

OAIC PIXEL TRACKING DECISIONS (Medmate and Monash IVF)

A PRACTICAL GUIDE - HOW THESE DECISIONS AFFECT DIGITAL ADVERTISING

The Decisions

Why these decisions matter

If you deploy pixels or conversion tracking snippets on your website or app, these rulings are about you. They may be tested further in the courts, but they show the OAIC's current interpretation of the Privacy Act.

It is clear that the OAIC will treat as PI any data that enables a business to 'single out' or distinguish an individual from others in a way that affects their rights and interests, even when the business cannot identify that individual.

The OAIC decided that using pixels to re-target ads to an individual on another platform, based on their website behaviour, was enough to meet this threshold, even when the business doing the re-targeting has no idea who the person is in the physical world.

The OAIC made it clear that the website operator who deploys the pixel ultimately bears responsibility for 'collecting' personal information through pixel tracking technologies (even when the data is stored only by the pixel provider).

Explainer: what did Medmate and Monash IVF do with the data?

Medmate's pixels transmitted to third party platforms the page URLs that revealed the conditions and medicines that patients were viewing. Monash IVF sent tracking pixels to third party platforms to build advertising audiences covering visitors to fertility, egg-freezing and appointment-booking pages.

	Medmate	Monash IVF
Categories of data collected by the pixel	• Page view information • Purchase information – when an individual completes a purchase (e.g. order ID, value) • Content views – when an individual views content or a specific product	• Page view information • Lead phone clicks/contact – track phone calls • Lead form submissions – track successful form submissions • Lead book appointment – track appointment bookings

What did the OAIC say?

The OAIC made determinations that Medmate (an online pharmacy and telehealth service) and Monash IVF interfered with patient privacy by using third-party tracking pixels to collect sensitive health information and disclose it to advertising platforms without consent.

Both providers were ordered to stop the non-compliant collection, destroy or de-identify the affected data where lawful, and put valid consent and notice in place before resuming.

The decisions are about sensitive information but the implications go much further – data collected by tracking technologies may be personal information and website operators will generally be liable for tracking technologies deployed on their websites.

Explainer: what are tracking pixels?

A tracking pixel is a small piece of code, generated by a third party, that an organisation embeds in its website. When a person loads a page, the pixel fires and sends data about that visit back to the third party's servers, often to build advertising audiences and measure ad performance.

What failures did the OAIC identify?

	What the Australian Privacy Principles require	The tracking pixel failure
APP 3.3	Sensitive information, including health information, may only be collected with the individual's consent and where reasonably necessary	Pixels collected patients' health information through their page visits, without valid consent
APP 5	Notify individuals about the collection of their personal information at or before the time it happens	Patients were not told that pixels were collecting their data and sending it to third parties
APP 7	Do not use or disclose personal information for direct marketing without a valid basis	Sensitive health data was disclosed to advertising platforms to target marketing

Four findings are particularly significant for IAB members

1

Data collected through a tracking pixel will typically be 'personal information' - 'singling out' is enough and identity is not required

The Commissioner confirmed that the definition of 'reasonably identifiable' in the Privacy Act now extends to situations where data permits a business to 'single out' or 'distinguish' an individual from others in a way that affects their rights or interests — even where that individual's name or other direct identifiers are never known ('individuation').

Critically, the Commissioner held that retargeting ads to an individual on the pixel providers' platforms, based on their website behaviour, is itself sufficient to meet this threshold.

What this means practically: if your website or app uses pixels to track individuals' online behaviour, you may be 'collecting' personal information under the Privacy Act. If so, the APPs apply.

Businesses should assess whether the information they hold 'reasonably identifies' an individual by looking at the inferences which they make using such information and how those inferences impact the individual (as well as looking at well established factors, such as the possibility of identification).

2

New technologies are expressly caught

The Commissioner was explicit that this is a deliberate evolution of the OAIC's interpretation of the law. She acknowledged the interpretation of 'reasonably identifiable' is 'novel' in the context of advanced tracking technologies, while emphasising that it is a logical progression of the Privacy Act's principles based, technology neutral framework.

"I observe that new technologies provide entities with new ways to affect the privacy of individuals by collecting, using and disclosing a range of types of information. Many of those types of information may historically not have been considered personal information, such as technical identifiers, social media handles, email addresses, or physical characteristics. However, as technology has evolved to make it possible for entities to use such information to track and target individuals, both in online and offline environments, our understanding of 'identifiability' has evolved in parallel."

— Privacy Commissioner Carly Kind, Monash IVF [71]

This is consistent with the OAIC's revised APP 3 guidance, which similarly broadens the circumstances in which organisations should treat data as personal information. The Commissioner argues in the Monash and Medimate decisions that she is extending the application of the existing law to changing technologies.

What this means practically: technical identifiers, behavioural signals, device fingerprints, hashed emails and social media handles used for targeting are all now within the definition of personal information where they enable individuation.

Any argument that *'we only see aggregated or anonymised data'* needs to be re-examined against this standard.

