Australian Government
Office of the Australian Information Commissioner

'DO' and Department of Veterans' Affairs [2014] AICmr 124 (13 November 2014)

Determination and reasons for decision of Privacy Commissioner, Timothy Pilgrim

Applicant:	**'DO'**
Respondent:	**Department of Veterans' Affairs**
Determination date:	**13 November 2014**
Application number:	**C15933**
Catchwords:	**Privacy — Privacy Act — Information Privacy Principles — (CTH) *Privacy Act 1988* s 52 — IPP 11.1 — Use and disclosure — 11.1(a), 11.1(c), 11.1(d) 11.1 (e) — Exceptions**

Summary 2
Background 2
Scope of complaint 5
The law 5
Investigation process 7
Claims 1 and 2: Disclosure of personal information to an ADF Senior Medical Officer and the Head of Joint Health Command in the Department of Defence on 20 October 2011 7
Information Privacy Principle (IPP) 11.1(a) 7
Information Privacy Principle (IPP) 11.1(c) 8
Information Privacy Principle (IPP) 11.1(d) 14
Information Privacy Principle (IPP) 11.1(e) 15
Findings 16
Claim 3: Disclosure of personal information to Chief of Air Force on 28 October 2011 16
Information Privacy Principle (IPP) 11.1(a) 16
Information Privacy Principle (IPP) 11.1(c) 19
Information Privacy Principle (IPP) 11.1(e) 20
Findings 20
Damages 20
The Department's participation in the OAIC's complaint handling process of this complaint 20

Determination 21

Summary

1. The Department of Veterans' Affairs (the Department) interfered with the complainant's privacy by disclosing his personal information, in breach of Information Privacy Principle (IPP) 11.1 of the *Privacy Act 1988* (Cth) (the Privacy Act).[1]
2. To redress this matter:
    - The Department shall apologise in writing to the complainant within two weeks of this determination.
    - The Secretary will initiate a review of the management of privacy complaints and advise me of the results of that review no later than two months from the date of this determination. In undertaking this review, particular consideration should be given to the steps undertaken by the Department in handling this matter.

Background

3. The complainant, a former Australian Defence Force (ADF) member, is a client of the Department.
4. The complainant had lodged compensation claims with the Department and was dissatisfied with the Department's management of those claims. The complainant wrote to the Department to express his dissatisfaction[2] and created a website[3] on which he outlined his criticisms of the Department's handling of his claims.
5. During September and October 2011, in particular, the complainant expressed anger and frustration about his engagement with the Department in a series of communications with the Departmental officers via email, phone and sms text messages.
6. The following events occurred leading up to the complainant's lodgement of his complaint to the Office of the Australian Information Commissioner (the OAIC)[4]:

[1] The Privacy Act was amended on 12 March 2014 and replaced the Information Privacy Principles (IPPs) with the Australian Privacy Principles (APPs). However, as the complaint relates to events that occurred prior to this date, it will be determined in accordance with the Privacy Act and the IPPs in effect at the time of the alleged events.

[2] The Office of the Australian Information Commissioner was provided excerpts of particular email exchanges between the complainant and the Department between August 2011 and October 2011.

[3] On an email dated 30 September 2011, the complainant advised that he created the website and provided a link to the website. The website appears to have been taken down during 2012-2013.

[4] The sequence of events is based on the information provided by the Department, in particular the contemporaneous note of disclosure written by Director Security and Personnel recording reasons for disclosure to RAAF Security Police (21 October 2011); the internal email communications between Departmental staff and communications with the complainant (21 October 2011); the note of disclosure written by Acting General Manager Support of the Department summarising the reasons for disclosure to ADF medical staff and the Head of Joint Health Command (22 October 2012), and the Department's submissions (various dates).

Date	Event
19 October 2011	• The complainant sent emails and text messages to the work email addresses and work mobile phones of Departmental staff that were drawn to the attention of the Department.[5]
20 October 2011	• The Department's Acting General Manager Support (GMS)[6] sought advice from the Department's Principal Medical Adviser (PMA). • The GMS also engaged its security area to conduct a risk assessment.[7] • The PMA contacted a Senior Medical Officer (SMO) in the ADF (the complainant's place of employment) 'to understand better the nature of [the complainant's] behaviour'[8]. The Department advised the ADF that the complainant submitted compensation claims with the Department and that in recent weeks, the complainant 'had become increasingly more abusive and aggressive towards staff'.[9] • The ADF advised the Department that the complainant did not have a psychiatric history.[10] • The PMA and the GMS had 'further conversations with an ADF medical officer' to understand the nature of the behaviour being exhibited by the complainant and to inform the Department's risk assessment of the situation.[11] • The Department was informed of the results of the security risk assessment undertaken which it said it 'came back as 'low''.[12] • The PMA and the GMS contacted a clinician[13] specialising in mental health issues in a military setting. The clinician was given a 'description' of the complainant's behaviour but was not provided copies of the emails sent by the complainant to the Department.[14] The clinician reportedly advised the Department that a psychiatric assessment of the complainant was warranted and should be undertaken as a priority.[15] • Following the advice of the clinician, the PMA and the GMS contacted the Head of Joint Health Command of the Department of Defence, about their concerns regarding the complainant's communications and sought support for medical intervention for the complainant.[16]

[5] File Note dated 22 October 2011 by Acting General Manager Support.
[6] This position is also referred to as the 'Acting General Manager Rehabilitation and Support' in the material provided by the Department.
[7] File Note dated 22 October 2011 by Acting General Manager Support.
[8] File Note dated 22 October 2011 by Acting General Manager Support.
[9] Submission by Department of 27 March 2012.
[10] File Note dated 22 October 2011 by Acting General Manager Support.
[11] File Note dated 22 October 2011 by Acting General Manager Support.
[12] File Note dated 22 October 2011 by Acting General Manager Support.
[13] No information has been provided about the relationship between the clinician and the Department.
[14] File Note dated 22 October 2011 by Acting General Manager Support.
[15] File Note dated 22 October 2011 by Acting General Manager Support.
[16] File Note dated 22 October 2011 by Acting General Manager Support.

