to do (Issue 2)
    - saving a copy of the Comcare Reports on Defence's DRMS where Defence staff could freely access the Reports and providing a copy of the redacted Comcare Report to a consultant without the complainant's consent (Issue 3)
    - forwarding an email dated 9 August 2012 to 1270 Defence staff, with a hyperlink to the redacted Comcare Report attached to the email (Issue 4)

17. The complainant seeks a declaration by me that Defence interfered with her privacy. She seeks an apology and compensation from Defence.

18. Defence contends that it has not interfered with the complainant's privacy.

19. The OAIC commenced its investigation into the complainant's complaint on 19 August 2014 under section 40(1) of the *Privacy Act 1988* (Cth) (**the Privacy Act**). The matter was not resolved through conciliation and I have decided to determine the matter under s 52 of the Privacy Act.

17. In making my determination, I have considered these documents, provided to the OAIC by the parties during the investigation:

a. the redacted Comcare Report
b. Defence's internal email correspondence dated 9-10 August 2012
c. Defence's WHS investigation report dated 8 November 2013
d. complaint to the OAIC dated 25 July 2014
e. medical and case assessment reports provided by the complainant dated 22 August 2012; 5 September 2012; 28 September 2012; 13 October 2012; 25 October 2012 and 8 November 2012;
f. Defence's submissions dated 13 November 2014; 17 February 2015; 17 April 2015; 11 March 2016; 5 April 2016; 26 May 2016; and 11 July 2016
g. the complainant's submissions dated 8 September 2014; 14 October 2014; 1 April 2016; and 27 June 2016
h. the complainant's receipts and invoices for legal costs (provided to the OAIC on 5 October 2015)
i. additional information received from the complainant in June 2017.

The Law

18. Section 52 of the Privacy Act provides that, after investigating a complaint, I may make a determination:

    (a) dismissing the complaint (s 52(1)(a)); or

    (b) finding the complaint substantiated and declaring that:

        (i) the respondent has engaged in conduct constituting an interference with privacy of an individual and should not repeat or continue such conduct (s 52(1)(b)(i)(B));

        (ii) the respondent must perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant (s 52(1)(b)(ii));

        (iii) the complainant is entitled to compensation of any loss or damage suffered by reason of the act or practice the subject of the complaint (s 52(1)(b)(iii));

        (iv) it would be inappropriate for any further action to be taken in the matter (s 52(1)(b)(iv)).

19. As the events occurred before 12 March 2014, and Defence is an agency, the former Information Privacy Principles (IPPs) apply. The IPPs were contained in section 14 of the Privacy Act and outlined standards for handling personal information held by certain Australian Government agencies.

20. Defence is an agency for the purposes of the Privacy Act. Under section 16 of the Privacy Act, an agency is prohibited from breaching the IPPs.

First Issue - IPP 1 - collection of personal information

21. The complainant alleges that Defence breached IPP 1 by collecting the Comcare Report and its redacted version (**the Comcare Reports**).

22. IPP 1 stated that personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and the collection of the information is necessary for or directly related to that purpose.

23. Defence argues that it must employ individuals to carry out its functions as an agency and that the Comcare Report was generated because of the complainant's allegation that her service at the Land Systems Division of Defence caused or contributed to a serious illness.

The Comcare Report

24. Defence is statutorily required under the *Work Health and Safety Act 2011* (Cth) (at the relevant time, the *Occupational Health and Safety Act 1991* (Cth) (**OHS Act**) was in force) to secure the health and safety of its workers and workplaces. At the relevant time, s 53(3) of the OHS Act required Comcare to provide Defence as the employer of the complainant with a copy of the Comcare Report. I accept that to comply with its statutory obligations, Defence had to collect and assess all information in relation to the complainant's allegations including the findings of Comcare's investigation, which constituted the Comcare Report. On this basis, I am satisfied that Defence was not in breach of IPP 1 in respect of its collection of the Comcare Report.

The redacted Comcare Report

25. As I understand it, Comcare provided the redacted Comcare Report to Defence following the issuing of the Comcare Report to the complainant under FOI and the publication of the redacted Report on Comcare's disclosure log. In this circumstance the complainant's personal information contained within the redacted Comcare Report held by Defence constituted unsolicited personal information.

26. The obligations in IPP 1 do not expressly distinguish between solicited and unsolicited personal information. The advisory *Plain English Guidelines to Information Privacy Principles 1-3,*[2] which applied at the relevant time, stated that an agency still collects personal information even if someone gives information to the agency about the individual without the agency asking for it.

