



Untju Alkata 2 by Tommy Watson

THE REVIEW

CLASS ACTIONS IN AUSTRALIA
2024/2025

KING&WOOD
MALLESONS
金杜律师事务所

NEW AVENUES, NEW EXPOSURES: THE EVOLUTION OF PRIVACY CLASS ACTIONS

Representative proceedings for alleged interferences with privacy (**Privacy Class Actions**) have recently emerged as an opportunity for class action proponents, particularly following high-profile cyber incidents (eg *Optus* and *Medibank*). They are attractive to plaintiff law firms and litigation funders given: large class sizes (often in the millions), easily identified group members (identified through the respondents' mandatory notification obligations), and elevated public awareness making it easier to register large numbers of individuals.

Until legislative amendments introduced in the review period, there was no clear direct cause of action for breaches of privacy. To date, groups of impacted individuals have typically sought relief using the 'representative complaint' mechanism under the Privacy Act which allows for group compensation claims to be made directly to (and determined by) the OAIC for breaches of the Australian Privacy Principles (**APPs**). In some cases, different firms have filed a class action proceeding with the Court and a representative complaint with the OAIC on behalf of the same class in respect of the same data breach.

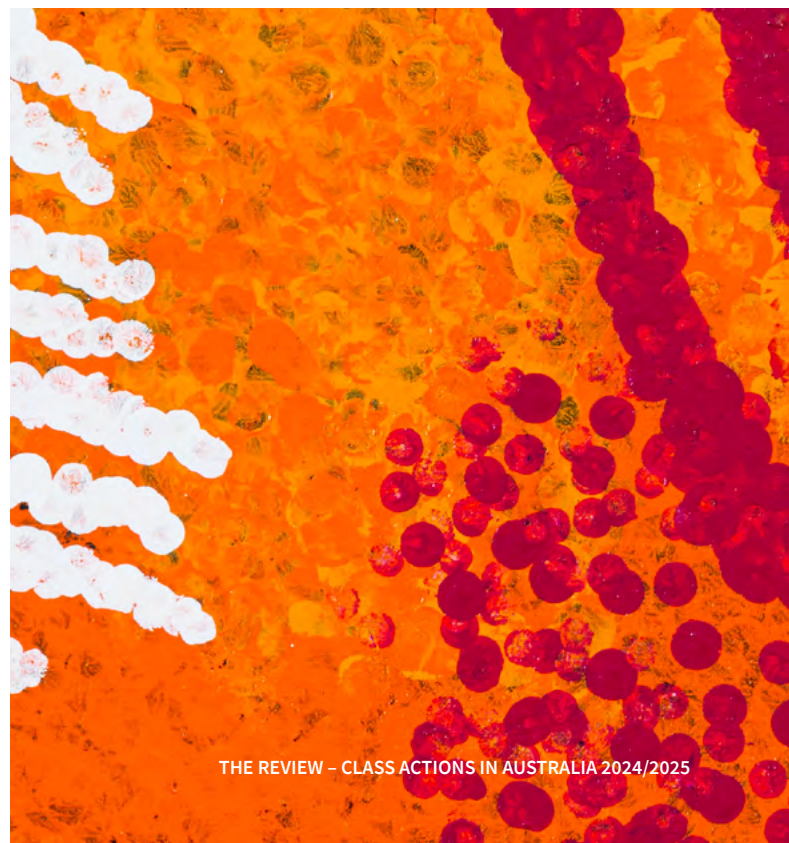
The appetite and urgency for a remedy accessible by consumers is underscored by the OAIC's latest statistics. In 2024, a record 1,113 data breaches were reported, representing a 25% increase from 893 notifications in 2023. Malicious and criminal attacks remain the main source of breaches, accounting for 69% of notifications in the second half of the year, with 61% of those being cyber security incidents. Health service providers and the Australian Government were the most affected sectors, together accounting for 37% of all breaches. The OAIC's report highlights the increasing risks to Australians' privacy and the need for organisations and agencies to step up privacy and security measures, as well as to ensure timely breach notifications.