Date	Event
21 October 2011	• The complainant's behaviour was raised with his Commanding Officer by an ADF Senior Medical Officer.[17] • The ADF advised the PMA that a General Practitioner appointment had been arranged for the complainant for 24 October 2011 and a psychiatric appointment for 25 October 2011.[18] • The Security Risk Assessment ('security assessment report') made by the Department Security Adviser dated 21 October 2011 stated that Security was instructed not to contact law enforcement or the Royal Australian Air Force (RAAF) in relation to the assessment.[19] The security assessment report recommended that all future contact be filtered through Security to monitor threat language and that the Department consider mediation and/or the appointment of a specialised single point of contact as soon as practically possible.[20] • The complainant became aware that the Department had notified ADF medical officers and the Department of Defence of his actions.[21] The complainant sent further emails, including an email to the personal email account of a Department staff member.[22] • The Department's Director of Security Personnel contacted the RAAF Security Police following a message received by a staff member on their personal email account. RAAF Security Police reportedly advised that as the DVA staff member was a civilian, they were unable to contact the complainant in relation to the matter and recommended that the DVA staff member contact civilian police directly. This was set out in a note of disclosure written by the Director, Security and Personnel recording reasons for disclosure to RAAF Security Police dated 21 October 2011.[23] • The Director Security Personnel advised the complainant by email that his level of contact with Departmental staff was unacceptable and that the staff member had been advised to contact the police to seek further advice in regards to their options.[24] • Following further email correspondence from the complainant, the Director Security and Personnel contacted the complainant by phone. The Director Security and Personnel reported phone call as 'productive' and one that 'ended on a good note'. The complainant reportedly denied he made threats of a physical nature against anyone or that he

[17] File Note dated 22 October 2011 by Acting General Manager Support.
[18] File Note dated 22 October 2011 by Acting General Manager Support.
[19] Security assessment report dated 21 October 2011 by Agency Security Adviser.
[20] Security assessment report dated 21 October 2011 by Agency Security Adviser.
[21] Email from complainant to Department's Director Security Personnel dated 21 October 2011.
[22] Email exchanges between Departmental staff on 21 October 2011 at 7:09 pm; Emails exchanges between complainant and Department's Director Security Personnel on 21 October 2011; Submission by Department of 27 March 2012.
[23] Note of Disclosure written by Director Security and Personnel summarising reasons for disclosure to RAAF Security Police; Email from Department's Director Security Personnel to Department staff on 21 October 2011 at 8:01 pm.
[24] Email from Department's Director Security Personnel to complainant on 21 October 2011 at 8:50 pm.

Date	Event
	'crossed the line'. The complainant reportedly became agitated that someone from the Department 'contacted the medics' and had taken the issue to his workplace. The complainant reportedly apologised for upsetting a DVA staff member and agreed to no further contact with DVA staff until issues were worked out. The complainant reportedly seemed amicable to the suggestion of a single point of contact through which he could raise his concerns or issues.[25]
22 October 2011	• Note of disclosure written by GMS summarising the reasons for disclosure to ADF medical staff and Department of Defence's Head of Joint Health Command.
28 October 2011	• In response to a request from the Minister for Veterans' Affairs, the Department wrote to the Chief of Air Force, and advised that the complainant had claims with the Department; that the complainant's correspondence with the Department had become more frequent and 'very personal, aggressive and highly offensive'; and that the complainant was the author of the website referred to in paragraph [4] of this decision.[26]
28 October 2011	• Note made by Department's Principal Legal Advisor indicating her agreement that disclosure of the complainant's personal information to an ADF Senior Medical Officer and to the Head of Joint Health Command in the Department of Defence was necessary and done in accordance with IPP 11.1(c).

Scope of complaint

7. On 21 November 2011, the complainant lodged a complaint under s 36 of the Privacy Act in relation to the Department's conduct.

8. The complainant says that the Department has breached IPP 11.1 in three ways:

   - disclosing his personal information to an ADF Senior Medical Officer on 20 October 2011 (claim 1);
   - disclosing his personal information to the Head of Joint Health Command in the Department of Defence on 20 October 2011 (claim 2); and
   - disclosing his personal information to the Chief of Air Force on 28 October 2011 (claim 3).

The law

9. The Information Privacy Principles (IPPs) in s 14 of the Privacy Act set out standards for handling personal information that are binding on an agency. Section 16 of the Privacy

[25] Email from Department's Director Security Personnel to Department staff on 21 October 2011 at 10:35 pm.
[26] Letter from Department's General Manager, Executive Division to Chief of Air Force dated 28 October 2011.

Act provides that an agency shall not do an act, or engage in a practice, that breaches an IPP.

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

> information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

11. IPP 11.1 prohibits the disclosure of personal information and sets out exceptions to the prohibition. It provides:

> **Information Privacy Principle 11.1**
>
> A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:
>
> (a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;
>
> (b) the individual concerned has consented to the disclosure;
>
> (c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;
>
> (d) the disclosure is required or authorised by or under law; or
>
> (e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.[27]

12. The Department is an agency for the purposes of the Privacy Act. As an agency, it is regarded as a 'record-keeper' in relation to a record if it has possession or control of a record that contains personal information.

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

- dismissing the complaint (s 52(1)(a)); or
- finding the complaint substantiated and declaring:
  - that the respondent has engaged in conduct constituting an interference with the privacy of an individual and should not repeat or continue such conduct (s 52(1)(b)(A)); and/or
  - the respondent should perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant (s 52(1)(b)(ii)); and/or
  - the complainant is entitled to compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint (s 52(1)(b)(iii)); and/or

[27] IPP 2 provides that an agency must take steps to tell individuals why they are collecting personal information, what laws give them authority to collect it, and to whom they usually disclose it. This is often done by what is called an 'IPP 2 notice'.

