Australian Government
Office of the Australian Information Commissioner

'IR' and NRMA Insurance, Insurance Australia Limited [2016] AICmr 37 (27 June 2016)

Determination and reasons for determination of
Acting Australian Information Commissioner, Timothy Pilgrim

Complainant:	**'IR'**
Respondent:	**NRMA Insurance, Insurance Australia Limited (ABN 11 000 016 722)**
Decision date:	**27 June 2016**
Application number:	**CP14/02961, CP15/00740**
Catchwords:	**Privacy — Privacy Act —Australian Privacy Principles — *Privacy Act 1988* (Cth) s 52 —APP 6 — Use or disclosure of personal information— APP 11 — Security of personal information — Compensation awarded — Non-economic loss — Aggravated damages not awarded**

Contents

Findings

1. Insurance Australia Limited trading as NRMA Insurance (**NRMA**) interfered with the complainant's privacy by:

    - disclosing her personal information to third parties, in breach of Australian Privacy Principles (**APP**) 6 and 11 under the *Privacy Act 1988* (Cth) (**Privacy Act**)

2. NRMA did not interfere with the privacy of the complainant's husband.

3. To redress the interference with the complainant's privacy NRMA shall within six (6) weeks of the date of this determination:

    - issue an apology to the complainant acknowledging NRMA's interference with the complainant's privacy

    - remove from certificates of insurance issued to the complainant and any joint policy holder, information about the complainant's assets (i.e. policy description and number) that are not directly related to the issued policy

    - pay the complainant $3,000 for non-economic loss caused by the interference with the complainant's privacy.

4. In relation to its practice of issuing certificates of insurance that set out details of all insured assets owned by the policy holder who has the most eligible policies and longest relationship with NRMA, NRMA shall within six (6) months of the date of this determination:

    - develop revised information guides for customers, which outline in detail the type of personal information that will be disclosed on certificates of insurance
    - review its practice of disclosing policy description and number (**asset information**) on certificates of insurance, which is not directly related to the policy being issued.
    - confirm with me that information guides have been revised and its review of NRMA practices concerning the disclosure of asset information to third parties via certificates of insurance has been completed, advising me of results of the revisions and review.

Background

5. The complainant held a home building insurance policy with the respondent NRMA. The policy was held jointly with another individual (**Ms X**).

6. The complainant also held a number of other policies with NRMA, separate to the home building insurance policy held with Ms X. Those other policies were jointly held with the complainant's husband.

7. On 17 March 2014 the complainant received a Certificate of Insurance Home Building Renewal for 2014-2015 (**the Certificate**).

8. The Certificate contained details of all the complainant's assets insured with NRMA, including assets not related to the policy with Ms X.

9. Particulars included full property address, policy types and reference numbers, in a format like the following:

YOUR POLICY LIST

This is a list of policies used to determine this policy's Loyalty Discount. It is based on the policy holder who has the most eligible policies and longest relationship with us. Please contact us if you have any policies that are not listed here.

Policy Type	**Description**	**Reference (Policy) Number**
NRMA Motoring and Services	Member status	Policy number
Compulsory Third Party	Car make, model and year, as well as car registration number	Policy number
Home Buildings	Full property address: number, street name, suburb, postcode and state	Policy number
Home@50 Buildings	Full property address: number, street name, suburb, postcode and state	Policy number
Comprehensive Motor	Car make, model and year, as well as car registration number	Policy number
Comprehensive Motor	Car make, model and year, as well as car registration number	Policy number

10. A joint policy holder is entitled to receive from NRMA on request a copy of the relevant Certificate of Insurance, which includes details of all of the assets owned by the policy holder who has the most eligible policies and longest relationship with NRMA.

11. The complainant realised that when Ms X received a copy of the Certificate of Insurance she would obtain a detailed list of all the complainant's other assets insured with NRMA, which did not relate to the jointly held home building insurance policy.

12. She complained to NRMA on 2, 8 and 11 June 2014 about the details of her other assets being disclosed to the joint policy holder, Ms X.

13. Subsequent to the complainant's complaint, NRMA updated the format of its Certificates of Insurance to reduce the level of detail in the description column:

Policy Type	**Description**	**Reference (Policy) Number**
NRMA Motoring and Services	Member status	Policy number
Compulsory Third Party	Car make, model and year	Policy number
Home Buildings	Suburb, postcode and state	Policy number
Home@50 Buildings	Suburb, postcode and state	Policy number
Comprehensive Motor	Car make, model, year	Policy number
Comprehensive Motor	Car make, model, year	Policy number
Comprehensive Motor	Car make, model, year	Policy number

14. The complainant was dissatisfied with the amended format, claiming that her privacy continued to be interfered with.[1]

[1] Complainant's privacy complaint to the OAIC, 17 June 2014.

