Australian Government

Office of the Australian Information Commissioner

Privacy regulatory action policy

Updated December 2022

OAIC

Contents

Overview of approach and guidance

1. The *Privacy Act 1988* (Privacy Act) confers on the Commissioner a range of privacy regulatory powers. These include powers that allow the Office of the Australian Information Commissioner (OAIC) to work with entities to facilitate legal compliance and best privacy practice, as well as investigative and enforcement powers to use in cases where a privacy breach has occurred.

2. The *Privacy regulatory action policy* explains the OAIC's approach to using its privacy regulatory powers and communicating information publicly. The policy relates to the OAIC's regulatory powers rather than its full range of regulatory functions. In particular, the purpose of this policy is to allow entities and the community to understand the OAIC's range of powers, and its regulatory strategy, approach and priorities.

3. The OAIC's preferred regulatory approach is to facilitate voluntary compliance with privacy obligations and to work with entities to ensure best privacy practice and prevent privacy breaches. When resolving matters brought to its attention, the OAIC will take into account the steps taken by an entity to comply with its privacy obligations, in addition to considering the factors outlined in this policy.

4. This policy also outlines the manner in which privacy regulatory activity is undertaken and the circumstances in which information about regulatory activity may be communicated publicly.

Guide to privacy regulatory action

5. A more detailed explanation of each privacy regulatory power is given in the *Guide to privacy regulatory action*. The guide will be a useful resource for stakeholders, as well as providing practical guidance for staff exercising privacy regulatory powers. The guide is available on the OAIC's website.[1]

The OAIC and its jurisdiction

6. The OAIC has a range of functions and powers directed towards protecting the privacy of individuals by ensuring the proper handling of personal information. These functions and powers are conferred by the Privacy Act and by other legislation containing privacy protection provisions.

7. This policy relates to the use of regulatory powers conferred on the Commissioner by the Privacy Act and other legislation. These include powers that allow the OAIC to engage and work with regulated entities to facilitate compliance and best privacy practice, as well as investigation and enforcement powers to redress privacy breaches. Most of the Commissioner's powers can be delegated to and exercised by staff of the OAIC.

8. Entities that are regulated by the Privacy Act are required to comply with relevant provisions in that Act and in legislative instruments made under that Act. This obligation applies to: agencies and organisations that must comply with the Australian Privacy Principles (APPs) in Schedule 1 or a registered APP code; credit reporting participants that must comply with Part IIIA (relating to credit reporting) and the registered CR Code; and tax file number recipients that must

[1] See Guide to Privacy Regulatory Action.

comply with Tax File Number Guidelines 2011 issued under s 17. A breach of any of these provisions is an 'interference with privacy'. An 'interference with privacy' can also arise from breaches of particular provisions in other legislation.[2] The OAIC can investigate an alleged interference with privacy (and certain other privacy breaches),[3] either following a complaint[4] or on the Commissioner's own initiative (Commissioner initiated investigation (CII)). A complaint or CII may result in enforcement action being taken.

9. The Commissioner also has privacy regulatory responsibilities in relation to the My Health Record system. The information in this policy is also relevant to the OAIC's regulatory action in connection with the My Health Record system. However, the *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016*[5] prevail over the terms of this policy in the event of any inconsistency between those two documents.

The goals of taking privacy regulatory action

10. The goal of the OAIC in taking privacy regulatory action is to promote and ensure the protection of personal information, consistent with the objects of the Privacy Act.

11. Regulatory action may also aid the OAIC's role as privacy regulator by:

- ensuring compliance by entities with personal information handling obligations
- increasing public knowledge of personal information handling rights and obligations and the Commissioner's privacy regulatory powers
- assisting and influencing entities to adopt best practice personal information handling practices
- deterring conduct that contravenes privacy obligations (both specifically and generally)
- securing an appropriate remedy for an aggrieved person where a privacy contravention has occurred
- addressing systemic issues (see paragraphs 12-13) in personal information handling
- instilling public confidence in the OAIC's role of ensuring the protection of personal information.