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

Investigation process

14. The OAIC's investigation of this complaint involved the following:

- On 25 January 2012, the Privacy Commissioner opened an investigation into the complainant's allegations under s 40(1) of the Privacy Act.
- The OAIC considered written submissions provided by both the complainant and the Department.
- On 18 July 2012, the OAIC provided the complainant and the Department with its preliminary view on the complaint which stated that the Department had met its obligations under IPP 2 and IPP 4, but had breached IPP 11.1.
- In response to the OAIC's preliminary view, both the complainant and the Department provided further submissions.
- In response to a request for further information by the OAIC, the Department also made further submissions.
- The parties were unable to reach a mutually agreeable outcome through conciliation and I decided to determine the matter under s 52 of the Privacy Act.

Claims 1 and 2: Disclosure of personal information to an ADF Senior Medical Officer and the Head of Joint Health Command in the Department of Defence on 20 October 2011

15. The complainant claims that in its correspondence to both an ADF Senior Medical Officer and the Head of Joint Health Command in Defence the Department improperly disclosed his personal information by:

- contacting his Senior Medical Officer to whom he claims, they stated 'I was displaying serious mental health issues';
- providing information about his compensation claims and his behaviour to his employer in response to his creation of a website in which he publicly criticised the Department;
- discussing the compensation claims he had lodged with the Department; and
- alleging that his communications with Departmental officers had become increasingly abusive and aggressive.

16. The Department seeks to rely on IPP 11.1(a), (c), (d) and (e) with respect to its disclosures to the ADF Senior Medical Officer and Defence's Head of Joint Health Command.

Information Privacy Principle (IPP) 11.1(a)

17. IPP 11.1(a) permits the disclosure of personal information where 'the individual concerned is reasonably likely to have been aware ... that information of that kind is usually passed to that person, body or agency'.

18. Guideline 19 of the OAIC's advisory *Plain English Guidelines to Information Privacy Principles 8-11* (**Plain English Guidelines)** explains that, in relation to IPP 11.1(a), 'the disclosing agency must be able to explain why it thought the person was reasonably likely to have been aware [and]…should take into account the relationship that the person the information is about has with the agency'.[28]

19. The Privacy Act does not define the meaning of the expression 'reasonably likely to have been aware'. I have had regard to Deputy President Forgie's consideration of the expression 'reasonably likely' in the context of IPP 11.1(a) in *Skase and Minister for Immigration and Multicultural and Indigenous Affairs*[29]:

> When used as an adverb, the ordinary meaning of "likely" is "probably". When used in conjunction with the word "reasonably" a judgment is required as to whether it is reasonable, as distinct from something that is irrational, absurd or ridiculous, to expect that Mrs Skase would probably have been aware that the information on her file would be passed to HWT [Herald & Weekly Times Pty Ltd]...

Submissions and considerations

20. In its initial correspondence with the OAIC, the Department submitted that its decision to disclose the complainant's personal information was based on its view that disclosure was necessary to lessen or prevent a serious and imminent threat (as discussed below). It was only more recently, in its submission of 29 July 2014, that the Department advised that it was now relying on IPP 11.1(a) in disclosing the complainant's claims for compensation to the Department of Defence. The Department says:

> (the complainant's) status as a DVA client was provided to the Department of Defence to give context to (the complainant's) [sic] communications with the DVA. This level of disclosure was reasonable in circumstances and in accordance with IPP 11.1(a).

21. However, in making this claim, the Department has not provided any explanation or information demonstrating how the complainant was aware, or was reasonably likely to have been aware, that information of that kind was usually passed to the ADF or the Department of Defence.

22. Therefore, there is insufficient information before me to conclude that the disclosures to the ADF and Department of Defence medical officers were justified under IPP 11.1(a).

Information Privacy Principle (IPP) 11.1(c)

23. For an agency to rely on the exception at IPP 11.1(c), it must believe on reasonable grounds that the disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's health or life.

---

[28] *Plain English Guidelines to Information Privacy Principles 8-11*, Guideline 19. These guidelines have been superseded by the APP Guidelines which apply from 12 March 2014.

[29] [2005] AATA 200, [64].

24. The Plain English Guidelines state that the exception in IPP 11.1(c) should only be used by an agency:

> …in an emergency…An agency should not use these exceptions to justify any class of routine uses or disclosures, even if those uses or disclosures are aimed at reducing serious threats to life or health.[30]

25. The term 'reasonable grounds' is not defined in the Privacy Act. The term should therefore be given its ordinary meaning. The Plain English Guidelines note that 'reasonable grounds' for believing that something is the case does not mean that something must actually be the case'[31]. It is sufficient that the disclosure was honestly made and made in the reasonable belief that it is likely to relieve a serious and imminent threat to an individual's life or health.[32]

26. The word 'necessary' is also not defined in the Privacy Act. The Macquarie Dictionary, 3rd edition, relevantly defines necessary as 'indispensable' or 'requisite'.[33] The Plain English Guidelines note that an agency must reasonably believe that it is necessary to take this action, that is to use or disclose an individual's personal information, to prevent the threat or lessen the threat to a noticeable extent.[34] Using or disclosing personal information, even to prevent or lessen a serious threat to health or life, may significantly disadvantage the person the information is about. If this is the case, an agency should seriously consider if there are any effective alternatives available that do not have this consequence.[35]

27. Nor is the phrase 'serious and imminent' defined in the Privacy Act. In attempting to define the term, I have relied on the ordinary meaning of the words 'serious' and 'imminent'. The Macquarie Dictionary relevantly defines 'serious' as 'grave' or 'being in earnest; not trifling'.[36] It defines 'imminent' as 'impending' or 'likely to occur at any moment'.[37]

