Chapter 6: Civil penalties — serious or repeated interference with privacy and other penalty provisions

Contents

Legislative framework

6.1 Section 80W of the Privacy Act empowers the Commissioner to apply to the Federal Court or Federal Circuit Court for an order that an entity, that is alleged to have contravened a civil penalty provision in that Act, pay the Commonwealth a penalty.

6.2 Each civil penalty provision specifies a maximum penalty for contravention of that provision. The penalty is expressed in 'penalty units'. The value of a penalty unit is contained in s 4AA of the *Crimes Act 1914* (Cth).[1]

6.3 The 'civil penalty provisions' in the Privacy Act include:

- a serious or repeated interference with privacy (s 13G) – 2000 penalty units

[1] The value of a penalty unit as at July 2017 is $210 — see https://www.legislation.gov.au/Series/C1914A00012

- various civil penalty provisions set out in Part IIIA – Credit reporting, with penalties of either 500, 1000 or 2000 penalty units.[2]

6.4 Under s 79 of the My Health Records Act, the Commissioner may apply to a court for an order that a person who is alleged to have contravened a civil penalty provision in that Act pay the Commonwealth a civil penalty. Section 79 triggers the provisions of Part 4 of the Regulatory Powers Act which deals with seeking and obtaining a civil penalty order for contraventions of civil penalty provisions.

6.5 The 'civil penalty provisions' in the My Health Records Act include:

- unauthorised collection, use or disclosure by a person of health information included in a healthcare recipient's My Health Record, where the person knows or is reckless as to the fact the collection, use or disclosure is not authorised (s 59(1) and (2)) — criminal offence penalty is 120 penalty units or imprisonment for 2 years, or both. The civil penalty is 600 penalty units.
- use or disclosure by a person of health information included in a healthcare recipient's My Health Record where the information was disclosed to the person in contravention of s 59(2) and the person knows or is reckless as to that fact (s 60(1)) — criminal offence penalty is 120 penalty units or imprisonment for 2 years, or both. The civil penalty is 600 penalty units.
- five other civil penalty provisions set out in Part 5 that relate to:
  - failing to provide required information to the My Health Record System Operator — 100 penalty units
  - failure by a registered healthcare provider organisation, registered repository operator, registered portal operator or a registered contracted service provider to notify a data breach, including a potential data breach, to the OAIC and/or My Health Record System Operator as soon as practicable after becoming aware of the breach — 100 penalty units.
  - failure by a registered healthcare provider organisation, a registered repository operator, a registered portal operator or a registered contracted service provider to notify the System Operator of ceasing to be eligible to be registered — 80 penalty units.
  - holding or taking records outside Australia — criminal offence penalty of 2 years imprisonment or 120 penalty units, or both, civil penalty of 600 penalty units.
  - certain contraventions of the My Health Records Rules — 100 penalty units.

6.6 Particular conduct may contravene both a civil penalty provision in the My Health Records Act and the 'serious or repeated interference with privacy' civil penalty provision in the Privacy Act (s 13G). This is because contraventions of the My Health Records Act are interferences with privacy for the purposes of the Privacy Act, and so the OAIC may be able to seek a civil penalty for contravention of s 13G of the Privacy Act where the interference with privacy arises from a breach of the My Health Records Act.

6.7 An entity (or person) will also contravene a civil penalty provision, and be liable to pay a penalty, if it:

[2] Some credit reporting civil penalty provisions have analogous 'offence' provisions. Sections 80ZD-80ZF of the Privacy Act outline when civil proceedings can be commenced and continued where criminal proceedings may also be initiated.

- attempts to contravene a civil penalty provision
- aids, abets, counsels or procures a contravention of a civil penalty provision
- induces a contravention of a civil penalty provision
- is knowingly concerned in or a party to a contravention of a civil penalty provision, or
- conspires with others to effect a contravention of a civil penalty provision.[3]

6.8 Under s 80W(2) of the Privacy Act, the Commissioner's application to the court for a civil penalty order must be made within six years of the alleged contravention. In relation to the My Health Records Act, the Commissioner's application to the court for a civil penalty order must be made within four years of the alleged contravention (s 79 of the My Health Records Act (see also Part 4 of the Regulatory Powers Act)).