Systemic privacy issues

12. A systemic privacy issue is a privacy issue that may have implications or an effect beyond a particular incident. This may occur where an incident indicates there is an ongoing or underlying problem with practices, procedures or systems that relate to privacy compliance, adherence to those practices, procedures or systems, or with attitudes to privacy compliance.

---

[2] For example, the *Data-matching Program (Assistance and Tax) Act 1990*, the 135AA guidelines issued under the *National Health Act 1953*, the *Healthcare Identifiers Act 2010*, the *My Health Records Act 2012*, the *National Cancer Screening Register Act 2016*, the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, and the *Personal Property Securities Act 2009*. Further information on the OAIC's role in investigating breaches of privacy provisions contained in other legislation is available at Other Legislation.

[3] The OAIC can also investigate breaches of the Spent Convictions scheme set out in the *Crimes Act 1914* (Cth).

[4] The OAIC can accept a complaint from an individual, or from an individual on behalf of a group of individuals (known as a 'representative complaint').

[5] See Federal Register of Legislation.

13. A privacy issue may be systemic within a single entity, or more broadly within an industry sector. A systemic privacy issue may be identified from an incident which is brought to the OAIC's attention by a single complaint, multiple complaints of a similar nature, or through other avenues such as a data breach notification to the OAIC or a report from an informant or a recognised external dispute resolution (EDR) scheme.

Regulatory action principles

14. The OAIC will be guided by the following principles when taking privacy regulatory action:

    - Independence — the OAIC will act independently and take action that is impartial and objective.
    - Accountability — the OAIC is accountable for its privacy regulatory action through a range of review and appeal rights, and will ensure stakeholders are aware of those rights[6].
    - Proportionality — the OAIC's privacy regulatory action will be proportionate to the situation or conduct concerned.
    - Consistency — the OAIC will strive to act consistently in a manner that is guided by and reflects this policy.
    - Timeliness — the OAIC will strive to conduct and finalise regulatory action as promptly as practicable.
    - Transparency — the OAIC will be open about how it uses its privacy regulatory powers, including by publishing relevant guidance (including this policy and the *Guide to privacy regulatory action*) and about the regulatory action it takes.

15. When taking privacy regulatory action, the OAIC will act consistently with general principles of good decision making, as explained in the *Best Practice Guides* published by the Administrative Review Council in 2007 and 2008.[7] In particular, the OAIC will act fairly and in accordance with principles of natural justice (or procedural fairness).

16. When dealing with an alleged contravention of the Privacy Act or other legislation, the OAIC will give individual consideration to that alleged contravention and have regard to all relevant circumstances.

17. In any litigation, the OAIC will act in accordance with its obligation to act as a model litigant in accordance with the *Legal Services Directions 2017*.

Commissioner's powers

A range of regulatory responses

18. The Privacy Act confers a range of regulatory powers on the Commissioner, including investigation and enforcement powers, which are based on an escalation model.

19. Privacy regulatory powers that allow the OAIC to work with an entity to facilitate compliance

[6] The available review and appeal rights are set out in the *Guide to privacy regulatory action*.

[7] The Administrative Review Council *Best Practice Guides* are published at Other ARC publications.

with privacy legal obligations and best practice privacy practice, include powers to:

- request an entity, group of entities, body or association to develop an APP code, or the CR code, and apply to the Commissioner for the code to be registered, or for the Commissioner to develop the code and register it (ss 26E(2), 26G, 26P(1) and 26R)
- direct an agency (but not an organisation) to give the Commissioner a privacy impact assessment (PIA) (s 33D)
- monitor, or conduct an assessment of, whether personal information is being maintained and handled by an entity as required by law, including requiring an entity that is the subject of an assessment to give information or produce a document (ss 28A and 33C)
- require an entity to give information, produce a document or answer questions relating to an actual or suspected eligible data breach or their compliance with notification obligations relating to an eligible data breach (s 26WU)
- direct a regulated entity to notify individuals at risk of serious harm, as well as the Commissioner, about an eligible data breach under Part IIIC of the Privacy Act (s 26WR).