27. In this circumstance, I find that Defence collected the redacted Comcare Report, which was the product of an FOI application made to Comcare, as part of its assessment of the complainant's allegations of workplace health and safety issues within Defence. I am satisfied that Defence was not in breach of IPP 1 in respect of its collection of the redacted Comcare Report.

Finding – IPP 1

28. I find that Defence's collection of the Comcare Reports is not an interference with the complainant's privacy.

Second Issue – IPP 4 – storage and security

IPP 4(a)

29. The complainant alleges that, contrary to IPP4(a), Defence failed to take such security safeguards as it was reasonable in the circumstances to take to ensure the Comcare Reports (**the record**) containing her personal information were protected against loss, unauthorised access, use, modification or disclosure.

[2] Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1-3*, October 1994.

30. For the purposes of the Act, an agency was a 'record-keeper' in relation to a record that contained personal information if it had possession or control of the record. The complainant asserts that Defence stored the Comcare Reports on its computer system without appropriate access restrictions or controls.

31. When assessing the reasonableness of security safeguards, Defence maintains these factors should be taken in account:

In relation to the redacted Comcare Report:

- the redacted Comcare Report had been saved onto Defence's records management system, formerly known as DRMS, in the belief that Comcare had properly redacted it
- access to documents stored in DRMS relied on a system of privileges. The redacted Comcare Report had been saved onto DRMS in 2011 in a Land Systems Division (LSD) folder, and could only be accessed by those with LSD Objective privileges
- additional restrictions were not applied as there had been no concerns raised about the content of the redacted Comcare Report, which was publicly available on the Comcare website with no access restraints
- all individuals recorded as accessing the redacted Comcare Report were in key executive roles within LSD except for the individual who first raised concerns about an alleged 'cancer cluster' within LSD.

In relation to the Comcare Report:

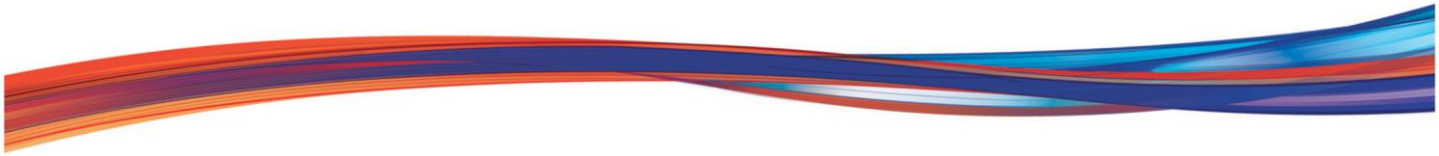
- a search of Defence's electronic records indicate that:
  - there is no evidence to suggest that the Comcare Report was saved in a general folder on DRMS
  - the Comcare Report was stored securely in folders with restricted access or folders that required security logins and passwords
  - the Comcare Report was only emailed to a small group of Defence personnel (seven individuals) involved in the original complaint and the subsequent Defence Work Health and Safety (WHS) investigation, and had a "need to know".

32. Several matters may be considered when assessing the reasonableness of steps or safeguards taken by entities to ensure information is kept secure. These include, for instance:

a. the nature and quantity of personal information held
b. the risk to the individuals concerned if the personal information is not secured
c. the data handling practices of the entity holding the information
d. the ease with which a security measure can be implemented.[3]

33. I am not aware of any specific policies or procedures Defence had in place to deal with the internal distribution of Comcare Investigation Reports. Defence has provided me with a *Communication Protocols for Defence and Comcare* document about Comcare Investigations under the OHS Act. However, this document does not provide any information about the internal circulation and/or dissemination of sensitive personal information amongst Defence personnel. Given the sensitivity of the information within

[3] 'Guide to information security: 'reasonable steps' to protect personal information', page 10



the Comcare Reports, there was a need for rigour in assessing the content of the Comcare Reports, and in considering to whom and how much of the complainant's personal sensitive information should be made available.

34. I accept that regarding the Comcare Report, only a small number of Defence personnel directly involved in investigating the complainant's complaint had access to it, and such access was provided on a 'needs-to-know' basis, with sufficient access controls and restrictions in place. I am satisfied that regarding the Comcare Report security safeguards were taken as were reasonable in the circumstances to take.

35. It seems little to no consideration was given to the contents of the redacted Comcare Report. Defence's belief that as the redacted Report was a Comcare Report, Comcare was responsible for its redaction, did not relieve Defence of its obligation to ensure the record containing that information was protected by such security safeguards as it was reasonable in the circumstances to take.