6.9 If the court is satisfied that the entity (or person) has contravened the civil penalty provision (taking into account the relevant matters set out in the applicable legislation), it may order the entity (or person) to pay such penalty as the court determines appropriate. The maximum penalty that the court can order is the amount listed in the civil penalty provision or, for a body corporate, five times that amount (Privacy Act s 80W(5) and My Health Records s 79 (see also Part 4 of the Regulatory Powers Act)).

6.10 Where conduct contravenes more than one civil penalty provision, proceedings may be commenced in relation to each contravention; however, the entity (or person) cannot be liable for more than one penalty in relation to that conduct (Privacy Act s 80Y; My Health Records Act s 79 (see also Part 4 of the Regulatory Powers Act)).

6.11 Where an entity (or person) contravenes a single civil penalty provision multiple times, the court may award a single civil penalty order. However, the amount of that penalty cannot exceed the sum of the maximum penalties that could be ordered if a separate civil penalty order was made for each contravention (Privacy Act s 80Z; My Health Records Act s 79 (see also Part 4 of the Regulatory Powers Act)).

Purpose and key features of seeking a civil penalty order

6.12 By requiring the payment of a penalty to the Commonwealth, a civil penalty order financially penalises an entity or person. A civil penalty order does not compensate individuals adversely affected by the contravention.[4]

6.13 The OAIC will not seek a civil penalty order for all contraventions of a civil penalty provision in the Privacy Act or My Health Records Act. The OAIC is unlikely to seek a civil penalty order for minor or inadvertent contraventions, where the entity or person responsible for the contravention has cooperated with the investigation and taken steps to avoid future contraventions.

---

[3] Section 80V of the Privacy Act and s 79 of the My Health Records Act (see also Part 4 of the Regulatory Powers Act).

[4] While a civil penalty order does not compensate individuals, sections 25 and 25A of the Privacy Act do permit an individual to recover compensation or other remedies where a civil penalty order is made against an entity for a contravention of a civil penalty provision contained in Part IIIA (Credit reporting) of the Privacy Act.

Who can be liable for a civil penalty?

6.14 A civil penalty order under the Privacy Act can only be made against 'an entity'. The term 'entity' means an agency, an organisation or a small business operator (these terms are further defined in s 6(1)). The term 'organisation' can include an individual (including a sole trader).

6.15 A civil penalty order under the My Health Records Act can only be made against 'a person'.[5] This term includes both individuals and participants in the My Health Record system, such as registered repository operators, portal operators and healthcare provider organisations.

Applicable mental elements

6.16 For certain civil penalty provisions under the My Health Records Act,[6] a person can only be liable for a penalty where a particular mental element (knowledge or recklessness) is made out.

6.17 There are no applicable mental elements for civil penalty provisions in the Privacy Act.

Determining the penalty to impose

6.18 In determining the penalty to be imposed, s 80W(6) of the Privacy Act and s 79 of the My Health Records Act (see also Part 4 of the Regulatory Powers Act) provide that the Court must take into account all relevant matters, including:

- the nature and extent of the contravention
- the nature and extent of any loss or damage suffered because of the contravention
- the circumstances in which the contravention took place
- whether the entity (or person) has previously been found by a court in proceedings under the Privacy Act or My Health Records Act (or the Crimes Act or Criminal Code in relation to the My Health Records Act) to have engaged in any similar conduct.

Serious or repeated interference with privacy

6.19 Section 13G of the Privacy Act is a civil penalty provision for cases of serious or repeated interference with privacy by an entity.

6.20 An 'interference with privacy' is defined in s 13 of the Act, and is a breach of the Privacy Act or of a privacy-related provision in certain other legislation.[7]

6.21 The phrases 'serious interference with privacy' and 'repeated interference with privacy' are not defined in the Privacy Act. The Explanatory Memorandum to the *Privacy Amendment*

---

[5] The term 'person' is not defined in the My Health Records Act, so the meaning is drawn from the *Acts Interpretation Act 1901* (Cth). That Act states that expressions used to denote persons generally, such as 'person', include a body politic or body corporate as well as an individual (s 2C).

[6] My Health Records Act ss 59 and 60.

[7] For example, the *Data-matching Program (Assistance and Tax) Act 1990*, the s 135AA guidelines issued under the *National Health Act 1953*, the *Healthcare Identifiers Act 2010*, the *Personally Controlled Electronic Health Records Act 2012*, the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, and the *Personal Property Securities Act 2009*.