28. Though not binding or exhaustive, the Plain English Guidelines explain that whether a threat is 'serious' is to be determined on the particular circumstances of each matter. Examples may include, relevantly here:

- an explicit threat of … assault
- a specific threat of physical harm to a particular officer in an agency (although abuse directed to staff in general does not usually count as a serious threat).[38]

29. In relation to whether a threat is imminent, the Plain English Guidelines explain that this means 'the threatened harm must be about to happen'.[39]

---

[30] *Plain English Guidelines to Information Privacy Principles 8-11*, Guideline 25.
[31] *Plain English Guidelines to Information Privacy Principles 8-11*, Guideline 26.
[32] *Plain English Guidelines to Information Privacy Principles 8-11*, Guideline 26.
[33] *The Macquarie Diction*ary (1997), 3rd ed, Macmillan Publishers Australia.
[34] *Plain English Guidelines to Information Privacy Principles 8-11*, Guideline 27.
[35] *Plain English Guidelines to Information Privacy Principles 8-11*, Guideline 27.
[36] *The Macquarie Diction*ary (1997), 3rd ed, Macmillan Publishers Australia.
[37] *The Macquarie Dictionary* (1997), 3rd ed, Macmillan Publishers Australia.
[38] *Plain English Guidelines to Information Privacy Principles 8-11*, Guideline 28.
[39] *Plain English Guidelines to Information Privacy Principles 8-11*, Guideline 28.

Submissions

30. In submissions to the OAIC, the complainant said that the Department could not rely on the exception in IPP 11.1(c) because it had not demonstrated that it had a reasonable belief that the complainant had made serious and imminent threats to the life or health of himself or Departmental staff.

31. The complainant accepted that his language was at times 'rude and obnoxious', but submitted that the language was a result of what he considered to be poor administration on the part of the Department in handling his matters. The complainant also submitted that the Department's own security risk assessment showed that he presented as a 'low' risk of danger.

32. In submissions to the OAIC, the Department acknowledged that its communications with ADF medical staff and the Department of Defence disclosed the complainant's personal information. However, the Department submitted that it relied on the exception in IPP 11.1(c) on the basis that the volume of the complainant's communications were escalating, the contents had become increasingly aggressive, abuse and offensive, and the Department had serious concerns for the health and safety of the complainant and Departmental staff.

33. In particular, the Department said that the complainant had contacted staff on their mobile phones and outside of normal business channels, including sending an email to a staff member's personal email address. I note the email to a staff member's personal email address was sent on 21 October 2011, after the initial disclosure to ADF and so could not have been a consideration in the initial disclosure on 20 October 2011.

34. The Department provided the OAIC with extracts of some of the emails from the complainant to Departmental officers. The Department said that the nature of the complainant's correspondence, both in emails to Departmental officers and on the complainant's website, had a significant impact on the mental health of its staff. The Department was of the view that the escalation in the complainant's communications presented an imminent threat to the health and wellbeing of its staff and that immediate action was required.

35. The Department submitted that standard practice in this type of situation was to contact the police. However, in this matter, the Department considered it preferable to contact the ADF as the complainant's employer, because of its duty of care to the complainant and its belief that the ADF was best placed to assist him.

36. The Department also submitted that it had a duty under the *Work Health and Safety Act 2011* (WHS Act) to ensure, as far as is reasonably practicable, the health and safety of workers. The Department submitted that its disclosure of the complainant's personal information was at a minimum authorised, if not required, by the WHS Act. This is not relevant to the application of IPP 11.1(c) and I have considered this submission in paragraphs [59] to [62] in relation to the application of IPP 11.1(d).

Considerations

37. In determining whether the Department's disclosures were permitted under IPP 11.1(c), I have considered whether the content of the complainant's

correspondence constituted a threat to his own life or health or that of Departmental officers; whether any such threats were serious and imminent; and whether the Department had reasonable grounds to believe that the disclosure of the complainant's personal information to the Department of Defence was necessary to prevent or lessen any threat.

38. I have reviewed the emails the complainant sent to the Department that the Department relies on in its claim that the disclosures were necessary because of a serious and imminent threat. The Department has highlighted a number of excerpts from these emails including:

> My clock is now definitely ticking, it's time to get on with it or I will run you down and hound you until you get off your fat arse and do what – by law you are obliged to do (Excerpt from an email dated 12 October 2011)
>
> A prompt response will avoid hand grenades (Excerpt from an email dated 19 October 2011)
>
> 'So more hot air? Hmm, no I've had enough of that from you and Co, I think I'll try blowtorch – since you clearly aren't getting the bleedingly obvious point (clean up your Department's act!) (Excerpt from an email dated 19 October 2011)
>
> 'Dear Lying bastards……you nothing but a lying sack of sh*t. …… You pr*cks have f***** me over every which way…… You better bring on your A game dipsh*ts, because I think you'll find it my turn to f*** you up!(Excerpts from an email dated 19 October 2011)

39. I have also considered the note of disclosure made by the GMS on 22 October 2011, which relevantly states:

> ..given the advice received, the continuing volume and nature of the emails received and the inability to contact [the complainant] directly, the PMA [Principal Medical Adviser] decided that in the continuing interests of [the complainant's] health to advise … Commander Joint Health of our concerns and seek his support for medical intervention. This telephone contact occurred on 20 October pm.

40. In my consideration of claims 1 and 2, I have not taken into account the complainant's contact with a staff member via her personal email account. As I noted above, this contact was made on 21 October 2011, after the alleged improper disclosures to the ADF Senior Medical Officer and Defence's Head of Joint Health Command and following the complainant's realisation that his personal information had been disclosed to his employer. In considering the circumstances in which it may have been reasonable for an agency to form the belief that there was a serious and imminent threat to the health or life of the complainant or another person, I must look at the circumstances at the time of disclosure, not at later circumstances that might have arisen.