36. As I understand it, the redacted Comcare Report was placed in a general division folder, to which 1,270 staff had access. Defence's apparent unawareness of what personal information may have still existed on the redacted Comcare Report stored in a folder accessible to 1270 individuals, attests to a lack of rigour around security measures for protecting personal information, including sensitive information.

37. In my view there was insufficient consideration given to the obligations imposed on Defence staff to protect the complainant's information. Defence received the redacted Comcare Report following its publication on Comcare's FOI disclosure log. On the face of it, it was clear the document contained sensitive medical information of a Defence staff member. The redacted Comcare Report identified the complainant by name, albeit inadvertently. Reviewing the redacted Comcare Report to ensure the information contained therein did not identify the staff member before making it available to 1270 staff, may have, in this case, been a sufficient step to take in order to meet its obligations under IPP4. I do not believe there were sufficient security safeguards around protecting the redacted Comcare Report as was reasonable in the circumstances to take. On this basis, I find that Defence is in breach of IPP 4(a).

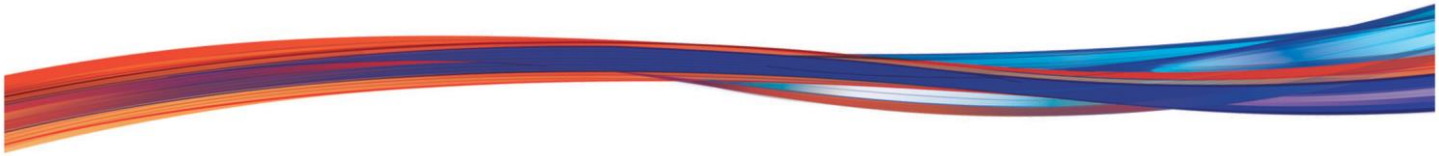
IPP 4(b)

38. The complainant alleges that Defence should have removed the identifying information from the redacted Comcare Report before providing it to the Consultant, or summarised the Comcare Report, and that by not doing so Defence has breached IPP 4(b).

39. IPP 4(b) stated that a record-keeper with possession or control of a record that contains personal information shall ensure that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

40. The Consultant had been engaged to look into alleged workplace practices including the incident of the alleged unauthorised release by email of the complainant's health information to Defence staff. Defence maintains it was therefore reasonable for the Consultant to be provided with the redacted Comcare Report as released by email to Defence staff. I agree. Accordingly, I am satisfied that Defence is not in breach of IPP 4(b) in this instance.

41. The complainant alleges that the Consultant subsequently placed the redacted Comcare Report on their investigations database. However, as the complainant has not provided any information to support this allegation, I will not consider this issue further.



Finding – IPP 4

42. I find that Defence interfered with the complainant's privacy by failing to take security safeguards as was reasonable in the circumstances to take to ensure that the redacted Comcare Report was protected against loss, unauthorised access, use, modification or disclosure.

Third Issue - IPP 10 - use of personal information

43. The complainant submits that Defence disclosed her personal information including health information to Defence staff by making the Comcare Reports available on Defence's record management system, and providing the Comcare Reports to a Consultant engaged by Defence to conduct an investigation on its behalf. As Defence did not release the Comcare Reports from its effective control, IPP 10 will apply. IPP 10 provides that a record-keeper with possession or control of a record containing personal information shall not use the information for any other purpose. There are several exceptions to this requirement, and I address relevant exceptions below.

The Comcare Report

44. Defence denies that it saved the Comcare Report onto its DRMS and made it available to LSD staff. It submits that a search of its electronic records indicate that the Comcare Report was only emailed to seven Defence personnel, all directly involved in the original complaint and the subsequent Defence Work Health and Safety (WHS) investigation. These individuals used the Comcare Report for the particular purpose for which it was obtained. Defence maintains that there is no evidence the Comcare Report was saved in a general folder on DRMS.

45. I accept that the Comcare Report was accessed and used for the purpose for which it was collected; that is, to assess the complainant's complaint and the findings of the Comcare investigation. I have no information available to me, to suggest that this is otherwise. Accordingly, I am satisfied that Defence did not interfere with the complainant's privacy when key personnel accessed and used the Comcare Report for assessment purposes and there has been no IPP 10 breach in this circumstance.