Privacy complaint and remedy sought

15. On 17 July 2014, the complainant lodged a complaint against NRMA with the Office of the Australian Information Commissioner (**OAIC**) under s 36 of the Privacy Act.[2]

16. On 6 May 2015, the complainant lodged a complaint with the OAIC on behalf of her husband who, along with the complainant, was a joint policy holder in respect of other listed assets on the Certificate.[3]

17. The complainant alleges that NRMA interfered with her and her husband's privacy by not taking steps to avoid the unauthorised disclosure of their personal information. She said:

> NRMA's policy is to include details of other insurance policies on the renewal statement, including those held jointly.
>
> As a consequence, the joint policy holder, [the party who holds the policy jointly with me] would be entitled to access a copy of the statement which would include other policies that are not held by the joint policy holder.[4]

18. NRMA has confirmed that it disclosed information about the complainant's other policies listed on the Certificate of Insurance to Ms X, but notes that this was undertaken in accordance with NRMA's normal practice.[5]

19. On 8 October 2014, the OAIC opened an investigation into the complainant's allegations under s 40(1) of the Privacy Act. The written submissions provided by both the complainant and NRMA were considered.

20. The matter was not resolved through conciliation and I decided to determine the matter under s 52 of the Privacy Act.

21. Section 52(1) provides that, after investigating the complaint, I may make a determination:
    - dismissing the complaint (s 52(1(a)); or
    - finding the complaint substantiated and make a determination that includes one or more of the following declarations:
        (i) that the respondent has engaged in conduct constituting an interference with privacy of an individual and must not repeat or continue such conduct (s 52(1)(b)(i)(B))

[2] Complainant's privacy complaint to the OAIC, 17 June 2014.
[3] Complainant's email to the OAIC, 6 May 2015
[4] Complainant's privacy complaint to the OAIC, 17 June 2014.
[5] NMRA letter to the OAIC, 18 November 2014, 2.

(ia) that the respondent must take specified steps within a specified period to ensure that such conduct is not repeated or continued

(ii) that the respondent must perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant

(iii) that the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint (s52(1)(b)(iii))

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

22. The complainant is seeking the following:

- an apology from NRMA and an acknowledgment of the breaches of privacy
- removal of the 'description' column outlined on the Certificate or whole removal of policy details that are not in the same name as the policy holder(s) of the relevant Certificate
- payment by NRMA of the renewal of one of her and her husband's NRMA insurance policies.

The Law

23. The 13 Australian Privacy Principles (**APPs**) contained in schedule 1 of the Privacy Act regulate the handling of personal information by Australian government agencies and some private sector organisations.

24. Under s 13(1) of the Privacy Act, an act or practice of an APP entity is an interference with the privacy of an individual if:

The act or practice breaches an Australian Privacy Principle in relation to personal information about the individual.

25. Personal information is defined in s 6(1) of the Privacy Act as:

information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

23. Under s 6(1) of the Privacy Act an 'APP entity' is defined to be an agency or organisation. An organisation is defined in s 6C to mean:

a) an individual; or

b) a body corporate; or

c) a partnership; or

d) any other unincorporated association; or

e) a trust

that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.

24. NRMA falls within the definition of an 'organisation' under s 6C, being a body corporate which is not a small business operator, a registered political party, a State or Territory authority or a prescribed instrumentality of a State or Territory.

25. APP 6 outlines when an APP entity may use or disclose personal information. Specifically, an APP entity may use or disclose an individual's personal information when it is done for the same purpose for which the information was collected (the primary purpose). Use or disclosure for another purpose (a secondary purpose) is only permitted where the individual has consented to the use or disclosure of the information or where an exception applies to the use or disclosure.

26. Those exceptions to the prohibition of use or disclosure are found in APP 6.2. Relevantly in this case, APP 6.2(a) provides that an entity may use or disclose personal information for a secondary purpose if:

- the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is (if the information is not sensitive information) related to the primary purpose.

27. APP 11 deals with the security of personal information and APP 11.1. requires an APP entity to take such steps as are reasonable in the circumstances to protect personal information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

Alleged Breach of APP 6

Complaint made on behalf of complainant's husband

28. The complainant on behalf of her husband contends that NRMA improperly disclosed his personal information to Ms X on the 17 March 2014 Certificate of Insurance Home Building Renewal for 2014-2015.

29. According to the complainant, the policies listed on the Certificate (aside from the home building insurance policy held with Ms X) are jointly held with her husband.

30. For information to constitute 'personal information' for the purposes of the Privacy Act, the information must be … 'about an identified individual, or an individual who is reasonably identifiable…'.[6]

[6] *Privacy Act 1988* (Cth), s 6.

31. In order for the complainant's husband to be 'an identified individual' one would need to look at the information on the Certificate and know or perceive plainly and clearly that it was information about the complainant's husband.

32. According to NRMA, for the policies to be listed on the Certificate, each policy must have at least one common insured name. The Certificate discloses the policy type, a description of the assets insured and the policy numbers. It does not name the policy holders.