20. Privacy regulatory powers that can be used to investigate or otherwise deal with an alleged interference with privacy are contained in Part V of the Privacy Act and include powers to:

- investigate a matter following a complaint (s 40(1)) or on the Commissioner's own initiative (referred to as a 'Commissioner initiated investigation' (CII)) (s 40(2))
- attempt to conciliate a complaint (s 40A)
- decline to investigate, or further investigate, a complaint (s 41)
- conduct preliminary inquiries to determine whether or not to open an investigation (s 42)
- decide whether or not to hold a hearing in response to a request from a complainant or respondent (for a complaint) or the respondent (for a CII) (s 43A)
- require information or a document to be produced, or a person to attend before the Commissioner to answer questions under oath or affirmation (ss 44–45)
- direct a complainant, respondent or other relevant person to attend a conference presided over by the Commissioner related to a complaint (failure to comply with the direction is an offence) (s 46)
- refer a complaint to an alternative complaint body specified in s 50.

21. Enforcement powers, that range from less serious to more serious regulatory action, include powers to:

- issue an infringement notice to a person who fails to give information, answer a question or produce a document when required to do so under the Act (ss 66(1) and 80UB)
- accept an enforceable undertaking (s 33E)
- bring proceedings to enforce an enforceable undertaking (s 33F)
- make a determination (s 52)
- bring proceedings to enforce a determination (ss 55A and 62)
- report to the Minister in certain circumstances following a CII, monitoring activity or assessment (ss 30 and 32)

- seek an injunction including before, during or after an investigation or the exercise of another regulatory power (s 98)
- apply to the court for a civil penalty order for a breach of a civil penalty provision (s 80W).

22. It is open to the OAIC to use a combination of privacy regulatory powers to address a particular matter.

23. The Commissioner has the power to share information or documents with enforcement bodies, alternative complaint bodies and other privacy authorities (including overseas privacy authorities) for the purpose of the Commissioner or the receiving body exercising their powers or performing their functions or duties (s 33A). Information-sharing can facilitate better cooperation between regulators to deliver better outcomes for Australians. The Commissioner also has the power to disclose certain information if it is in the public interest to do so (s 33B).

Approach to using privacy regulatory powers

Working with entities

24. The preferred regulatory approach of the OAIC is to work with entities to facilitate legal and best practice compliance. This will often be a more efficient and effective means of pursuing the objects of the Privacy Act. The OAIC can use a range of steps as part of this approach, only some of which involve the use of regulatory powers.

25. Our preferred regulatory approach is to facilitate voluntary compliance. The available steps for this include:

- engaging with regulated entities to provide guidance, promote best practice compliance, and identify and seek to address privacy concerns as they arise. This engagement may occur in different ways, including by providing policy guidance to entities, directing entities to relevant OAIC resources, conducting open dialogue between the OAIC and specific entities, and notifying an entity of any concerns held by the OAIC that the entity may not be complying with privacy obligations and allowing the entity an opportunity to respond to those concerns
- engaging with regulated entities who notify the Commissioner of a data breach incident to ensure compliance with relevant reporting obligations
- conducting an assessment of whether personal information is being maintained and handled by entities in accordance with applicable privacy legislative obligations, such as the APPs (s 33C). An assessment may enable the OAIC to identify privacy risks and areas of non-compliance, and may include recommendations as to how an entity might reduce risks or address areas of non-compliance
- recommending that an entity conduct a PIA where the entity proposes to engage in a new activity or function involving the handling of personal information about individuals, or when a change is proposed to information handling practices. A PIA is a systematic written assessment of an activity or function that identifies the impact that the activity or function might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.

26. In some cases, the OAIC may need to use its compulsive regulatory powers. The available steps include:

- requiring an entity to give information, produce a document or answer questions relating to an actual or suspected eligible data breach or their compliance with notification obligations relating to an eligible data breach (s 26WU)
- giving a notice to an entity being assessed by the OAIC requiring the entity to give information or produce a document (s 33C)
- formally directing an agency to conduct a PIA where the entity proposes either to engage in a new activity or function involving the handling of personal information about individuals, or to make a substantive change to information handling practices, and the OAIC considers that the activity or function might have a significant impact on the privacy of individuals (s 33D).