41. The security assessment report is dated 21 October 2011, which is also subsequent to the alleged improper disclosures in claims 1 and 2. I note, however, that the file note made by the Department's GMS indicates that the Department's Security area's risk assessment of the situation came back as 'low' and that this assessment was communicated to the Department's GMS prior to the Department's consultation with

a clinician and prior to contact with the Head of Joint Health Command on 20 October 2011. I have consequently taken this security assessment report into consideration in relation to claim 2 in deciding whether or not the belief reportedly formed by the Department was a reasonable one.

Whether the complainant's threats were 'serious' and 'imminent'

42. The file note written by the Department's GMS on 22 October 2011 indicates concern with the complainant's own health and the general well-being of Departmental staff. The receipt of the emails sent by the complainant would, I believe, have been disturbing and confronting for Departmental staff who, as with any employee, should not be subjected to communications of this nature.

43. I am of the view that the email communications sent by the complainant to the Department during September and October 2011 contain language that could be considered abrasive, inappropriate and offensive. However, on reading the material provided, which includes complete emails and extracts such as those above at [38], I am not satisfied that the emails imply threats of serious and imminent violence.

44. There is no information to suggest that the concerns of the Department, however well meaning, do amount or could amount to a perception of a serious and imminent threat to the health or safety of the complainant or another person. I note that the Department's own security assessment of the complainant's behaviour states 'that no direct threat of harm has been provided' in the relevant communications with Departmental staff.

45. I note that a psychiatric assessment was recommended by the specialist clinician contacted by the Department in relation to the complainant's behaviour. The clinician, having been provided with a 'description' of the complainant's behaviour and not copies of the emails, reportedly confirmed the Department's view that the complainant's escalating behaviour raised safety concerns with respect to the complainant's own health and that of Departmental staff. The clinician reportedly recommended that the complainant undertake a psychiatric assessment. There is, however, no record of any concerns on the clinician's part that there was a serious and imminent threat to identified persons or to the complainant himself and that the complainant was likely to act on those threats. In my view, if there were reasonable grounds to believe there was a serious and imminent threat, this would have been recorded extensively by the Department's PMA and in discussion with the clinician, and more immediate action would have been taken. There is no indication that potential victims were informed of any impending threat or that police were notified at that time.

46. It is also particularly important to note the disclosure to the ADF medical officer (claim 1) was made prior to consultation with the specialist clinician. Therefore, the clinician's specialist opinion in relation to the safety of the complainant or other persons is not relevant to my consideration of the circumstances at the time of the alleged improper disclosure to the ADF Senior Medical Officer.

47. If I were to accept that the concerns were serious, the timing of the Department's actions does not suggest the Department considered the threats to be imminent. The Department pointed to an escalation in the volume and tone of the complainant's

emails from September to October 2011, but there is no information before me that on or prior to 20 October 2011 (the date of the alleged improper disclosures) the Department advised the complainant of its concerns regarding the tone and nature of his communications, foreshadowed action it would take if the tone and nature of the complainant's communication did not change, or took action in response to the alleged threats. This suggests to me that it was not an immediate concern for the Department because when the complainant subsequently contacted a staff member via their personal email address, the Department did contact the complainant directly to discuss their concerns about his behaviour.

48. There is, as far as I am aware in the information that has been provided, insufficient documentation to indicate there was an impending threat and the situation was serious and imminent.

49. Based on the information before me, the complainant's actions do not meet the meaning of 'serious and imminent' as contemplated by the Privacy Act.

Whether the disclosure was 'necessary'

50. If I were to accept that the complainant's communications could be characterised as a serious and imminent threat to either the life or health of himself or that of another person, I am nevertheless not satisfied that the disclosure of that conduct to the Department of Defence was necessary to protect him or any other person from that threat. It is particularly unclear how the Department could have considered it was necessary to disclose the complainant's personal information to his employer in order to prevent or lessen the serious and imminent threat to the life or health of a DVA staff member, when the security assessment report recommended the Department consider mediation and/or the appointment of a specialised single point of contact as soon as practically possible.

51. If the Department considered the threat to be serious and imminent, then disclosure to the police, in accordance with reported standard Departmental practice, would seem the appropriate course of action to address the situation. It is also unclear why when making such a disclosure it would be relevant to disclose details of the complainant's compensation claims. I am not persuaded on the information before me, that any threat that may have existed at that time mandated disclosure to ADF medical staff or Defence's Head of Joint Health Command in order to prevent or lessen it.

'Reasonable grounds'

52. The exception at IPP 11.1(c) provides an objective test where a belief that disclosure is necessary to prevent or lessen a serious and imminent threat is held on reasonable grounds.

53. The Department appears to have relied on an escalation of email communications from the complainant as the basis for making contact with ADF medical staff on 20 October 2011. It has then relied on those communications as well as a clinician's recommendation that the complainant undertake psychiatric assessment as the basis for the subsequent disclosure to Defence's Head of Joint Health Command. It has submitted that it had reasonable grounds to believe that the disclosures were necessary to prevent or lessen risk to the life or health of the complainant and/or that

of Departmental staff. A file note of 22 October 2011 describing the contact with the ADF on 20 October 2011 states the Department did so 'to understand better the nature' of the applicant's behaviour. It has not provided any information to indicate how it thought that the disclosure of the complainant's information to the ADF and the Department of Defence could prevent or lessen a threat to life or health.

54. While the Department may have had a genuine concern for the complainant's life or health or that of its staff, as outlined above, I am satisfied that the complainant's conduct did not constitute a serious and imminent threat. In my view, on the totality of the information before me, any belief that the Department may have held that the complainant's conduct posed a serious and imminent threat was not reasonable.

55. The circumstances presented here do not meet the threshold required for IPP 11.1(c) to be applicable and the Department was therefore not entitled to rely on it.