33. It is reasonable to conclude that Ms X would be aware that the complainant was a holder of the listed policies. However, there is no information on the Certificate which indicates whether or not the listed policies (aside from the home building insurance policy to which the Certificate pertains) are solely or jointed held, and if jointly held, who the other policy holder might be.

34. In other words, there is no information on the Certificate that plainly and clearly identifies the complainant's husband.

35. The APP guidelines issued by Information Commissioner, which outline the mandatory requirements of the APPs, as well as how the OAIC will interpret the APPs and matters the OAIC may take into account when exercising functions and powers under the Privacy Act (**APP guidelines**), consider the meaning of 'reasonably identifiable'.[7]

36. Whether or not an individual is 'reasonably identifiable' from particular information about that individual will depend on considerations including: 'the nature and extent of the information, the circumstances of its receipt, and whether it is possible for the person or entity that holds or has access to the information to identify the individual using available resources'.[8]

37. There is no information before me which suggests that Ms X would be able to use the asset descriptions and policy numbers of other listed policies to identify whether or not those other policies were held solely or jointly by the complainant, and if jointly held, that the joint policy holder was the complainant's husband.

38. NRMA has confirmed that Ms X would not be able to obtain any further information about the complainant's other listed policies, other than the information already provided on the Certificate of Insurance.[9]

---

[7] Office of the Australian Information Commissioner, *APP Guidelines,* Key Concepts (March 2015), [B.91] – [B.93] <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-keyconcepts#personal-information>.

[8] *APP Guidelines*, [B.91]

[9] NRMA letter to the OAIC, 18 November 2014, 3.

39. The complainant herself may be able to use the policy information on the Certificate with other information available to her to identify her husband. The information relating to other listed policies is also her personal information as the joint policy holder of those policies.

40. There is however nothing from the description of the listed policies on the Certificate which identifies the complainant's husband, or from which the complainant's husband is reasonably identifiable to anyone with the exception of the complainant herself.

41. Accordingly, I am of the view that the details of the policies listed on the Certificate do not constitute the personal information of the complainant's husband. I find therefore that there has not been an interference with the privacy of the complainant's husband, and the practice complained of does not amount to a privacy breach.

42. I dismiss the complaint made on behalf of the complainant's husband under s 52(1)(a) of the Privacy Act.

Complaint about the disclosure of the complainant's personal information

43. The complainant alleges a breach of APP 6 on the basis that her personal information was improperly disclosed to Ms X, and NRMA cannot rely on any exceptions to the prohibition of disclosure under the Privacy Act.

44. NRMA does not dispute that it disclosed the complainant's personal information to Ms X.[10]

45. It claims that it is NRMA's standard practice to list all of the eligible policies of one policy holder on certificates of insurance and to disclose this information to the joint policy holder of the policy in respect of which a certificate of insurance is issued. It contends that the format of the certificates of insurance was designed in response to feedback provided by NRMA customers.[11] NRMA claims that as a result of the format of the certificates of insurance NRMA customers are able to check that the number of policies listed is the same number of policies that a customer has with NRMA.

46. According to NRMA this ensures that customer data is accurate, complete and up-to-date, and guarantees that customers receive the maximum benefit available to them through NRMA's loyalty discount scheme, a discount initiative that was introduced in March 2014.[12]

47. NRMA claims that its disclosure of the complainant's insurance policy information on the Certificate of Insurance provided to both the complainant and Ms X is

[10] NRMA letter to the OAIC, 18 November 2014, 2.
[11] NRMA letter to the complainant, 2 July 2014.
[12] NRMA letter to the OAIC, 18 November 2014.

commensurate with the terms of NRMA's privacy policy and its Product Disclosure Statements (**PDS**).[13]

48. It submits that:

> ..because insureds are clearly informed:
>
> - via their PDS, that their COI (Certificate of Insurance) will contain information to assist them in ensuring they are receiving the correct discounts; and
> - via [NRMA's] Privacy Policy that their personal information may be disclosed to a joint insured
>
> ..it would [be] reasonable to expect us to print the list of businesses that directly contributes to that joint policy holder's Loyalty Discount, on the dually-addressed contractually binding document.[14]

49. In this regard, NRMA contends that its practice is permitted under APP 6.2(a) where the insured would reasonably expect NRMA to disclose their personal information on the certificate of insurance for the secondary purpose of ensuring they receive the maximum discount they are entitled to.

Findings in relation to alleged breach of APP 6

50. As noted NRMA's standard practice is to detail on a certificate of insurance issued in respect of a particular policy a list of all eligible policies that contribute to a customer's loyalty discount.

Related secondary purpose

51. The APP 6.2(a) exception to the disclosure of personal information is limited to disclosing the information for a secondary purpose that is related to the primary purpose of collection.

