SQUIRE PATTON BOGGS

Is Your Business at Risk? Understanding Australia's Privacy Tort

Australia – June 2025

The *Privacy Act 1988* (Cth) (Act) is one of the longest-standing pieces of national data protection legislation in the world, but – despite its name – it has been more concerned with regulating use of individuals' personal data than granting them an actionable, stand-alone right to privacy.

As of last week, this has changed. Australians now have access to a new statutory cause of action (or tort), built into the Act, for serious invasions of their privacy. The elements of the tort have been much discussed already, but in short, the cause of action arises in the following circumstances:

- An individual suffers an invasion of their privacy either by an intrusion into their seclusion and/or misuse of information. The Act contemplates an individual may be able to claim for both elements, e.g. where any material produced from an intrusion into seclusion is published by the defendant.
- A person in the individual's position would have had a reasonable expectation of privacy.
- The invasion of privacy was intentional or reckless.
- The invasion of privacy was serious.
- the public interest in the plaintiff's privacy outweighed any countervailing public interest.

Here are our answers to some of the questions we have heard our clients ask:

- **How does this cause of action relate to other parts of the Privacy Act?** In short – it generally does not. Section 6(2) of Schedule 2 states that unless specified otherwise, "in determining the meaning of an expression used in [Schedule 2], an expression used in the rest of this Act is to be disregarded." We know that expressions used in, for example, the Australian Privacy Principles (APPs) (such as "collect") will not have the same meaning when they are used in Schedule 2. The invasion of privacy also does not need to involve "personal information" (as defined in the Act) or constitute a breach of any other part of the Act to be actionable.
- **But what about existing exemptions?** It is likely that these will not apply either. Under Section 7B(3), the "employee records" provision exempts from the Act an act or practice engaged in by an "organisation" that is or was an employer, if the act or practice is directly related to:
  - A current or former employment relationship between the employer and the individual
  - An employee record held by the employer that relates to the individual

  Schedule 1 to the Act – which sets out the APPs – only applies to "organisations". Accordingly, any organisation that is covered by the employee records exemption is not required to comply with the APPs, at least in relation to covered acts and practices. Schedule 2 – containing the tort – gives an individual (aka "plaintiff") the right to claim against "another person" (aka "defendant"). Since Schedule 2 allows for claims to be made against a broader category of persons than "organisations", the employee records exemption will not protect a defendant from the application of the tort.

  In practice, however, it may be difficult for an employee plaintiff to satisfy the other elements of the tort. For example, some state and territory surveillance laws require employers to tell their staff about monitoring of email, internet and other company resources, while other laws require an employee's consent. Where notice has been provided or consent has been obtained, a plaintiff may find it more difficult to establish a "reasonable expectation of privacy".
- **What is meant by "intruding upon seclusion" and "misuse of information"?** Both concepts are well understood under other commonwealth and/or US laws, and Australian courts may look to case law in these countries when interpreting these terms. The Act nonexhaustively defines "intruding upon…seclusion" as *physically* intruding on a person's private space, or watching, listening to or recording a person's private activities or affairs. There seems to be no requirement for subsequent action (e.g. publication). The New Zealand High Court[1] interpreted the term in a similar way: a defendant who recorded his flatmate's girlfriend in the shower was found to have "intruded into [her] solitude and seclusion",[2] even without any further communication of the video.

  "Misusing information" is defined more broadly (and nonexhaustively) as collecting, using or disclosing information about an individual. Again, looking to other jurisdictions (this time, the UK), "misuse" has taken on a variety of meanings, including disclosure of text or images but also the very act of intrusion itself (even if no disclosure was made).[3]

1 *C v Holland* [2012] 3 NZLR 672

2 Id at Paragraph 6.

3 See, for example, *Gulati v MGN Limited* [2015] EWHC 1482, where the High Court agreed with the claimants that the newspapers engaged in "three areas of wrongful behaviour", including "the general [phone] hacking activity". Phone hacking constituted a misuse of private information "irrespective of whether an article was published" and for which damages could be awarded separately from damage arising from publication: Paragraph 155.