Information Privacy Principle (IPP) 11.1(d)

56. IPP 11.1(d) permits the disclosure of information where the disclosure is required or authorised by law.

57. Guideline 33 of the Plain English Guidelines explains:

> There is a difference between "required by law" and "authorised by law". If an agency is required by law to use or disclose personal information, it has no choice in the matter. If an agency is authorised by law to use or disclose personal information, it has a discretion as to whether it will do so.

58. The Guidelines also provide that:

> Before an agency relies on these exceptions to use or disclose personal information, it should identify exactly what law requires or authorises that use or disclosure.[40]

Submissions and considerations

59. The Department submitted that its disclosure of the complainant's personal information was at a minimum authorised, if not required, by the *Work Health and Safety Act 2011* (WHS Act).[41] The Department said it had a duty under the WHS Act to ensure, as far as is reasonably practicable, the health and safety of workers. It did not explicitly identify a legislative provision which authorised the disclosure but submitted that its general duty of care amounted to a lawful authority to disclose.

60. The WHS Act did not commence until 1 January 2012 and was therefore not in effect at the time of the Department's disclosure. As the WHS Act does not operate retrospectively, it cannot be relied on by the Department.

61. The *Occupational Health and Safety Act 1991* was in place at the time of the Department's disclosure. I am not satisfied that any obligations the Department may have under that legislation may be relied on to permit the disclosure under IPP 11.1(d). Even if a duty of care existed as asserted by the Department and that duty of care could have been categorised as a law for the purposes of IPP 11.1(d), it is not clear that authorisation to disclose would permit disclosure to the complainant's

[40] *Plain English Guidelines to Information Privacy Principles 8-11*, Guideline 35.
[41] Submission of Department of 8 August 2012.

employer under the exception in IPP 11.1 (d) of the Privacy Act. No specific legislative reference to the range of persons personal information may be disclosed to in the discharge of such a duty of care has been identified. Nor it seems was this disclosure in keeping with standard practice (the Department's standard practice would normally involve disclosure to the police). In my view, the Department's actions were not consistent with the notion that it was discharging a perceived duty of care.

62. Accordingly, on the information available to me, I am satisfied that the Department cannot rely on the exemption contained in IPP 11.1(d).

Information Privacy Principle (IPP) 11.1(e)

63. IPP 11.1(e) permits disclosure of personal information where 'the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue'.

64. Guideline 37 of the Plain English Guidelines explains that an agency may want to apply this exemption provision to three types of use or disclosure, including relevantly here, disclosures for specific investigations. Such a disclosure may involve:

> an agency ….. disclosing personal information about a particular person, reasonably believing it will safeguard one of the public purposes listed in the exceptions in a predicable way.
>
> For example: if a person is suspected of a crime, an agency may disclose information about that person to an investigating body.[42]

Submissions and consideration

65. The Department submitted on 28 March 2012 that the disclosures were reasonably necessary for the enforcement of the *Defence Force Disciplinary Act 1982* (DFDA) and referred in particular to sections 33 and 60, which deal with 'assault, insulting or provocative words' and prejudicial conduct respectively.

66. If I were to accept that the term 'enforcement of criminal law' or 'enforcement of a law involving pecuniary penalty' in IPP 11.1(e) includes disciplinary action taken by the Department of Defence under the *Defence Force Discipline Act 1982* (DFDA), I am not aware of any type of arrangement between the Department and Defence, that existed at the time of the alleged improper disclosures, to the effect that these agencies shared information relevant to Defence's law enforcement functions under the DFDA. Nor has any information been presented to me to indicate that the complainant was the subject of an investigation of a service offence at the time of the disclosures.

67. I am not satisfied that disclosure of the complainant's information to ADF medical officers could reasonably be expected to be necessary for the enforcement of any disciplinary action under the DFDA. The Head of Joint Health Command is, amongst other things, responsible for the provision of health care to members of the ADF. The ADF Senior Medical Officer also has a role in the provision of health care to ADF personnel. Even if there was an intention to disclose for the purpose of law enforcement, I am not satisfied that it was reasonably necessary to disclose that personal information to ADF and Department of Defence medical staff.

[42] *Plain English Guidelines to Information Privacy Principles 8-11*, Guideline 37.

68. I also have had regard to IPP 11.2 of the Privacy Act which provides that:

> where personal information is disclosed, for the purposes of the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.

69. I have considered the file note written by the GMS, which indicates concern about the complainant's conduct. This record indicates that disclosures were precipitated by concerns over the complainant's escalating communications towards Departmental staff. There is no information before me to suggest that the Department's disclosures to an ADF Senior Medical Officer and to Defence's Head of Joint Health Command were undertaken for the purpose of law enforcement.

70. Accordingly, I am satisfied that the exception contained in IPP 11.1(e) was not available to the Department in relation to its disclosures to an ADF Senior Medical Officer and the Head of Joint Health Command.

Findings

71. The Department was not entitled to rely on the exceptions in IPP 11.1 (a), (c), (d) or (e) in disclosing the complainant's personal information to an ADF Senior Medical Officer on 20 October 2011 (claim 1).

72. The Department was not entitled to rely on the exceptions in IPP 11.1 (a), (c), (d) or (e) in disclosing the complainant's personal information to the Department of Defence's Head of Joint Health Command on 20 October 2011 (claim 2).

73. The Department breached IPP 11.1 with respect to claims 1 and 2.

Claim 3: Disclosure of personal information to Chief of Air Force on 28 October 2011

74. The complainant says that the Department also disclosed his personal information in its correspondence to the Chief of Air Force on 28 October 2011.

75. The Department acknowledged that it had disclosed the complainant's personal information in this correspondence, but relied on the exceptions in IPP 11.1(a), (c) and (e).