The redacted Comcare Report

46. Defence acknowledges that the redacted Comcare Report was available in a general folder, which all LSD staff could access. There were approximately 1,270 staff in the Land Services Division. Defence submits it stored the redacted Comcare Report because it had to collect and assess all relevant evidence in relation to the complainant's allegations and the findings of Comcare's investigation, which were included in the redacted Comcare Report. Defence contends that it was made accessible to all staff in LSD Division for 'transparency' purposes, because the redacted Comcare Report investigated allegations that LSD employees were being exposed to a 'cancer cluster'.[4] An audit log recorded by Defence reveals that five individuals accessed the redacted Comcare Report within the LSD folder, four of whom were 'key' LSD executives.

47. Though Defence did not seek to rely on any of the exceptions under IPP 10 in this circumstance, I have considered the IPP 10(1)(e) exception to the prohibition to use, which provides that use is permitted for a secondary purpose, where that secondary purpose is directly related to the primary purpose of collection. I am of the view that the 'transparency' purpose for which the redacted Comcare Report was made

[4] Defence submission to the OAIC, 11 March 2016, paragraph 4.28.

available to 1,270 staff was not directly related to the particular purpose for which it was obtained. To provide other employees who also worked in the Land Services Division with the complainant's health information for the purposes of making the investigation into allegations of a 'cancer-cluster' transparent, is not in my view a purpose directly related to the purpose of collection. It may have been reasonable to have provided a de-identified version of the Comcare Report, if that was possible, but that was not what occurred. I am therefore satisfied that Defence's use of the redacted Comcare Report in the circumstance of making the Report accessible to LSD staff was in breach IPP 10.

Use by the Consultant

48. The complainant contends that Defence provided copies of the Comcare Reports to the Consultant, without the complainant's consent.

49. Defence acknowledges that it contracted the Consultant to conduct an investigation on its behalf, but denies that it provided a copy of the Comcare Report to the Consultant. Given this, and because of the lack of any information to support the complainant's contention that Defence provided the Comcare Report to the Consultant, I cannot make a finding on IPP 10 in this respect.

50. This aside, Defence provided the Consultant with the redacted Comcare Report. Defence contends it did this because of the relevance of the redacted Comcare Report to the investigation the Consultant was contracted to undertake. The Consultant was engaged to investigate issues highlighted in an email sent by a Defence employee who, amongst other things, complained that the complainant's personal information had been released in an email sent by Defence. Defence maintains that for the purpose of the Consultant's investigation it was necessary for the Consultant to review exactly what was sent in that email. Defence has sought to rely on exceptions to the prohibition on use for a secondary purpose under IPP 10.1(c) and IPP 10.1(d) of the Act.

IPP 10.1(c) – required or authorised by law

51. Defence has sought to rely on IPP 10.1(c) which permitted a use for a secondary purpose where that use is required or authorised by or under law. Defends contends that under the WHS Act, as a person conducting a business or undertaking (a PCBU) it must ensure, so far as is reasonably practicable, the health and safety of workers and other persons.[5] Defence submits, and I accept, that as the 13 August 2012 email by a Defence employee alleged amongst other things workplace behaviour and practices, which could constitute bullying or harassment under the WHS Act, it had to investigate those allegations.

52. At paragraph [40] I accepted that the redacted Comcare Report related to the Consultant's investigation into the workplace practices alleged in the 13 August 2012 email. I find that Defence's use of the redacted Comcare Report for the Consultant's investigation, was authorised under law for IPP 10.1(c) and that Defence has not breached IPP 10 in this circumstance.

IPP 10.1(d) – law enforcement

53. For completion's sake, I will consider IPP 10.1(d) on which Defence also seeks to rely. IPP 10.1(d) provided that a record-keeper with possession or control of a record containing personal information, may use the information for a secondary purpose where that use is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty.

[5] Respondent's submissions, 17 February 2015, 3.

54. Defence maintains that provision of the redacted Comcare Report to the Consultant was reasonably necessary for determining whether there was a breach of the WHS Act, which contains sanctions including criminal and pecuniary penalties for breaching employer obligations under that Act. I am not however satisfied that Defence has any regulatory functions or powers for enforcement under the WHS Act or that using the redacted Comcare Report was reasonably necessary for that purpose. I am therefore not satisfied that IPP 10.1(d) applies.

Finding – IPP 10

55. I find that Defence interfered with the complainant's privacy by using the redacted Comcare Report, through making it accessible to 1,270 Defence staff for the purpose of 'transparency' while it contained the complainant's personal information, in breach of IPP 10.

Issue 4 - IPP 11 – disclosure of personal information

56. The complainant alleges that Defence improperly disclosed her personal information, including health information when it forwarded an email dated 9 August 2012 to 1270 Defence staff, with an attached hyperlink to the redacted Comcare Report.

57. IPP 11 prohibits a record-keeper with possession or control of a record that contains personal information from disclosing that information, subject to certain exceptions, which do not arise here.