52. NRMA's privacy policy in place at the time of the alleged improper disclosures in March 2014 (**NRMA's privacy policy**) lists the purposes for which it and its agents, distributors and related entities may collect, hold, use and disclose personal information.[15] These purposes include its primary purpose of providing customers with a product or service (including the issuing, renewing or amending of a policy).[15] The privacy policy also lists 'pricing a policy, offering excesses and discounts' as a purpose for which NRMA may handle personal information.

---

[13] NRMA letter to the OAIC, 18 November 2014, 2.
[14] NRMA letter to the OAIC, 18 November 2014, 2.
[15] NRMA, *Privacy Policy* (11 January 2014) NRMA, *Privacy Policy* (11 January 2014) http://www.nrma.com.au/sites/default/files/NRMA-Documents/NRMA_Privacy_Policy_11Jan2014.pdf>.

53. For a purpose to be a related secondary purpose it must be connected to or associated with the primary purpose.[16] The APP guidelines provide that 'there must be more than a tenuous link'.[17]

54. NRMA contends that to ensure a customer's loyalty discount rate is correctly calculated, it is important to show customers a list of their policies so that they can check that the number listed is correct. NRMA argues that showing its customers their list of insured assets at renewal time via a customer's certificate of insurance is a business initiative to maximise the accuracy of customer data matching:

> We know from analysis of our customer records that there are some inaccuracies in our customer data matching. This means that even though an individual NRMA Insurance customer may have x amount of insurance policies with us, our system may not always match those policies back to one individual (e.g. we may not always know that John Smith of Potts Point is also John Smithe who recently moved to Glebe). This error rate is due to a number of causes, which include customers changing their names or addresses without informing us, customer data sitting on different systems, and typing or spelling errors. While this error rate does not affect a customer's insurance cover, it can affect things such as their Loyalty Discount rate.[18]

55. The Certificate issued to the complainant and Ms X provides, at page 2 under the heading 'Your Policy List', a list of policies. It states that the list of policies is:

> …. used to determine this policy's Loyalty Discount. It is based on the policy holder who has the most eligible policies and longest relationship with us. Please contact us if you have any policies that are not listed here.

56. I accept that the act of *using* the complainant's policy information to calculate the maximum discount she and Ms X are entitled to under the loyalty discount scheme is for a related secondary purpose. I also accept that NRMA's practice of disclosing policy information on certificates of insurance is associated with the calculating of a correct discount for the customer. However, the connection between disclosing the full extent of information about the complainant's other policies, such as the detailed information about the assets to which the policies related, to Ms X and NRMA's calculation of the discount Ms X and the complainant, as joint holders of one policy might be entitled to, is in my view, tenuous.

Reasonably expects

57. For the disclosure of personal information to be permitted under APP 6.2(a), the act or practice of disclosure must not only be for a related secondary purpose, but must also

[16] *APP guidelines*, [6.24]-[6.25].
[17] *APP guidelines*, [6.24].
[18] NRMA letter to the OAIC, 18 November 2014, 1.

be within the reasonable expectations of the individual whose information is being disclosed.

58. The APP guidelines provide that:

> The 'reasonably expects' test is an objective one that has regard to what a reasonable person, who is properly informed, would expect in the circumstances.[19]

59. I have examined NRMA's privacy policy to determine whether or not the complainant would 'reasonably expect' the disclosure of her asset information to Ms X via the Certificate for the secondary purpose of determining the discount available to her and Ms X on the jointly-held policy.

60. The privacy policy lists, at Table A, those entities through which NRMA may collect an insured's personal information. These entities included 'a joint insured on [an insured's] policy'.

61. Page 3 of NRMA's privacy policy under the heading '*The purposes for which we collect, hold, use and disclose personal information*' states:

> We and Our Parties may:
> - hold and use your personal information, and
> - disclose your personal information to the Entities listed in Table A.

62. I accept that customers are notified by NRMA through its privacy policy that personal information may be disclosed to joint policy holders.

63. NRMA claims that the disclosure of a joint policy holder's personal information to the other joint policy holder is minimal and must be weighed against the benefit to customers being able to confirm the list of policies as accurate, complete and up-to-date, and ensuring they receive the maximum benefit they are entitled to.

> We constantly work on initiatives to maximise the accuracy of our customer matching, which helps ensure our customers get the discount they are entitled to. One initiative has been to allocate full-time resources to analyse and better match our customer data. Another initiative we have found that works effectively is to be transparent, and show our customers their list of businesses so they can check the number of policies they have with us is correct. [20]

[19] *APP Guidelines*, [6.20].
[20] NRMA letter to the OAIC, 18 November 2014, 2.

64. NRMA's Premium Excess and Discount (**PED**) guides in place at the time of the alleged improper disclosures in March 2014 provided the following information:[21]

Loyalty Discount

Your Loyalty Discount is based on how long you have had a relationship with us and how many eligible policies you have. This discount is determined for each individual customer and applied across all your eligible policies.