27. The fact that an entity has engaged cooperatively with the OAIC will be taken into account in deciding whether to take regulatory action and what regulatory action to take.

Investigating an alleged interference with privacy

28. An investigation may be commenced by the OAIC into a suspected or alleged interference with privacy, either on receipt of a complaint or as a Commissioner initiated investigation (CII).

29. The OAIC is required to investigate a complaint made under the Act about an act or practice that is alleged to be an interference with the privacy of an individual or class of individuals, if certain conditions are satisfied (ss 36, 40), and the complaint is not declined under s 41[8] or referred to an alternative complaint body under s 50.

30. When investigating a complaint, the OAIC must make a reasonable attempt to conciliate the complaint (s 40A). Most complaints are resolved in this way. The OAIC may decline to investigate or further investigate a complaint if there is no reasonable likelihood of a conciliated outcome (s 40A(4)).

31. The Commissioner may, on his or her own initiative, decide to investigate an act or practice that may be an interference with the privacy of an individual or a breach of APP 1 (s 40(2)). The Commissioner may decide to commence a CII following a complaint or notification of a data breach incident, or may commence a CII independently of any complaint or notification.[9]

32. When deciding whether or not to open a CII, the OAIC may consider whether the entity has complied with data breach notification requirements, has taken appropriate steps to respond to a breach, and has cooperated with the OAIC in remedying any breach.

33. In investigating a complaint or conducting a CII, the OAIC will seek to work with the parties concerned. The Commissioner may use the formal powers conferred by the Privacy Act including to require an individual or entity to provide information and documents (s 44).

Exercising enforcement powers

34. Following a complaint investigation or CII, the Commissioner may decide to take enforcement

[8] The OAIC's approach to using the decline powers in s 41 is outlined in the *Guide to privacy regulatory action*. Examples of where a complaint may be declined include where it is frivolous, vexatious, misconceived, lacking in substance or not made in good faith; an investigation is not warranted having regard to all the circumstances; the complaint was made more than 12 months after the complainant became aware of the relevant act or practice; and the complaint would be more effectively or appropriately dealt with by a recognised external dispute resolution scheme.

[9] For more information on when a CII may be commenced, see Chapter 2 of the *Guide to privacy regulatory action*.

action against an entity.

35. The available enforcement powers escalate from less serious to more serious options as outlined in paragraph 21 above.

Selecting appropriate privacy regulatory action

36. Alleged interferences with privacy or other privacy concerns may come to the OAIC's attention through a range of avenues that include:

- a complaint by an individual, or a representative complaint
- a data breach notification
- engagement with stakeholders
- a referral from another regulator or external dispute resolution scheme
- media and social media
- information provided by an informant
- information provided by a law enforcement agency
- during the course of an assessment or investigation conducted by the OAIC.

37. As noted above, the OAIC is required to investigate a complaint if certain conditions are satisfied, but has a discretion to take other privacy regulatory action, including commencing a CII.

38. Noting its preferred approach to work with entities in the first instance, the OAIC will use discretion to select and target matters that warrant privacy regulatory action, and to decide what action to take in those matters. This involves considering both the risk that a matter poses to the goal of promoting and ensuring personal information protection, and the opportunity that taking action presents.

39. For example, risk is likely to be greater where the personal information of a larger number of people is involved, while the opportunity might be greatest where an alleged contravention is suspected to be systemic within an industry and regulatory action can deliver a targeted compliance message to that industry.

Factors taken into account

40. Where it has a discretion as to whether to take regulatory action, the OAIC must prioritise matters for privacy regulatory action and select the most appropriate power in the circumstances. Factors the OAIC will take into account in deciding when to take privacy regulatory action, and what action to take, include the following (as applicable):

- the objects of the Privacy Act (set out in s 2A)
- the seriousness of the incident or conduct to be investigated (or the potential impact of a proposal), including:
    - the number of persons potentially affected