58. For the purposes of the Privacy Act, a record does not include a generally available publication. Section 6 of the Privacy Act defines a 'generally available publication' to mean "a magazine, book, newspaper or other publication (however published) that is or will be generally available to members of the public". The redacted Comcare Report, although it contained the complainant's personal information, sat on the webpage of Comcare's FOI disclosure log and was available to members of the public.

59. According to the Macquarie Dictionary, a 'link' is "a hypertext connection between two documents".[6] The connection between the generally available publication and the Defence record remained functional for only as long as Comcare allowed the redacted Comcare Report to be available on its website. The link (and so the connection between the two documents) was removed by Comcare after being advised by Defence that the redacted Comcare Report contained the complainant's personal information, including health information. In these circumstances, the redacted Comcare Report was a generally available publication in Comcare's possession or control for the purposes of the Privacy Act, and was not a Defence record.

60. While I am satisfied that the 9 August 2012 email was a record in Defence's possession or control, the redacted Comcare Report to which the email was hyperlinked was not such a record.

61. The complainant suggests that Defence may have redirected the webpage from Defence records to the Comcare web location. She also alleges that the author of the email and his staff knew that the embedded link contained the complainant's personal information. The complainant has not provided enough information to support these assertions. The extent of the author's knowledge (or lack thereof) is, in any case, not determinative of a breach of IPP 11 (or IPP 10).

[6] Macquarie Dictionary, *Macquarie Dictionary Online*, 6th edition (October 2013) < https://www.macquariedictionary.com.au >.

Finding - IPP 11

62. I find that in the circumstance of the 9 August 2012 disclosure to Defence staff of an email containing a link to the redacted Comcare Report, Defence was not the record-keeper in possession or control of a record that contained the complainant's personal information. Defence is consequently not in breach of IPP 11 in this circumstance.

Findings - Remedies

63. I have found the Defence has interfered with the complainant's privacy, including by improperly using her personal information, including health information, and by failing to protect that information by such security safeguards as it was reasonable in the circumstances to take.

64. The complainant seeks a declaration she is entitled to an apology and compensation. Section 52(1)(b)(ii) provides that I can declare that the respondent must perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant. I am satisfied that in the circumstances, Defence should issue an apology. The apology should include an acceptance of responsibility for the breaches and an acknowledgement of the complainant's distress.

65. In addition section 52(1)(b)(ia) provides that I can declare that the respondent must take specified steps within a specified period to ensure that such conduct is not repeated or continued. I am satisfied that it is appropriate in the circumstances that Defence review its relevant procedures and report back to me within nine (9) months on the review and its implementation to minimise the risk of a recurrence of a similar breach. I have outlined in more detail what the review and report back should cover in the declaration below.

Damages

66. Having found that Defence has breached IPP 4 and IPP 10, I have the discretion under section 52(1)(b)(iii) of the Privacy Act to award compensation for 'any loss or damage suffered by reason of the act or practice the subject of the complaint'. Section 52(1A) provides that loss or damage can include "injury to the complainant's feelings or humiliation suffered by the complainant".

67. In assessing compensation I am guided by these principles on awarding compensation, summarised by the Administrative Appeals Tribunal (AAT) in *Rummery and Federal Privacy Commissioner*[7]:

    a. where a complaint is substantiated and loss or damage is suffered, the legislation contemplates some form of redress in the ordinary course

    b. awards should be restrained but not minimal

    c. in measuring compensation the principles of damages applied in tort law will assist, although the ultimate guide is the words of the statute

    d. in an appropriate case, aggravated damages may be awarded.

---

[7] *Rummery and Federal Privacy Commissioner and Anor* [2004] AATA 1221, [32]. In setting out the factors relevant to compensation awards under the Privacy Act, the AAT considered the Federal Court's approach to the assessment of damages under the *Sex Discrimination Act 1984* (Cth) in *Hall v A & A Sheiban Pty Ltd* [1989] FCA 72.

e. compensation should be assessed having regard to the complainant's reaction and not to the perceived reaction of the majority of the community or of a reasonable person in similar circumstances.

Economic loss

68. In *EQ and Office of the Australian Information Commissioner*[8], the AAT discusses that damages for economic loss are awarded to restore an individual to "the same position as he would have been in if he had not sustained the wrong for which he is now getting his compensation".

69. The complainant has requested compensation for economic loss, including:

    a. $5,000 for travelling costs, medication and expenses related to her medical treatment since August 2012; and

    b. $250,000 for future economic loss, based on the referral by her commanding officer for a psychiatric or psychological examination, which the complainant claims may lead to the 'cutting short' of her career.