…

To receive a Loyalty Discount, the eligible policies must:

- be current; and
- have at least one common insured named on each policy. …

On renewal your Certificate of Insurance will show a list of what policies contributed to your Loyalty Discount.

The following is a list of the policies that:

- contribute to your policy count
- are eligible to receive the Loyalty Discount.

Policies	**Policy Count**	**Discount applied**
Motor		
Comprehensive Plus	✓	✓
Comprehensive	✓	✓
Third Party Fire and Theft	✓	✓
Third Party Property Damage	✓	✓
Veteran, Vintage and Classic Vehicle	✓	✓
Home		
Buildings	✓	✓
Contents	✓	✓
Buildings and Contents	✓	✓
Landlord		
Buildings	✓	✓
Contents	✓	✓
Building and Contents	✓	✓
On-site Caravan	✓	✓
Touring Caravan	✓	✓
Boat	✓	✓
Retail Business Insurance	✓	✗
Transport Accident Insurance	✓	✓
Compulsory Third Party (CTP)	✓	✗

[21] For example, NRMA, *NRMA Motor Insurance Premium, Excess and Discounts Guide* <https://www.nrma.com.au/sites/default/files/NRMA_MOTPED_0314.pdf>.

65. NRMA has advised that although the complainant would not have received a PED guide in the mail pack with the Certificate, it is a document which is available online or on request.[22] It is also referenced in the relevant PDSs (including the Supplementary PDSs) provided to policy holders with the issuing of their certificates of insurance:[23]

> For full details on the discounts you may be eligible for, refer to our NRMA Home [/Landlord] Insurance Premium, Excess, Discounts & Benefits Guide. You can get a copy by visiting www.nrma.com.au/homeped or contacting us on 132 132.[24]

66. It is clear that customers are notified by NRMA that the certificates of insurance will show a list of the policies that have contributed to their loyalty discount. Accordingly, it seems that a reasonable person who is properly informed might expect NRMA to provide some personal information concerning them in jointly-held certificates where they are one of the joint holders.

67. I also accept that one way customers may be able to 'check the number of policies they have with [NRMA] is correct'[25] and also check their data is accurate, up-to-date and complete, is for the certificates of insurance to show a list of what policies NRMA has considered in its calculation of customer discounts.

68. That said, NRMA has not explained why personal information that contributes to the loyalty discount offered to joint-holders, but that is otherwise unrelated to the policy being issued, is disclosed to the joint policy holder who has no connection with the information. For instance, it does not assist the joint policy holder to have access to listed policies that do not belong to them. The joint policy holder is unable to check that such data is accurate, up-to-date or complete, or that the information listed is correct.

69. Secondly, even though a reasonable person who is properly informed might expect NRMA to disclose some of their personal information in certificates of insurance to other joint holders, there is no information before me to suggest that customers would expect disclosure of their asset details to a joint holder when the joint holder is not in any way connected to those assets. NRMA has not given any reason why a joint holder could not simply be advised that they are eligible for a loyalty discount because of the number of policies held by the other joint policy holder. Nor has NRMA explained why policy numbers alone (rather than car model and makes, and property location) are not sufficient for the purpose of checking the accuracy of the data held by NRMA.

---

[22] NRMA email to the OAIC, 1 February 2016.
[23] NRMA email to the OAIC, 1 February 2016.
[24] NRMA Home Insurance Buildings & Contents Supplementary Product Disclosure Statement (ed. 2.2); NRMA Landlord Insurance Supplementary Product Disclosure Statement (ed. 2.2).
[25] NRMA letter to the OAIC, 18 November 2014, 2.

70. Section 6.21 of the APP guidelines states that:

> An APP entity should consider whether an individual would reasonably expect it to use or disclose for a secondary purpose only some of the personal information it holds about the individual, rather than all of the personal information it holds. T*he entity should only use or disclose the minimum amount of personal information sufficient for the secondary purpose* (italics added).[26]

71. There is no information in the PED guide which suggests any more detail is to be provided on the certificates of insurance than that tabled under the heading 'Loyalty Discount' and set out at paragraph [65] above. Customers are advised that it is the number of policies a customer holds that enables NRMA to correctly calculate the loyalty discount rate that a customer is entitled to. Customers are not advised that a detailed description of insured assets will also be disclosed on the certificates.

72. In my view providing on a certificate of insurance a detailed description of assets that are unrelated to the policy for which a certificate is issued, is not consistent with the notice provided in the PED guides about what information to expect on a certificate of insurance. There is no information before me to suggest that the complainant should have reasonably expected that descriptions about other assets unrelated to the policy in respect of which the Certificate was issued would be disclosed to the extent they were.

73. I am of the view that NRMA cannot rely on APP 6.2(a) to justify the extent of its disclosure of the complainant's personal information. I am not satisfied that there is sufficient connection between the extent of the disclosure of the information about the complainant's other policies, to the joint policy holder, such as the detailed information about the assets to which those policies related, and the purpose of calculating the loyalty discount. In any case, whether or not disclosure was for a secondary related purpose, it was not commensurate with the complainant's reasonable expectations.