Recent reforms to the Privacy Act have potentially shifted the landscape by introducing both:

- a **direct cause of action** for breach of privacy (the new statutory tort for serious invasions of privacy), and
- an avenue for **individuals to claim compensation from the Court** where the Australian Information Commissioner (**AIC**) is seeking a civil penalty against the entity for breach of the APPs (the new s80UA).

While the impact of these reforms is uncertain, we take a look at the possible future implications for Privacy Class Actions — and in particular, the following key questions facing applicants:

- **Federal Court v the OAIC:** which will emerge as the forum of choice?
- **Statutory tort v s80UA:** which avenue to compensation will prove more fruitful?



EXISTING LANDSCAPE

Historically, claimants faced a choice between 2 forums.

01

CLASS ACTION PROCEEDINGS IN COURT

No right to sue for breach of APPs, or any other direct cause of action

'Roundabout' causes of action instead: breach of contract, misleading and deceptive conduct, breach of confidence, negligence

Uncertain entitlement to damages for non-economic loss

02

REPRESENTATIVE COMPLAINT TO THE OAIC

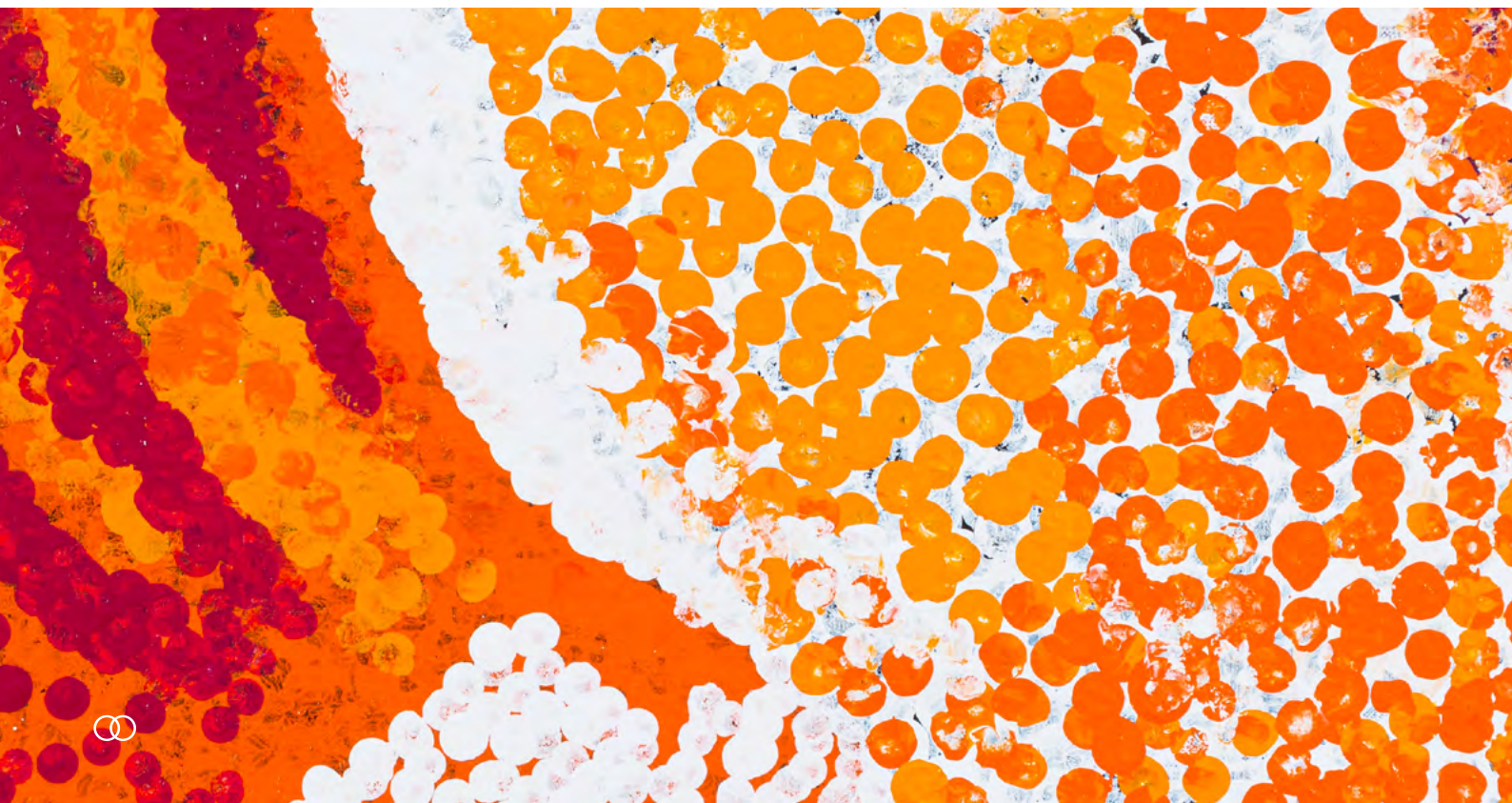
Only question on liability is breach of the APPs