(Enhancing Privacy Protection) Act 2012[8] which introduced these terms into the Privacy Act states that the ordinary meaning of the terms 'serious' and 'repeated' will apply.

6.22 'Serious interference with privacy' and 'repeated interference with privacy' are two distinct concepts, either of which may lead the OAIC to seek a civil penalty against an entity. However, in some cases, acts or practices may meet the requirements for both concepts, for example where a single incident that forms part of a repeated interference with privacy is also a serious interference with privacy.

Serious interference with privacy

6.23 Whether an interference with privacy is 'serious' is an objective question that will reflect what a reasonable person would consider serious. This means that what is considered a serious interference with privacy may vary and evolve over time as technology and community expectations regarding privacy protections change.

6.24 The following factors are relevant in considering whether a particular interference with privacy is serious:

- the number of individuals potentially affected
- whether it involved 'sensitive information' or other information of a sensitive nature
- whether significant adverse consequences were caused or are likely to be caused to one or more individuals from the interference
- whether vulnerable or disadvantaged people may have been or may be particularly adversely affected or targeted
- whether it involved deliberate or reckless conduct
- whether senior or experienced personnel were responsible for the conduct.

6.25 The OAIC will not seek a civil penalty order in all matters involving a 'serious' interference with privacy. The OAIC is more likely to seek a civil penalty in a particular matter where one of the following factors is present:

- the serious interference with privacy is particularly serious or egregious in nature. This may arise because a number of different indicators of seriousness are present (for example, the breach involved the health information of a large number of individuals and significant adverse consequences have arisen or are likely to arise), or because one particular indicator of seriousness is present to a significant extent, such as a very large number of individuals being affected, or very substantial detriment having occurred
- the entity has a history of serious interferences with privacy
- the OAIC reasonably considers the serious interference with privacy arose because of a failure by the entity to take its privacy obligations seriously, or a blatant disregard by the entity for its privacy obligations.

6.26 In addition, when deciding whether to commence proceedings against an entity seeking a civil penalty for serious interference with privacy, the OAIC will take into account the factors outlined in paragraph 38 of the *Privacy regulatory action policy*.

[8] See https://www.legislation.gov.au/Series/C2012A00197

6.27 While a history of serious contraventions can be a relevant factor, it is not a prerequisite to the OAIC seeking a civil penalty for serious interference with privacy, and it is possible for a single breach by an entity to be the catalyst for the commencement of proceedings.

Repeated interference with privacy

6.28 'Repeated interference with privacy' means that an entity has interfered with the privacy of an individual or individuals on two or more separate occasions. These repeated interferences with privacy could arise from:

- the same act or practice done on two or more occasions
- different acts or practices done on two or more occasions.

6.29 The relevant acts or practices must have occurred on separate occasions. This means that an act or practice that simultaneously results in the interference with privacy of several individuals – such as a mail merge error leading to the personal information of multiple individuals being disclosed to third parties – will not in itself constitute a 'repeated' interference with privacy. Similarly, a single act which results in the breach of multiple APPs will not in itself be a 'repeated' privacy interference.[9]

6.30 The OAIC will not seek a civil penalty order in all matters involving repeated interference with privacy. The cases in which the OAIC is more likely to seek a civil penalty for repeated interference with privacy are those where:

- the entity failed to take reasonable steps to correct and improve its privacy practices following earlier interferences with privacy. The reasonable steps in a particular circumstance will depend on the nature and causes of the earlier interferences with privacy, but may include having conducted an audit of privacy practices and implementing audit findings, conducting staff privacy training, updating entity policies and procedures relating to personal information handling, and improving information security measures
- the repeated privacy interferences demonstrate a failure by the entity to take its privacy obligations seriously, or a blatant disregard by the entity for its privacy obligations
- the contraventions comprising the repeated privacy interferences are more serious in nature (whether or not a penalty for serious interference with privacy has previously been imposed)
- interferences with privacy have occurred on a greater number of occasions
- the repeated privacy interferences occur within a short period of time.

6.31 In addition, when deciding whether to commence proceedings against an entity seeking a civil penalty for repeated interference with privacy, the OAIC will take into account the factors outlined in paragraph 38 of the *Privacy regulatory action policy*.