70. At the time of the privacy breaches, the complainant was employed by Defence as a Major, Staff Officer 2, Knowledge Systems. The complainant has provided me with several medical reports, which confirm that she underwent psychological and psychiatric assessments following the privacy breaches, but she has not otherwise addressed economic loss. I have no information, which indicates the claimed loss of $5,000 results from Defence's privacy breaches. There is therefore no basis for awarding compensation for the contended economic loss.

71. The complainant also contends that Defence's breaches will probably result in the termination of her career. She claims that the privacy breaches have resulted in at least two 'administrative referrals', that is, referrals made by Defence for the complainant to undertake psychological and psychiatric assessment. The complainant contends that because the referrals are on her record, her supervisor may issue a 'show cause' why she should not be dismissed immediately from her employment.

72. The complainant claims that her posting to the Defence Community Organisation (DCO) was initially withdrawn, as a result of the administrative referral in August 2012, and then reinstated. A termination notice, calling upon her to show cause why her appointment as an officer of the Australian Army should not be terminated, was issued to her on 8 September 2014 and later withdrawn on 7 October 2015. She claims that if Defence had not breached its privacy obligations, she would not be "fighting for her job".

73. While it appears that the initial 'administrative referral' of the complainant by Defence was connected to the distress that the complainant experienced upon becoming aware that Defence had forwarded an email to staff containing a hyperlink to the redacted Comcare Report, this not an act or practice by Defence that I have found to be an interference with the complainant's privacy.

74. On the information provided, I am not satisfied that the complainant's career has been "cut short" by the specific conduct of Defence which I have found to be in breach of the Act, or that the breaches have impaired her future earning capacity. In '*EQ' and Office of the Australian Information Commissioner*, the AAT noted that "in terms of future loss, the onus remains on the Applicant 'to provide what if anything, he was now not capable of earning' (see *McCracken v Melbourne Storm Rugby Club Limited and Ors*

[8] [2016] AATA 785 (6 October 2016).

[2007] NSWCA 353)".[9] In the circumstances, I find there is no basis for awarding compensation for future economic loss.

Non-economic loss

75. Here, the complainant is seeking an award of damages for non-economic loss for $150,000. She claims that when she found out that Defence had made available the redacted Comcare Report on Defence's DRMS so all LSD staff could readily access it, she suffered "severe shock".[10] The complainant claims her symptoms, which included migraine, difficulty sleeping, severe depression and anxiety attacks continued for months after she learned of the unauthorised use.[11] She contends that the impact of Defence's interference with her privacy was made worse by the constant humiliation and embarrassment in the workplace where colleagues and others would discuss her case.[12]

76. The complainant contends that because of the misuse of her personal information by Defence she was subjected to serious and sustained bullying and harassment by Defence. I note that allegations of harassment and bullying are outside the operation of section 52 of the Privacy Act and I have no power to consider these further.

77. The complainant also argues that Defence should pay compensation for non-economic loss resulting from the decision of her commanding officer at Defence to administratively refer her for a psychiatric or psychological examination. The complainant has not however provided sufficient evidence to substantiate a causative link between Defence's privacy breaches and any losses in this respect. The complainant has provided several documents to support her claim for non-economic loss, including reports from her treating psychiatrist and psychologist, which confirm the account of her distress.[13]

78. The complainant also claims she has suffered other effects, such as severe choking at times of acute stress, and weight gain because of the privacy breaches. The complainant has not provided enough information to substantiate a causal link between these effects and Defence's breaches.

79. Because of the material in reports from her treating doctors, and the complainant's own accounts of her distress caused by Defence's interferences with her privacy, I am satisfied that it is appropriate to award damages for non-economic loss in respect of the impact of Defence's breaches. It is evident that a proportion of the complainant's distress was caused by Comcare's interference with her privacy. In the complainant's matter against Comcare, I awarded $20,000 for non-economic loss for the unauthorised disclosure of the redacted Comcare Report on Comcare's website, where the information was publicly available for over one year.[14] I am of the view however that Defence's breaches impacted on the complainant's distress even if there were other contributory causes.