74. I do not consider any other exception in APP 6 permitted disclosure of the complainant's personal information to this extent. I therefore find that NRMA failed to comply with APP 6.1 when it disclosed the complainant's personal information on the joint Certificate of Insurance.

Alleged Breach of APP 11

75. The complainant also alleges NRMA breached APP 11 by not taking reasonable steps to protect her personal information from unauthorised access or disclosure to Ms X.

[26] APP Guidelines, [6.21]

76. The complainant contends that the inclusion of the description column on the Certificate, which describes her insured assets with NRMA, including those which are not insured jointly with Ms X, is not a reasonable step in securing her personal information against unauthorised access or disclosure.

77. The NRMA does not dispute that the complainant's information was disclosed to Ms X via the Certificate. It claims that this practice of disclosure of asset information on the certificates of insurance is intentionally done to assist customers to easily confirm their information is accurate, up-to-date and complete.[27] The reasoning behind NRMA's practice is outlined at paragraphs [55] and [64] above.

78. NRMA argues that the disclosure of the complainant's asset information is limited to the information provided in the Certificate. It contends that such a disclosure could not result in any adverse consequences for the complainant because Ms X could not obtain any more personal information about the complainant from those policy details:

> …[the joint policy holder] would not be able to obtain any further information about [the complainant's] policies, other than the information provided in the joint Certificate of Insurance, unless she fraudulently represented herself to be [the complainant], or she was an authorised third party on the complainant's policies. [28]

Findings in relation to alleged breach of APP 11

Taking reasonable steps

79. NRMA argues that its practice of disclosing the asset information of policy holders on certificates of insurances is not an unreasonable step to take in terms of the protecting customers' information against any inaccuracies with respect to the personal information that NRMA holds about them.

80. It states that it has made a considered decision to limit the disclosure of asset information while still keeping that information useful to customers:

> You will note that the information such as a car's registration number and the specific address of a property is not disclosed.[29]

81. The complainant argues that to meet its obligations under APP 11, NRMA should further limit the disclosure of information (i.e. not provide information about the make, model and year of insured cars or about the suburb in which insured properties sit).

[27] NRMA letter to the OAIC, 18 November 2014, 2
[28] NRMA letter to the OAIC, 18 November 2014, 2
[29] Fuller disclosure was provided in certificates of insurance prior to the complainant's initial complaint to NRMA in June 2014.

82. What I must consider under APP 11 is whether or not NRMA has taken reasonable steps to protect the complainant's personal information against misuse, interference and loss, and from unauthorised access, modification or disclosure.

83. The APP guidelines outline some of the circumstances that affect the assessment of reasonable steps:

> The 'reasonable steps' that an APP entity should take to ensure the security of personal information will depend upon circumstances that include:
>
> - the nature of the APP entity
> - the amount and sensitivity of the personal information held
> - the possible adverse consequences for an individual in the case of a breach
> - the practical implications of implementing the security measure, including time and cost involved
> - whether a security measure is in itself privacy invasive.[30]

84. NRMA contends that to ensure customers receive the benefit of any discounts to which they are entitled and to provide a way customers can check whether or not their information held by NRMA is accurate, some impact on an individual's privacy may be justified.

85. While I note the objects of the Act recognise that the protection of the privacy of individuals must be balanced with the interests of entities carrying out their functions or activities[31], NRMA's contention that disclosure in this instance is a standard business practice is not an alternative to it meeting its obligations under the Privacy Act. If I find that NRMA's business practice falls short of the requirements under the Act, then I may consider the entity in breach, and the business practice an interference with an individual's privacy.

Sensitivity of personal information

86. Although financial information is not classified as 'sensitive information' for the purposes of the Privacy Act, it is generally accepted that such information is 'more sensitive' than other kinds of information. As a result, individuals often expect this type of information to be subject to a higher level of protection. This expectation is reflected in protections in the Privacy Act relating to credit reporting information and tax file numbers.[32]

---

[30] APP guidelines Chapter 11: APP 11 – Security of personal information,3.

[31] *Privacy Act 1988* (Cth), s2A.

[32] Office of the Australian Information Commissioner, *Guide to securing personal information* (January 2015) <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>.

Adverse consequences

87. NRMA asserts that the disclosure of the complainant's asset information to Ms X does not hold any real adverse consequences for the complainant. It notes that even if a joint policy holder was armed with a co-holder's asset information to the extent currently provided on the certificates of insurance, the risk of that information being subject to misuse, interference and loss, or unauthorised access, modification or disclosure, is not heightened.[33]

88. Despite this contention NRMA does concede the possibility that Ms X, if she represented herself fraudulently, may be able to gain unauthorised access to further personal information. [34]

89. I think it is clear that the more information disclosed about a person, the more vulnerable they become to misuse of, interference with or inappropriate access to, their information.