  - whether the matter involves 'sensitive information'[10] or other information of a sensitive nature, the adverse consequences caused or likely to be caused to one or more individuals arising from an incident or conduct
  - whether disadvantaged or vulnerable groups may have been or may be particularly adversely affected or targeted
  - whether conduct was deliberate or reckless
  - the seniority and level of experience of the person or persons responsible for the conduct
- the level of public interest or concern relating to the conduct, proposal or activity (with regulatory action more likely to be taken where significant public interest or concern exists)
- whether the burden on the entity likely to arise from the regulatory action is justified by the risk posed to the protection of personal information
- the specific and general educational, deterrent or precedential value of the particular privacy regulatory action, including whether pursuing court action (where applicable) would test or clarify the law
- whether the entity responsible for the incident or conduct has been the subject of prior compliance or regulatory enforcement action by the OAIC, and the outcome of that action
- the likelihood of the entity contravening the Privacy Act, or other legislation that confers functions relating to privacy on the Commissioner, in the future
- whether the conduct is an isolated instance, or whether it indicates a potential systemic issue[11] (either within the entity concerned or within an industry) or an increasing issue which may pose ongoing compliance or enforcement issues
- action taken by the entity to remedy and address the consequences of the conduct, including whether the entity attempted to conceal a contravention or a data breach, and whether the entity cooperated with the OAIC and notified affected individuals if appropriate
- the time since the conduct occurred
- the cost and time to the OAIC in order to achieve an appropriate remedy through enforcement action
- whether there is adequate evidence available and admissible in a court to prove a contravention on the balance of probabilities
- that a new personal information handling activity or function or change to an existing personal information handling activity or function is planned, or a new personal information handling practice has been recently implemented or an existing practice changed
- any other factors which the OAIC considers relevant in the circumstances, including factors which are relevant to the specific regulatory power being used.

41. The OAIC may also undertake an assessment of an entity where it is specifically funded to do so

[10] 'Sensitive information' is defined in s 6 of the *Privacy Act 1988* (Cth).

[11] See paragraphs 12–13 of this policy.

under a memorandum of understanding (MOU). The OAIC is a party to MOUs with various government agencies. The MOUs are published on the OAIC website. Details about funding for assessments are contained in the Office's annual report.

Sources of information

42. The OAIC will use the approach and factors outlined above to decide when to take privacy regulatory action in a particular matter, and what action to take. However, the OAIC will also seek to identify both systemic issues[12] and serious issues that can be targeted for privacy regulatory action. The OAIC will use a range of sources for this purpose, including:

- individual complaints and data breach notifications
- complaint and data breach notification trends
- international developments
- media reports
- informants
- surveys
- privacy assessments
- Commissioner initiated investigations
- credit reporting body annual reports
- information from recognised external dispute resolution schemes, including in annual reports provided to the OAIC
- reports from APP code administrators.

43. The information may also be used to identify particular sectors in government or industry, or recurring acts or practices, that warrant privacy regulatory action. These sectors or acts or practices are areas where the OAIC believes privacy regulatory action is necessary in order to have a significant impact on the protection and handling of personal information. For example, if its complaints statistics showed that a significant number of complaints relate to a particular industry, that industry may be identified for privacy regulatory action. In addition to using the prioritisation factors in the above list, the OAIC will also prioritise matters that fit within any identified sector or involve an identified act or practice. Where sectors or acts or practices are identified from time to time, they will be noted on the OAIC's website.

Working with other complaint and regulatory bodies

Interaction with recognised EDR schemes

44. Under s 35A of the Privacy Act, the Commissioner may recognise an external dispute resolution (EDR) scheme to handle particular privacy related complaints. EDR schemes constitute the second tier of a three-tiered complaint process:

[12] See paragraphs 12–13 of the policy.

- an individual should first make a complaint in writing to a respondent entity and allow the entity a reasonable time to respond
- an individual who is not satisfied with the response or outcome may complain to a recognised EDR scheme of which the entity is a member (if any)
- an individual who is not satisfied with the outcome of the EDR process may complain to the OAIC. The OAIC will consider whether to accept the complaint or to decline to investigate under s 41 of the Privacy Act.

45. A complainant who has not first complained to a recognised EDR scheme of which the respondent entity is a member will generally be advised to do so before the OAIC will accept the complaint.[13] Otherwise, the OAIC will generally use its power to decline complaints that are being or could be dealt with by a recognised EDR scheme (ss 41(dc) and (dd)), in preference to formally referring the matter to the recognised EDR scheme (s 50).