80. In deciding the damages for non-economic loss, I have had regard to amounts awarded in previous privacy determinations, paying particular regard to cases of similar ilk, noting that I am not bound by

---

[9] Deputy President Melick in *EQ and Office of the Australian Information Commissioner* [2016] AATA 785 at [44].
[10] Letter from the Complainant's solicitors to the OAIC, 8 September 2014, page 1.
[11] Letter from the Complainant's solicitors to the OAIC, 8 September 2014, page 1.
[12] Letter from the Complainant's solicitors to the OAIC, 8 September 2014, page 2.
[13] Department of Defence, *Report on a case referred for a psychiatric or psychological examination*, 22 August 2012; Defence Force Psychology Organisation, *Psychological report*, 5 September 2012; Department of Defence, *Specialist report*, 13 October 2012; Department of Defence, *Specialist report*, 8 November 2012; Defence Force Psychology Organisation, *Psychological report*, 11 December 2012.
[14] *'LB' and Comcare (Privacy)* [2017] AICmr 28 (24 March 2017).

those determinations, rather by the statute itself.[15] I am also guided by AAT's decision in *Rummery* to make a declaration awarding Mr Rummery $8,000. There, the amount was awarded for loss and damage in circumstances where Mr Rummery's personal information was disclosed to the ACT Ombudsman by Mr Rummery's former employer during an investigation into a public interest disclosure Mr Rummery made to the ACT Ombudsman.

81. The circumstances of this current matter must take into account that the complainant has suffered distress because of the unauthorised access and use of her personal information, and that her information, including health information was available to 1,270 Defence staff for over one year. I also take into account that Defence's audit log records that five individuals accessed the redacted Comcare Report during that period, all of whom were in key executive roles within LSD apart from the one individual who initially raised concerns in relation to the alleged 'cancer cluster'. Accordingly, I have determined that $10,000 is an appropriate amount of non-economic compensation for the damage the lack of protection and misuse of her personal information has caused the complainant.

82. I find that Defence should pay the complainant $10,000 for the non-economic loss suffered because of Defence's interference with her privacy.

Aggravated damages

83. Section 52(1)(iii) of the Privacy Act provides me with the power to award an amount 'by way of compensation' for any loss or damages suffered as a result of the breach of the complainant's privacy. These relevantly include aggravated damages.

84. I have previously made reference to two principles which provide useful guidance in determining whether an award of aggravated damages is warranted:

- where the respondent behaved 'high-handedly, maliciously, insultingly or oppressively'
- where the manner in which a defendant conducts his or her case exacerbates the hurt and injury suffered by the complainant.[16]

85. I do not consider how Defence has conducted its case falls within these categories, to justify an award of aggravated damages. On learning that the redacted Comcare Report contained the complainant's personal information, Defence notified Comcare to make it aware, it advised staff to destroy copies they may have downloaded, and it restricted folder access to the redacted Comcare Report. Although Defence disputed it interfered with the complainant's privacy, it entered discussions with the complainant to resolve the matter.

86. The complainant alleges that Defence knowingly provided misinformation to the OAIC; however, on the information available I am not satisfied this is the case.

87. Here, I am satisfied that Defence's actions were not reflective of conduct that is high-handed, malicious, insulting or oppressive. I do not consider that it is appropriate to award the complainant aggravated damages.

---

[15] See for example *'BO' and Aerocare Pty Ltd* [2014] AICmr 32 (8 April 2014); *'KA' and Commonwealth Bank of Australia Limited* [2016] AICmr 80 (25 November 2016);

[16] '*D' v Wentworthville Leagues Club* [2001] AICmr 9 [50]; *'S' v Veda Advantage Information Services and Solutions Limited* [2012] AICmr 33 [93]; *'BO' v AeroCare Pty Ltd* [2014] AICmr 37 [57]; *'HW' v Freelancer International Pty Limited* [2015] AICmr 86 [379].

Expenses reasonably incurred

88. The complainant seeks reimbursement of her legal fees to $24,605.99.

89. Section 52(3) of the Privacy Act provides me with a discretion to declare that a complainant is entitled to a specified amount to reimburse the complaint for "expenses reasonably incurred ... in connection with the making of the complaint and the investigation of the complaint".

90. Defence, in its submissions, does not accept liability for the complainant's legal costs, referring to the OAIC's website which states:

> You do not need to be represented by a lawyer to make a complaint about your privacy. However, if you decide to hire a lawyer, you must pay for the lawyer yourself.[17]

91. Although most privacy complaints can be resolved without legal representation, I am satisfied that it was appropriate for the complainant to engage a legal professional due to the issues in contention, and that it is consequently appropriate for her to be reimbursed for legal expenses reasonably incurred in connection with her privacy complaint against Defence. Notwithstanding this, s 52(3) does not have the effect of automatically transferring a complainant's legal expenses to the respondent, and I will not exercise the discretion on every occasion on which the complainant incurs legal or other expenses.