Practicality

90. The practicality of implementing a security measure, including time and cost involved, will influence the reasonableness of taking that step.[35] Firstly, as I said before, NRMA has not explained how disclosing the complainant's personal information to the joint holder via the Certificate can assist the joint-holder to check the accuracy of the information NRMA holds about her.

    Additionally, NRMA has not explained why less information might not be just as valuable helping customers like the complainant to check the accuracy of their information and receive the benefit of the discount scheme.

91. As noted in the certificates of insurance themselves, as well as the PDS and the PED guides, the loyal discount scheme benefits are linked to the *number* of policies any particular customer may have with NRMA. There is no information to suggest that the type of car someone owns, or the suburbs in which owned properties might sit, has an effect on how much discount a customer might receive under the discount scheme.

92. Providing less information may be a reasonable and practicable step towards protecting customer information from misuse, or unauthorised access or disclosure. There is nothing to suggest for example that simply checking policy numbers against policy types (i.e. altogether removing the descriptor column from certificates of insurance) would not achieve the same business aims for NRMA.

---

[33] NRMA letter to the OAIC, 18 November 2014, 2.

[34] NRMA letter to the OAIC, 18 November 2014, 2. See also paragraph [78] above.

[35] Office of the Australian Information Commissioner, *Guide to securing personal information (*January 2015) <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>.

93. Alternatively notice to policy holders at the time of joining or policy renewal would provide policy holders with an opportunity to feedback to NRMA concerns they may have about intended disclosures on the certificates. NRMA does not provide notice that details of all insured assets, along with policy types and policy numbers, will be disclosed on the certificates of insurance. Notice in itself may be a reasonable (and practicable) step towards protecting customer information from misuse, or unauthorised access or disclosure.

94. Accordingly, I am of the view that NRMA has failed to comply with APP 11 by not taking reasonable steps (those steps being, not least, the provision of notice to the complainant) to protect the complainant's personal information from misuse, or unauthorised access or disclosure.

Finding on damages

95. The complainant states that she has experienced anxiety and distress at the disclosure of her (and her husband's) investment property location and car ownership details to Ms X.[36] She seeks compensation for non-economic loss by way of payment of the renewal of one of her insurance policies.

96. I have a discretion under s 52(1)(b)(iii) of the Privacy Act to award a specific amount 'by way of compensation' for 'any loss or damage suffered by reason of' the interference with privacy'. Section 52(1A) states that loss or damage can include 'injury to the complainant's feelings or humiliation suffered by the complainant'.

97. Aside from her statement the complainant has not submitted any other evidence to support her claim. Notwithstanding this, I am guided by the following principles on awarding compensation, summarised by the Administrative Appeals Tribunal (AAT) (Full Tribunal) in *Rummery and Federal Privacy Commissioner*: [37]

- where a complaint is substantiated and loss or damage is suffered, the legislation contemplates some form of redress in the ordinary course
- awards should be restrained but not minimal
- in measuring compensation, the principles of damages applied in tort law will assist, although the ultimate guide is the words of the statute
- in an appropriate case, aggravated damages may be awarded
- 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. [38]

[36] Complainant email to the OAIC, 30 April 2015.
[37] *Rummery and Federal Privacy Commissioner* [2004] AATA 1221 [32].
[38] *Rummery and Federal Privacy Commissioner* [2004] AATA 1221 [32].

98. Accordingly, I have considered and given weight to the statement made by the complainant. I have also had regard to the type of information that has been disclosed to the joint policy holder. Although it does not constitute sensitive information for the purposes of the Privacy Act, financial information does constitute personal information which is 'more private' than other kinds of information. I therefore accept that there may be some instances where disclosure of customers' insured asset information to persons unrelated to those assets may cause some distress or concern.

99. I am satisfied that NRMA's practice of disclosing the complainant's personal information on the certificates of insurance has caused the complainant some anxiety and distress and that an award of damages is consequently appropriate.

100. In all the circumstances I consider it appropriate to award the complainant $3,000 in compensation for non-economic loss. In forming this view, I have taken into account the considerations identified in *Rummery*[39], as well as amounts awarded in previous Privacy Act determinations and amounts awarded or settled on in discrimination cases as outlined in *Federal Discrimination Law Online*[40] and the Conciliation Register of the Australian Human Rights Commission.[41]

101. In those matters to which I have had regard, amounts have been awarded in the range of:

- $8000 for injury to a complainant's feelings when he learned of the details of disclosures by an officer of his former employ to the ACT Ombudsman about his character and conduct[42]

- $5000 to compensate for the heightened anxiety and stress a complainant suffered as a result of the Department of Defence's unauthorised disclosure of a psychologist's report to the complainant's treating doctor[43]

- $2500 for the humiliation and embarrassment suffered by a complainant as a result of an improper disclosure of his army record to his new employer[44]