- **What are the inbuilt limitations on this cause of action?** It is critical to understand that the (many) required elements of this tort have the effect of limiting the circumstances where the tort is actionable. In particular:
  - It seems like a defendant must take positive action before a plaintiff can claim that either an intrusion upon seclusion or a misuse of information has taken place. Even "misuse" of information seems to require that the information is first used by the defendant in some way. Although it would not be binding on Australian courts, this view is supported by *Warren v DSG Retail Ltd*,[4] where the English High Court held that DSG Retail Limited's failure to keep data secure through "basic security measures" did not constitute a positive "misuse" of the data when the data was eventually hacked by a third party.
  - Individuals must have a reasonable expectation of privacy. As discussed above, there may be circumstances where this expectation cannot be established, including in a workplace context where surveillance has been notified to staff (in accordance with any applicable workplace surveillance laws). Similarly, it is unlikely that an individual would be able to argue that they had a reasonable expectation of privacy in a public place, including, for example, a shopping centre or public park. The English Court of Appeal's statement[5] that "courts should, in the absence of special facts, generally expect people to adopt a reasonably robust and realistic approach to living in the 21st century" is not binding but might help set the scene for Australian courts.
  - The invasion of privacy must be either intentional or reckless. At first glance, this might assuage fears around all data breaches suddenly giving rise to tortious claims. Many such breaches will be caused by negligence, rather than intention or even recklessness. While this may not always be the case, this requirement – combined with the need to establish "positive action" (as set out above) – may "raise the bar" when a plaintiff is attempting to prove that a corporate defendant is responsible under Schedule 2.
- **So where might individuals choose to exercise this cause of action?** Acknowledging that this involves some crystal ball gazing, we have come up with the following scenarios:
  - **Employer vicarious liability for employee conduct.** Many data breaches are unlikely to meet the threshold – both in terms of "misuse of information" and in relation to intention/recklessness. However, it is possible that an employee may recklessly publish their organisation's confidential or private data, such as a customer list or information about other staff's salaries. In such circumstances, an employer may find itself liable for its employee's actions if it can be established that the conduct occurred in the course of the employee performing their ordinary duties – particularly if the employer had not taken reasonable measures to prevent this.
  - **Decisions by companies to use information or surveil users in a way that goes against advice and/or where they are aware of the risks.** As above, the threshold of intentionality may make these claims difficult, but we think there is scope for the tort to be "triggered" in scenarios where an organisation acts against advice or where they are aware of the risk. For example, if leadership is aware of the known security risks of a particular legacy system and choose to continuing using it, there is an argument that they are "reckless" in their storage of such data on that system.
  - Equally, we have seen in the UK[6] that Google's ability to bypass its users' privacy settings to install third-party cookies on their devices could constitute a misuse of personal information in certain circumstances. If other elements could also be established (particularly intention and seriousness), this kind of activity could potentially be actionable under the Australian tort.
  - **New and emerging media**. Even though there is a far-reaching exemption for journalists and their handling of "journalistic material" (see Section 15), it will not apply in certain circumstances, including where the person publishing the content is not a professional journalist and/or where they are publishing material that does not – among other things – have the character of news, current affairs or a documentary. Not all content will fall within the exemption, especially if it is published by nontraditional sources (e.g. a creator on social media) and/or does not constitute "news" in the traditional sense (e.g. gossip about a public figure). In terms of corporate responsibility, it is interesting to consider whether a social media platform's failure to take down content after repeated requests to do so could help to establish that that entity is being reckless about a potential intrusion of privacy taking place on their platform.

What You Need To Do

While we wait with bated breath for judicial interpretation of Schedule 2, we recommend that businesses do the following now:

- Review your employee privacy/security training and ensure least privilege access to confidential and private data. This means ensuring that staff, systems and vendors are granted the minimum level of access necessary to perform their function.
- Update staff policies, especially around workplace surveillance. In particular, ensure your workplace surveillance policy clearly and accurately notifies staff of the surveillance that is conducted in practice, to limit any argument that a staff member had a reasonable expectation of privacy.
- Train relevant staff on the new tort and steps that must be taken to ensure that circumstances giving rise to the cause of action do not arise. This may include reframing takedown and complaint processes to take alleged invasions of privacy into account.

[4] [2021] EWHC 2168 (QB)

[5] *Ambrosiadou v Coward* [2011] EWCA Civ 409 at Paragraph 30.

[6] *Vidal-Hall and others v Google Inc* [2014] EWHC 13 (QB).

- Ensure senior management, board members and other stakeholders are aware of the changes and the obligations and implications arising as a result of this new tort.
- Be prepared with draft skeleton submissions "on ice" in case an action is brought. We note that the Act permits injunctions to be granted restraining invasions of privacy – applications for injunctions move quickly and require material to be prepared rapidly. Applications can also be made for the summary dismissal of actions without merit.
- Implement the usual measures for potential claims and litigation, such as seeking legal advice and assistance early, taking care with internal communications (ensuring they are protected by legal professional privilege as far as possible), and creating and maintaining well organised records so relevant information and documents can be accessed quickly and efficiently if required.
- Remain vigilant as to any further privacy law reforms, including any changes to the employee records exemption.
- Establish relationships with external legal counsel in advance so that help is on hand if you need it.

Contacts

Tanvi Mehta Krensel
Partner, Sydney
T +61 2 8248 7810
E tanvi.mehtakrensel@squirepb.com

Angela Radich
Director, Sydney
T +61 2 8248 7874
E angela.radich@squirepb.com

Elisa Blakers
Senior Associate, Sydney
T +61 2 8248 7840
E elisa.blakers@squirepb.com