Information Privacy Principle (IPP) 11.1(a)

Submissions

76. The Department advised that following a request from the then Minister for Veterans' Affairs, the Hon Warren Snowdon MP, the Department contacted the Chief of Air Force on 28 October 2011 about the complainant's behaviour. The Minister's request to the Department followed email correspondence received by him from the complainant on 20 October 2011. The Department submitted that the content of the complainant's correspondence to the Minister was offensive and critical of the Minister and raised disciplinary issues under the DFDA, as well as concerns for the health or safety of the complainant and/or Departmental staff.

77. In submissions to the OAIC, the Department said that, as a serving member of the ADF, the complainant would have been aware that information about his communication with the Minister would have been reported to his employer as it constituted a potential offence under the DFDA. For this reason, the Department relied on the exception in IPP 11.1(a).

78. In submissions to the OAIC, the complainant stated that he was familiar with military law, but disagreed with the Department that his actions were in breach of the DFDA.

Consideration

79. I have reviewed the 28 October 2011 correspondence from the Department to the Chief of Air Force. The correspondence details the complainant's then recent communications with Departmental staff and discloses the fact that the complainant had developed a website, which was extremely critical of the Department.

80. I have also had regard to an excerpt of the email sent by the complainant to the Minister on 20 October 2011. I am of the view that the email communication sent by the complainant to the Minister contains language that could be considered aggressive, inappropriate and offensive.

81. I do not have any documentation before me, other than the Department's claim, to support the existence of a request by the then Minister's Office made to the Department to contact the Air Force Chief. In the absence of documentation, I will accept that that there was a request by the then Minister's Office to the Department to contact the Air Force Chief. In circumstances whereby such communications were made to a Minister, this would not be unusual and would be considered standard governmental practice.

82. I accept the Department's submissions that, as a serving member of the ADF, the complainant would have been reasonably likely to be aware of the DFDA and of those acts or omissions that may constitute offences under the DFDA. The complainant's own submissions support this notion.

83. I am satisfied that, a reasonable person in the complainant's position – that is someone with familiarity with military law and with what is expected of defence personnel in terms of behaviour – would be reasonably likely to have been aware that any email communication they sent to the Minister of Veteran Affairs that was offensive and critical of the Minister may be brought to the attention of the Department of Defence.

84. However, the letter to the Chief of Air Force dated 28 October 2011 discloses more than the complainant's email communication to the Minister. It also details the specific nature of the complainant's relationship with the Department and his recent conduct towards Departmental staff. The letter states that the complainant 'has engaged in frequent correspondence with numerous officers across the department. The level of this correspondence is increasing in frequency and the tone has become very personal, aggressive and highly offensive'. It also notes that the complainant has authored a website critical of the Department and the Minister and that a number of staff now fear of their safety and wellbeing, both mental and physical. The letter goes on to say that the Department has in the circumstances decided the best course of

action is 'to continue to process [the complainant's] claims and to assign a single point of contact to deal with all his issues and correspondence'.

85. I note that the letter is dated 28 October 2011, a week after the complainant was contacted directly by the Director Security and Personnel. I also note that the letter did not go on to explain that as a result of that conversation between the Director Security and Personnel and the complainant that the complainant had agreed to cease his escalated behaviour, apologised for upsetting staff, and had seemingly agreed to the concept of a single point of contact and to cease further contact until a way forward had been negotiated. The letter to the Chief of Air Force does not acknowledge this communication with the complainant, or that his behaviour had apparently moderated following that contact.

86. Further, the letter did not state that a security assessment had been undertaken assessing the complainant's risk as 'low' and that it was the security assessment report that had recommended a single point of contact for the complainant in his dealings with the Department. The letter states that staff 'now fear for their safety and wellbeing' but does not indicate that the complainant's communications that had caused those concerns had ceased. The author of the letter offers to meet with the Chief of Air Force to discuss the matter. It is unclear on the information before me whether that meeting took place.

87. I have considered whether a reasonable person with a history similar to that of the complainant would have been 'reasonably likely to be aware' that certain personal information of this kind would usually be passed to Defence. It is not clear to me that a person, albeit a military officer, would be aware that, without there being some type of authorisation or investigation on foot, information of this additional detail, would be passed onto his employer. It is clear from his email communications that the complainant was upset to discover that his personal information concerning his relationship with the Department had been disclosed to Defence.

88. As I noted above, I have not been made aware of any type of arrangement whereby if an agency such as the Department receives information concerning the behaviour or conduct of a military officer, then that agency shares the information with the Department of Defence. Even if such an arrangement did exist, any such agreement would still need to comply with the Privacy Act. Arguably, if this were not the case, the Department would be able to exchange any personal information about Defence personnel with the Department of Defence it chose to. I have no information which suggests that there was a general understanding or expectation amongst military personnel that personal information could or would generally be disclosed to Defence if issues arose in the context of the Department's dealings with compensation claims lodged by Defence personnel.

89. Given the passage of time, albeit only a week since events had escalated and apparently subsided, it is unclear why the complainant's personal information was disclosed in this way and to this extent.

90. It is clearly appropriate for a Minister to raise concerns about what could reasonably be seen as offensive communications with them, through their Department. Further, it is also appropriate for that Minister's Department to then raise these concerns with another relevant Department. However, when this is done, care needs to be taken to

ensure that only that information which is directly relevant to those specific concerns is disclosed, or where it is believed that other information is required that it is a complete and accurate record of events.

91. In situations such as this, raising concerns about a person's behaviour which goes to questioning their psychological state with their employer can have significant ramifications. This, in my view, places a greater need on ensuring disclosure is necessary and where such a need for disclosure is identified the full context of the situation is disclosed.

92. I am therefore of the view that the Department was not entitled to rely on the exception at IPP 11.1(a) in disclosing the complainant's personal information to the Chief of Air Force to the extent it was disclosed on 28 October 2011.

Information Privacy Principle (IPP) 11.1(c)

Submissions and considerations

93. In relation to IPP 11.1(c), the Department relied on the reasons outlined above for claims 1 and 2 in paragraphs [30] to [36] of this determination.