- $2000 for distress and anxiety caused to a complainant by reason of Veda's failure to take reasonable steps to ensure that her personal information

---

[39] *Rummery and Federal Privacy Commissioner* [2004] AATA 1221 [32].
[40] Australian Human Rights Commission, *Federal Discrimination Law* (2011) www.hreoc.gov.au/legal/FDL/index.html, ch 7 at 20 March 2014.
[41] Australian Human Rights Commission, *Conciliation Register*, http://www.humanrights.gov.au/complaints/conciliation-register
[42] *Rummery and Federal Privacy Commissioner* [2004] AATA 1221, [32].
[43] *'CP' v Department of Defence* [2014] AICmr 88.
[44] *'A', Complainant and the Secretary, Department of Defence* [1993] PrivCmr ACD 1 (22 December 1993).

contained in the complainant's credit file was accurate, up-to-date, complete and not misleading.[45]

102. The complainant in this case suffered distress and anxiety as a result of NRMA's practice of allowing the joint policy holder to access information about the assets insured by the complainant. Taking into account the considerations identified in *Rummery*[46], I have given significant weight to the complainant's evidence about her distress and anxiety. I note that comparable cases in terms of the distress and anxiety suffered by the complainant have awarded amounts in the lower range of between $2000 and $4000.

103. I have also taken into account that financial information may be considered 'more sensitive' than other personal information, and that the disclosure was an overt disclosure to a known third party. In my view a modest, but not insignificant, amount of compensation in the sum of $3000 should be given to the complainant in recognition of her anxiety and distress.

Aggravated damages

104. The power to award damages in s 52 of the Privacy Act includes the power to award aggravated damages in addition to general damages.[47]

105. Aggravated damages may be awarded where:

- the respondent has behaved 'high-handedly, maliciously, insultingly or oppressively'
- manner in which a respondent conducts his or her case may exacerbate the hurt and injury suffered by the plaintiff.[48]

106. In *'HW' v Freelancer International Pty Limited*[49] I awarded aggravated damages in the amount of $5000. In that case I found that Freelancer demonstrated a repeated disregard for the complainant's privacy rights and its own privacy obligations, which escalated and prolonged the distress caused to the complainant.

107. In the case presently before me, there is no evidence to suggest that the disclosure was high-handed, malicious or oppressive. I note that the NRMA had made an offer of compensation. While that amount of compensation was rejected, NRMA's conduct in this proceeding has nevertheless been conciliatory and I do not consider there is any basis for awarding aggravated damages.[50]

---

[45] *'S' and Veda Advantage Information Services and Solutions Limited* [2012] AICmr 33.
[46] *Rummery and Federal Privacy Commissioner* [2004] AATA 1221 [32].
[47] *Rummery and Federal Privacy Commissioner and Anor* [2004] AATA 1221, [32].
[48] *'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].
[49] [2015] AICmr 86.
[50] *Elliott v Nanda & Commonwealth* [2001] FCA 418, [180].

Determination

108. I declare in accordance with s 52(1)(a) of the Privacy Act that the complaint made by the complainant on behalf of the complainant's husband is dismissed.

109. I declare in accordance with s 52(1)(b)(i)(B) of the Privacy Act that:

- the complaint made by the complainant about her own personal information is substantiated

- that NRMA has breached APP 6 by improperly disclosing personal information about the complainant to a joint policy holder on a certificate of insurance

- that NRMA has breached APP 11 by not taking reasonable steps to secure the complainant's personal information on the jointly issued certificate of insurance against misuse, and unauthorised access or disclosure.

110. I declare in accordance with s 52(1)(b)(ii) of the Privacy Act that within six (6) weeks of this determination NRMA must:

- issue a written apology to the complainant acknowledging its interference with the complainant's privacy

- remove from certificates of insurance issued to the complainant and any joint policy holder, information about the complainant's assets that are not directly related to the issued policy

- pay the complainant $3,000 for non-economic loss caused by the interference with the complainant's privacy

111. I declare in accordance with s 52(1)(b)(iii) that the complainant is entitled to $3,000 for the non-economic loss suffered as a result of NRMA's interference with her privacy.

112. I further declare in accordance with s 52(1)(ia) of the Act that in relation to its practice of issuing certificates of insurance that set out details of all insured assets owned by the policy holder who has the most eligible policies and longest relationship with NRMA, NRMA shall within six (6) months of this determination:

- develop revised information guides for customers, which outline in detail the type of personal information that will be disclosed on certificates of insurance in compliance with APP 6 and APP 11 of the Privacy Act

- review its practice of disclosing asset information on certificates of insurance, which is not directly related to the policy being issued

- confirm with me that information guides have been revised and its review of NRMA practices concerning the disclosure of asset information to third parties via certificates of insurance has been completed, advising me of results of the revisions and review.

Timothy Pilgrim
Acting Australian Information Commissioner
27 June 2016

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.