46. Generally, the OAIC will seek to work in partnership with recognised EDR schemes, with a view to achieving consistent and efficient regulatory outcomes. The OAIC will seek to implement open communication practices to ensure information and experience is shared between the OAIC and the schemes, and that clear procedures are established to enable information about complaints to be transmitted.

Interaction with domestic regulators and alternative complaint bodies

47. A matter may fall within the jurisdiction both of the OAIC and of another Australian regulator, including State and Territory privacy regulators, regulators in other sectors and law enforcement agencies.

48. The OAIC will seek to work in partnership with other regulators, recognising the practical and resource advantages in doing so. This may include agreeing to a written protocol or principles for collaboration, regular communication about privacy issues, sharing experience and coordinating the regulatory processes of the OAIC and other regulators.

49. The OAIC also has information sharing powers, including the ability to share information acquired in the exercise of its powers or performing its functions or duties under the Privacy Act with enforcement bodies, alternative complaint bodies and privacy authorities of Australian State or Territory governments (s 33A), and the ability to disclose information if satisfied that it is in the public interest to do so (s 33B). However, the OAIC will always operate independently within its legislative framework, including limits on its ability to share information.

50. Where the OAIC receives a complaint, it may not always be the most appropriate body to investigate and resolve that complaint. It has various powers to decline to investigate where there is an alternative applicable law or complaint handling body, or to refer complaints to other complaint bodies in certain circumstances.

[13] The Privacy Act s 40(1A) similarly provides that the OAIC shall not investigate a complaint if the complainant has not first complained to the respondent entity and allowed a reasonable time to respond, unless the OAIC decides that it is not appropriate to require the complainant to take that step (see also s 41(2)).

Interaction with foreign regulators

51. Many privacy threats and challenges extend beyond national boundaries. A coordinated and consistent global response can be an effective regulatory response to a global privacy issue.

52. In dealing with an interference with privacy or potential privacy risk that operates across national boundaries, there can be a practical and resource advantage in liaising with other privacy regulators to avoid duplication, share information and coordinate the release of investigation findings. The OAIC has the power to share relevant information acquired in the exercise of its powers or performing its functions or duties under the Privacy Act with foreign privacy authorities (s 33A).

53. The OAIC will seek to work in partnership with privacy regulators in foreign jurisdictions where there is a shared interest in working together to address privacy breaches, threats and risks. Through such partnerships, the OAIC will share knowledge and expertise with a view to ensuring a consistent and harmonised approach to regulatory action in a particular matter. If appropriate, it may also seek to coordinate regulatory activities and share investigative information with foreign privacy regulators. However, the OAIC will always operate independently within its legislative framework, including limits on its ability to share information. In addition, where information is shared including under ss 33A and 33B, only necessary information will be shared and the information exchange will generally occur under information sharing frameworks which protect the confidentiality of the information, for example the Global Cross Border Enforcement Cooperation Arrangement, the APEC Cooperation Arrangement for Cross-Border Privacy Enforcement or a memorandum of understanding.

54. As part of this commitment to international cooperation and privacy enforcement, the OAIC will continue to actively engage with global privacy networks, including the Asia Pacific Privacy Authorities Forum (APPA), the OECD Global Privacy Enforcement Network (GPEN) and the APEC Cross Border Privacy Enforcement Arrangement.

Public communication as part of privacy regulatory action

55. Public communication of the work of the OAIC is an important element in privacy regulatory action and fulfilling the objectives of the Privacy Act. This includes:

    - encouraging privacy compliance by increasing awareness and knowledge of privacy rights and obligations, and deterring contravening conduct
    - promoting public confidence in the regulatory activities of the OAIC, by publicising actions taken to address privacy breaches and deal with entities that are not complying with privacy obligations or compelling relevant non-complying entities to do so, and
    - ensuring transparency and accountability around the OAIC's use of its privacy regulatory powers.