3

Responsibility sits with the website operator who deployed the pixel

The Commissioner rejected the Medmate and Monash arguments that they were not the 'collector' of the data because it sat on the pixel providers' servers. The analysis turned on control, not custody:

- The collection would not have occurred if Medmate/Monash had not actively commissioned the tracking pixels.
- Medmate/Monash exercised control over the deployment and configuration of those pixels.
- Medmate/Monash could adjust the parameters of information collected after initial setup.
- Medmate/Monash instructed and paid pixel providers for advertising services and directed retargeting based on parameters it set.

The fact that Medmate/Monash outsourced day-to-day campaign management to external marketing agencies made no difference. Nor did the fact that neither website operator held the data. The responsibility sat with the website operators as the entities that chose to embed the pixels.

These decisions did not address the liability of agencies or platforms in detail, so you should not assume that these entities are relieved of responsibility more generally. The OAIC may find multiple liability – in its recent guidance on APP 3, the OAIC clarified that two entities may collect personal information at the same time.

What this means practically: if a pixel is on your website, you own the compliance obligation — regardless of who set it up, who manages the campaign, or on whose servers the data lands.

'Our agency handles that' and 'the pixel provider controls the data' are not defences for a website operator.

4

The OAIC may now take a stricter stance on 'notification'

The OAIC found that neither Medmate nor Monash took reasonable steps to notify individuals of their use of pixels, as required under APP 5.2.

Both policies stated that personal information could be used for direct marketing, but not in a way that recognised the reality of pixel based ad tracking.

The OAIC suggests that organisations should use a point in time notification, such as a banner or pop-up in relation to the use of tracking pixels. It is not clear whether a more comprehensive privacy policy – without point in time notifications – would have been adequate.

What this means practically: general references in a privacy policy to 'direct marketing' will not be sufficient notification of the use of pixel tracking. Privacy policies should be reviewed to include further detail on how pixels are used and where the data will go.

It is currently unclear whether the OAIC will require point in time notifications – such as banners or pop-ups – in addition to privacy policy disclosures.

Practical steps — what organisations should do now

The following steps are drawn from the OAIC's accompanying guidance published 24 June 2026 - [here](#). They apply to any organisation that deploys tracking pixels or similar technologies on a website that handles personal or sensitive information.

1. Know what tracking technologies are in place and where

Do not assume you know. The OAIC found organisations using pixels they had forgotten about or that third-party vendors had installed.

Organisations must understand their data flows and identify which tracking pixels are in use:

- Conduct an audit of your website. Free tools such as Blacklight (The Markup), Brave, Ghostery and Chrome DevTools can identify trackers on websites.
- Document every tracking technology in use: what data it collects, where that data is sent, and who controls the configuration.
- Conduct regular, ongoing reviews — tracking pixels are not a 'set and forget' tool.
- If you use external marketing agencies or website developers, contractually require disclosure of any tracking technologies they deploy.

2. Assess the sensitivity of data (actual and inferred) and configure pixels appropriately

Tracking pixels will typically share information about your website visitors and what they did on the website. Consider who may visit your website and what inferences can be drawn from their browsing activity.

Browsing data may be personal and sensitive information. Every page view potentially reveals or infers information about an individual. If a user visits a page about anxiety, STIs or fertility treatment, it is likely they have a personal health interest.

Tracking pixels should be configured to limit the collection of personal information to the minimum amount reasonably necessary and to avoid the disclosure of sensitive information to social media platforms.

Check whether 'advanced matching' is enabled on any pixel. This is a feature that can enhance a pixel by securely sending user identifiers (e.g. hashed email addresses) so ad platforms can more accurately match website conversions to users. Its use will increase the likelihood that an individual is 'reasonably identifiable'. Sensitive information should only be collected via a tracking pixel with an individual's express consent.

3. Ensure transparency and valid consent mechanisms are in place

Organisations must ensure that their privacy policy and collection notices contain clear and transparent information about the use of tracking pixels.

The OAIC's guidance note says that:

When using tracking pixels to target individuals with online advertising on social media platforms, organisations must provide individuals with a simple way to opt-out. For example, an organisation could deploy a banner or pop-up when a user first visits a website which provides notice of the use of third party tracking pixels for marketing or advertising purposes and allows the user to opt-out.

4. Implement a privacy by design approach

The Privacy Act does not prohibit the use of tracking pixels, but it requires organisations to use them responsibly.

For organisations that handle sensitive information or serve vulnerable communities, the OAIC goes further and recommends reconsidering the use of tracking tools altogether.

Bottom line

These findings produce an expanded compliance perimeter for any organisation involved in digital advertising:

- the personal information threshold may be lower than you have previously assumed, due to the concept of 'individuation';
- the technologies by which 'collection' can take place are constantly evolving and now include pixel tracking technologies;
- responsibility sits with the website operator who deploys the pixel, even where they do not execute it or store the data;

-
- notification of pixel tracking to consumers must be specific and may need to be a point in time notification.
-

This document is prepared by IAB Australia for members' information. It does not constitute legal advice.