92. In making a declaration that Defence pay the complainant a specific amount, I am guided by the principles of what is 'fair and reasonable' when courts award on a party/party basis or what appears to have been 'unreasonably incurred' or 'unreasonable in amount' when courts award on an indemnity basis. I have outlined those principles and those factors to have regard to in an assessment of 'fair and reasonable' in *'LB' and Comcare (Privacy)*.[18] An assessment of what is 'fair and reasonable' will include the labour and responsibility involved. Proportionality has also been considered by the courts as a relevant factor when assessing costs, including the notion that the amount for costs should be proportional to the outcome the successful party has obtained.[19]

93. The complainant has provided several invoices. However, I am not satisfied that it would be appropriate to reimburse the complainant for the whole of the legal expenses incurred. Not all the expenses incurred were in connection with making the complainant's privacy complaint against Defence and in the investigation of it. Moreover, the expenses incurred are disproportionate to the remedy I have awarded.

94. For the above reasons, I have decided that a portion of the complainant's legal expenses were reasonably incurred in connection with the complaint against Defence, and I have elected to exercise my discretion to declare that the complainant should be reimbursed for a portion of those expenses. I declare that under section 52(3) Defence should pay the complainant an amount of $3,000 as reimbursement for expenses reasonably incurred in the making and investigation of the complainant's privacy complaint against Defence.

Declarations

95. I declare, under section 52(1)(b)(i)(B) of the Privacy Act, that the complaint is substantiated, because the respondent, the Department of Defence:

---

[17] https://oaic.gov.au/individuals/how-do-i-make-a-privacy-complaint
[18] [2017] AICmr 28 (24 March 2017).
[19] See for example, *Ghosh v Ninemsn Pty Ltd* [2015] NSWCA 334.

i. failed to take security safeguards as were reasonable in the circumstances to protect the complainant's personal information against loss, against unauthorised access, use, modification or disclosure, and against other misuse, in breach of IPP 4.1(a), and

ii. improperly used the redacted Comcare Report that contained the complainant's sensitive information for a purpose other than the particular purpose for which it was obtained, in breach of IPP 10.1.

96. I declare, under section 52(1)(b)(ia) of the Privacy Act, that the Department of Defence must:

i. review its procedures in relation to the internal handling and dissemination of personal information, particularly sensitive information and develop and/or update processes and/or practices on the internal circulation of sensitive information focussing on document caveats and controls, and redaction processes that may apply for internal dissemination of sensitive information

ii. report to the OAIC within nine (9) months of this determination, on the results of the review and the implementing of such measures as those listed at (i) to minimise the risk of recurrence of similar breaches under the Privacy Act.

97. I declare, under section 52(1)(b)(ii) of the Privacy Act, that within 60 days of this determination, the Department of Defence must issue a written apology to the complainant, which includes an acknowledgment of the breaches and of the complainant's distress because of the Department of Defence's interference with her privacy.

98. I declare, under section 52(1)(b)(iii) of the Privacy Act, that within 60 days of this determination, the Department of Defence must pay the complainant $10,000 for loss or damage caused by its interference with the complainant's privacy.

99. I declare under section 52(3) of the Privacy Act, that within 60 days of this determination, the Department of Defence must pay the complainant $3,000 to reimburse the complainant for expenses reasonably incurred in connection with the complaint.

Timothy Pilgrim
Australian Privacy Commissioner
26 June 2017

Review rights

A party may apply under s 96 of the *Privacy Act 1988* to have a decision under s 52(1) or (1A) to make a determination reviewed by the Administrative Appeals Tribunal (AAT). The AAT provides independent merits review of administrative decisions and has power to set aside, vary, or affirm a privacy determination. An application to the AAT must be made within 28 days after the day on which the person is given the privacy determination (s 29(2) of the *Administrative Appeals Tribunal Act 1975*). An application fee may be payable when lodging an application for review to the AAT. Further information is available on the AAT's website (www.aat.gov.au) or by telephoning 1300 366 700.

A party may also apply under s 5 of the *Administrative Decisions (Judicial Review) Act 1977* to have the determination reviewed by the Federal Circuit Court or the Federal Court of Australia. The Court may refer the

matter back to the OAIC for further consideration if it finds the Information Commissioner's decision was wrong in law or the Information Commissioner's powers were not exercised properly. An application to the Court must be lodged within 28 days of the date of the determination. An application fee may be payable when lodging an application to the Court. Further information is available on the Court's website (http://www.federalcourt.gov.au/) or by contacting your nearest District Registry.