Statutory ability to award compensation for non-economic loss, including for injury to feelings and humiliation

OAIC determination is not binding and requires a fresh hearing (*de novo*) in the Federal Court to enforce

Uncertain entitlement to legal costs for law firms/funders

In both the *Medibank* and *Optus* examples, the respondents are presently facing class actions in the Federal Court *and* a representative complaint before the OAIC, in addition to civil penalty proceedings brought by the OAIC (and, in the case of *Optus*, the Australian Communications and Media Authority (**ACMA**)).



THE PRIVACY ACT REFORMS

Passed on 29 November 2024 (and effective from 10 June 2025), the *Privacy and Other Legislation Amendment Act 2024* (Cth) introduced 2 important reforms:

STATUTORY TORT (SCH 2)	SECTION 80UA
<p>Under the direct right of action, plaintiffs must prove:</p> <ul style="list-style-type: none"> • a serious invasion of privacy by intrusion upon seclusion or misuse of personal information • a reasonable expectation of privacy in the circumstances • the invasion was intentional or reckless • the invasion was serious, and • the public interest in protecting privacy outweighs any countervailing interest (eg freedom of expression). <p>Proof of actual damage is not required, but harm may be relevant to ‘seriousness’ and remedies.</p> <p>Remedies include damages (including emotional distress), injunctions, apologies, and others.</p> <p>Exemptions apply to journalists and others (including intelligence and law enforcement).</p>	<p>In a civil penalty proceeding commenced by the AIC, the Court can now make orders:</p> <ul style="list-style-type: none"> • that the respondent pay compensation to individuals for loss or damage suffered, or likely to be suffered, because of the contravention, and • requiring remedial action or changes to practices. <p>An application for compensation under s80UA can be made by the Commissioner, <i>or an affected individual</i>.</p> <p>An order can be made if the Court <i>has, or will</i>, determine that an entity has contravened a civil penalty provision.</p>

STRATEGIC IMPLICATIONS FOR CLASS ACTION RISK

The reforms made no change to the representative complaint mechanism, which remains available as a pathway for groups of individuals to seek compensation for breaches of the APPs.

The limitations of the pre-existing representative complaint mechanism (opaque processes, non-binding determinations, and lack of clear mechanism to achieve returns on investment) mean that the statutory tort may be preferred where the defendant’s conduct meets the test – but the requirements that the interference be ‘serious’ and result from intentional or reckless conduct by the defendant may limit its viability, particularly in cyber breach cases. It is likely that applicants will continue to plead other causes of action (breaches of contract and confidence, misleading or deceptive conduct, negligence) at least until there is clear authority on the scope of the tort.