6.32 While the seriousness of the contraventions comprising the repeated interference with privacy will be taken into account, the separate contraventions comprising the sequence of repeated interferences with privacy do not need to be serious for the OAIC to seek a civil

[9] While these examples would not in themselves constitute repeated interferences with privacy, depending on the circumstances the incidents could still constitute a serious interference with privacy or, if it is one incident in a series of other contraventions committed by the same entity, it could constitute repeated privacy interference together with those other contraventions.

penalty. If the OAIC is satisfied that another aspect of the contraventions justifies the seeking of a civil penalty order (such as an apparent blatant disregard by the entity for its privacy obligations) then the OAIC may decide to seek a civil penalty order.

Serious or repeated privacy interference and pre-12 March 2014 conduct

6.33 Item 6 of Schedule 6 to the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* provides that s 13G applies in relation to an act done, or a practice engaged in, after 12 March 2014.

6.34 This means that where the OAIC applies to a court for a civil penalty order against an entity for serious or repeated interference with privacy, the OAIC can only lead evidence relating to interferences with privacy that have occurred since 12 March 2014 to establish its case.

Procedural steps

6.35 When seeking a civil penalty order from the courts is a possible regulatory outcome in a matter, the OAIC will generally use the following process:

- The OAIC will first investigate the matter, either in response to a complaint or on the Commissioner's own initiative. Information on complaint investigations is contained in Chapter 1 of this guide, while information on Commissioner initiated investigations is contained in Chapter 2.
- Where the OAIC's investigation indicates that it is likely that an interference with privacy has occurred, the OAIC will consider whether to take enforcement action and, if so, what enforcement action to take. The OAIC will review the matter against either the *Privacy regulatory action policy* (including the factors set out in paragraph 38) or the My Health Records Enforcement Guidelines as applicable to assess the appropriate enforcement response.
- Where seeking a civil penalty order is identified as the appropriate regulatory response in the circumstances, the OAIC will assess the matter to determine whether or not sufficient evidence exists to take successful court action. External legal counsel may be briefed. This includes evaluating:
    - whether there is sufficient admissible evidence for each element of the alleged contravention to successfully establish the case on the balance of probabilities
    - the availability, competence and credibility of witnesses
    - any mitigating factors that might reasonably be raised before the court by the respondent
    - the possibility that any evidence might be excluded by a court.
- Where the available evidence is sufficient, the Commissioner will consider and decide whether to commence proceedings. To make this decision, the Commissioner will use either the *Privacy regulatory action policy* (including the factors set out in paragraph 38) or the My Health Records Enforcement Guidelines as applicable. Where proceedings are to be commenced, external legal counsel will usually be engaged to run the matter.

- The court documents to initiate proceedings will be prepared and lodged with the court, and served on the respondent entity.
- The OAIC will pursue the court proceedings in accordance with its model litigant obligations, any relevant court rules and procedures, and any directions or orders issued by the court.
- Following judgment, the OAIC will generally publicly communicate the outcome of the proceedings.
- If the OAIC is dissatisfied with the court's decision (for example, if the court refused to impose a penalty, or the OAIC considers the imposed penalty inadequate), the OAIC may consider the possible grounds for appeal and whether or not to institute appeal proceedings. In making this decision, the OAIC will act in accordance with its model litigant obligations.
- If the respondent appeals the decision, the OAIC will participate in the appeal proceedings and will act in accordance with its model litigant obligations.

Publication

6.36 The OAIC will publicly communicate the following information in connection with civil penalty proceedings:

- civil penalty proceedings against a particular respondent have been initiated
- the outcome of civil penalty proceedings
- the lodgement of appeal proceedings by either the OAIC or the respondent
- the outcome of any appeal proceedings.

6.37 Where it is appropriate for the OAIC to comment on civil penalty proceedings prior to their resolution, such comment will generally be restricted to the history of the proceedings and any earlier findings by the OAIC or an alternative complaint body.

6.38 Any publications relating to civil penalty proceedings will comply with any relevant court orders.

Additional resources

- Chapter 1 of this guide for information relating to the OAIC's complaint investigation procedures
- Chapter 2 of this guide for information relating to the OAIC's Commissioner initiated investigation procedures.