94. I note that in the 24-hour period following the Department's disclosures to the ADF Senior Medical Officer and Defence's Head Joint Health Command on 20 October 2011, the complainant further escalated his email communications with Departmental staff, including contacting a Department staff member via her personal email account on 21 October 2011. Email records suggest that these further communications by the complainant (which were undertaken following the complainant's realisation that his personal information had been disclosed to his employer) raised further concern by the Department about the complainant's conduct towards its staff. It was following the communication to a staff member via her personal email account that the Director Security and Personnel contacted the RAAF Security Police, who advised that they were unable to deal with the matter and recommended the targeted staff member contact civilian police directly.

95. If I were to accept that these additional actions by the complainant, together with the preceding communications to the Department, constituted a more serious threat than previously existed, there is still nothing to indicate that the threat was sufficiently serious and imminent to meet the threshold of IPP 11.1(c). In reaching this conclusion, I have taken into consideration the email of 21 October 2011 (at 10.35 pm) from the Director Security and Personnel to relevant Departmental staff outlining the details of a phone call to the complainant following his further email communications to staff. The email notes that during the phone call the complainant indicated the language used in his emails was a reflection of his sense of humour. The complainant reportedly denied that he had made direct threats to any individuals, apologised that he caused distress to a certain staff member and agreed not to make further contact with Departmental staff while his concerns were being addressed.

96. This account is not consistent with notion that the complainant's behaviour was sufficiently threatening to create a reasonable belief that there was a serious and imminent threat to the life or health of either the complainant himself or some other person. I also note again that the disclosure to the Chief of Air Force was made some

six days after these communications. Further, I have no information before me to suggest that aggressive email communication with Departmental staff continued subsequent to the Director Security and Personnel's phone contact with the complainant on 21 October 2011.

97. I am therefore of the view that the Department cannot rely on the 11.1(c) exemption in relation to claim 3.

Information Privacy Principle (IPP) 11.1(e)

Submissions and considerations

98. The arguments raised in relation to the Department's reliance on 11.1(e) reflect those made in respect of claims 1 and 2. For the same reasons I have provided in relation to claims 1 and 2, I am also of the view that the Department cannot rely on the 11.1(e) exception in relation to claim 3.

Findings

99. The Department was not entitled to rely on the exceptions in IPP 11.1(c) and (e) in disclosing the complainant's personal information to the Chief of Air Force on 28 October 2011 (claim 3).

100. The Department was entitled to rely on the exception in 11.1(a) to the extent that the letter to the Chief of Air Force dated 28 October 2011 addressed the complainant's correspondence to the Minister. However, the Department was not entitled to rely on the exception in IPP 11.1(a) in disclosing the complainant's personal information, to the extent it was disclosed to the Chief of Air Force on 28 October 2011.

101. On this basis, the Department breached IPP 11.1 in relation to claim 3.

Damages

102. Under s 52(1)(b)(iii) of the Privacy Act, I may find the complaint substantiated and make a determination that includes a declaration that the complainant is entitled to a payment of compensation for 'any loss or damage suffered by reason of' the interference with privacy. Under section 52(1A), loss or damage can include 'injury to the complainant's feelings or humiliation suffered by the complainant'.

103. As the complainant is seeking an apology as an outcome to the determination process, I have not considered whether compensation would be warranted in this matter.

The Department's participation in the OAIC's complaint handling process of this complaint

104. These events occurred in October 2011. The complaint was received on 20 November 2011, a few weeks after the events and now nearly three years ago. The Department was formally notified of the complaint by me on 25 January 2012.

105. I am concerned that this matter was unable to be resolved by conciliation and has been finalised by a formal determination under s 52 of the Privacy Act.

106. Given the modest outcome that the complainant was seeking, and the efforts by the OAIC to resolve the matter informally, it is unfortunate that this matter was not able to be finalised informally in the intervening period.

Determination

107. I declare in accordance with s 52(1)(b)(i)(B) of the Privacy Act that the complainant's complaint is substantiated and that the Department breached IPP 11.1 by disclosing the personal information of the complainant.

108. I declare in accordance with s 52(1)(b)(ii) of the Privacy Act that:

- The Department shall apologise in writing to the complainant within two weeks of this determination; and
- The Secretary will initiate a review of the management of privacy complaints within the Department and advise me of the results of the review no later than two months from the date of this determination. In undertaking this review, particular consideration should be given to the steps undertaken by the Department in handling this matter.

Timothy Pilgrim
Privacy Commissioner

13 November 2014

Review rights

If a party to a privacy determination is unsatisfied with the privacy determination, they may apply under s 5 of the *Administrative Decisions (Judicial Review) Act 1977* to have the determination reviewed by the Federal Court of Australia or the Federal Circuit Court. The Court will not review the merits of the determination, but 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.

Determinations involving Australian Government agencies – compensation

If a party to a privacy determination about a complaint involving an Australian or ACT government agency disagrees with the amount of compensation set by the Information Commissioner, they may apply under s 61 of the *Privacy Act 1988* to the Administrative Appeals Tribunal (AAT) to review the declaration about compensation. The AAT provides independent merits review of administrative decisions and has power to set aside, vary, or affirm the Information Commissioner's declaration about compensation.

An application to the AAT must be made within 28 days of the day on which the applicant 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. The current application fee is $861, which may be reduced or may not apply in certain circumstances. Further information is available on the AAT's website (www.aat.gov.au) or by telephoning 1300 366 700.

Enforcement of determination

Under s 58 of the *Privacy Act 1988*, a respondent agency to a privacy determination is obliged to comply with any declarations made by the Information Commissioner in that determination.

Section 62 of the *Privacy Act 1988* provides that either the complainant or Information Commissioner may commence proceedings in the Federal Court or the Federal Circuit Court for an order to enforce the determination.