The availability of relief under s80UA depends entirely on the AIC seeking a civil penalty (and whether the AIC also applies for compensation orders under s80UA itself, as in *Optus*). For defendants, the new provision may make settling civil penalty proceedings with the AIC more complex, as any admissions leading to the imposition of a civil penalty can be relied upon directly by claimants to enliven compensation claims (including for non-economic loss).

When multiple pathways run in parallel – individual OAIC complaints, representative complaints, class actions under the statutory tort, and OAIC civil penalty proceedings – the interaction between them can create procedural complexity that may affect available remedies, timing, exposure for defendants and *res judicata* considerations. Different limitation periods, evidentiary rules, and liability thresholds apply across the different forums. In this regard, see the [Competing systems of redress](#) section of The Review.

A stark example of this complexity is *Optus*. As a result of the 2022 data breach, Optus is now subject to:

- 3 consumer claims, comprising 2 representative complaints before the OAIC lodged by Johnson Winter Slattery (October 2022) and Maurice Blackburn (April 2023) for breach of the APPs, and a class action in the Federal Court filed by Slater and Gordon (April 2023) claiming, among other things, negligence and breach of contract, and
- 2 civil penalty proceedings filed by the ACMA (in May 2024) and the AIC (in August 2025) for interferences with privacy. The AIC's claim also includes a claim for consumer compensation under the new s80UA (an avenue not available to the class action claimants at the time of filing).

The Court is now considering the most appropriate way to manage the overlapping allegations, claims and group members across all proceedings involving multiple forums, regulators and causes of action.

CASE STUDY & UPDATE

Background: In March 2020, the OAIC commenced civil penalty proceedings in the Federal Court (NSD 246/2020) over the Cambridge Analytica matter (where Facebook users' information was disclosed to third parties and risked being used for political profiling purposes), alleging serious or repeated interferences with privacy (s13G) affecting an estimated 311,127 Australian users.

Outcome: On 17 December 2024, the OAIC accepted an enforceable undertaking from Meta under s114 of the *Regulatory Powers (Standard Provisions) Act 2014*, establishing a \$50m payment program for eligible users. The OAIC discontinued the civil penalty proceedings — and the undertaking was accepted on a no-admissions basis and includes independent administration of the scheme.

Why it's interesting: Resolving the Federal Court proceeding via an enforceable undertaking delivered a compensation pathway without declarations of contravening conduct or the imposition of a civil penalty.

Practice point: For organisations facing overlapping enforcement and litigation risk, early, coordinated engagement with the OAIC can streamline resolution and minimise duplicative proceedings — especially where forward-looking remediation and a pragmatic compensation mechanism can be agreed with the OAIC. A resolution of this kind is likely to be attractive for defendants, particularly now given the risk of a compensation order under s80UA in a civil penalty proceeding — but may be very difficult to achieve now that the regulator has a statutory pathway to achieve both a penalty and compensation.

King & Wood Mallesons acted for Meta Platforms, Inc.



ABOUT KING & WOOD MALLESONS

A firm born in Asia, underpinned by world class capability. With over 3,700 lawyers in 26 global locations, we draw from our Eastern and Western perspectives to deliver incisive counsel.

We help our clients manage their risk and enable their growth. Our full-service offering combines un-matched top tier local capability complemented with an international platform. We work with our clients to cut through the cultural, regulatory and technical barriers and get deals done in new markets.



JOIN THE CONVERSATION



SUBSCRIBE TO OUR WECHAT COMMUNITY.
SEARCH: KWM_CHINA

Disclaimer

This publication provides information on and material containing matters of interest produced by King & Wood Mallesons. The material in this publication is provided only for your information and does not constitute legal or other advice on any specific matter. Readers should seek specific legal advice from KWM legal professionals before acting on the information contained in this publication.

Asia Pacific | North America

King & Wood Mallesons refers to the network of firms which are members of the King & Wood Mallesons network. See kwm.com for more information.

www.kwm.com

© 2025 King & Wood Mallesons