56. The OAIC may communicate directly with the public or in limited circumstances can compel a person or entity to publish or otherwise communicate information. Specifically:

- where there has been a determination under s 52, the OAIC may compel a person or entity to publish (or communicate by other agreed means) information about the breach and appropriate remediation action (ss 52(1)(b)(iia), 52(1A)(ba))
- if the Commissioner is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity, the Commissioner may direct the entity to prepare a statement and notify individuals about the eligible data breach (s 26WR).

Communications approach

57. A decision to communicate information publicly will be guided by the principles identified in this policy under the heading 'Regulatory action principles': see paragraph 14. In addition, the OAIC will strive to ensure that:

    - all public statements are accurate, fair and balanced
    - it is clear that an allegation of an 'interference with privacy' is no more than an allegation until substantiated by the OAIC, a tribunal or a court
    - a comment on a court proceeding involving a Privacy Act issue, prior to the resolution of the proceedings, will generally be confined to the history of the proceedings and any earlier findings by the OAIC or an alternative complaint body and will comply with any other limitations such as implied undertakings and suppression orders
    - all public statements comply with the OAIC's legal obligations, including privacy, confidentiality and secrecy obligations and court or tribunal rules and orders
    - if the OAIC has previously commented publicly that it is investigating an alleged privacy breach by an entity, and later finds that a privacy breach was not substantiated, a public statement to that effect will generally be made.

58. Under s 33B, the OAIC has the power to disclose information acquired by the Commissioner if it is in the public interest to do so. When considering the public interest for the purposes of information published pursuant to this power, the Commissioner must consider the factors set out in s 33B(2):

    - the rights and interests of any complainant or respondent
    - whether the disclosure is likely to prejudice another investigation by the Commissioner
    - whether the disclosure is likely to disclose the personal information of another person
    - whether the disclosure is likely to disclose any confidential commercial information
    - whether the disclosure would be likely to prejudice enforcement related activities by or on behalf of an enforcement body.

59. The OAIC is committed to dealing fairly with any entity that may be the subject of privacy regulatory action when making any public statement relating to that regulatory action. The OAIC is mindful of the negative inferences and reputational damage to an entity that may arise from the fact that an investigation has been opened or that an 'interference with privacy' has been alleged.

60. Where making a public statement in connection with privacy regulatory action, the OAIC will aim to contact the respondent entity in advance of making the statement if it is possible and appropriate in the circumstances. However, it will generally not provide an individual or entity with an assurance that the OAIC will not publicise its regulatory action or that it will give

advance warning.

61. To the extent possible, the OAIC will publish reports and other documents relevant to the exercise of regulatory powers in full or in an abridged version on the OAIC website. It is sometimes inappropriate to publish all or part of a report or document because of statutory secrecy provisions or for reasons including privacy, confidentiality, commercial sensitivity, security or privilege.[14]

Examples of OAIC communications

62. The OAIC may communicate publicly the outcome of privacy regulatory action, including in the following ways:

- issuing a public report following an assessment (s 33C(8))
- publishing a PIA direction issued to an agency
- publishing a determination made by the Commissioner (s 52(5A))
- publishing an enforceable undertaking accepted by the Commissioner
- issuing a public statement at the commencement and conclusion of a CII
- issuing a public statement where the OAIC commences court proceedings and upon finalisation of those proceedings.

63. The OAIC generally will not comment publicly about ongoing complaint investigations, complaint conciliations, CIIs, the content of data breach notifications or the exercise of investigative powers. However, where a particular incident is of community concern and has already been reported in the media, the OAIC may confirm publicly that it is investigating or making inquiries in relation to the matter but will generally not comment further until the inquiries or investigation is complete. The OAIC may also comment publicly on a particular incident where there is a public interest in it doing so, for example to enable members of the public to respond to a data breach.

64. The OAIC will publish general statistics which reflect both its privacy regulatory action processes and regulatory outcomes. These statistics will be contained in the annual report, and include statistics on:

- complaints received
- the stage at which complaints were closed
- complaints declined via the various decline powers contained in s 41
- complaint outcomes
- CIIs undertaken
- data breach notifications received
- assessments undertaken.

[14] Section 33 of the Privacy Act is also relevant to the inclusion of certain matters in reports to the Minister.