Australia's Blueprint for Privacy Reforms – What it Means for Media

Authors: Tim Brookes, Geoff McGrath, Rebecca Cope and **Andrew Hilton** (Ashurst), and **Leon Franklin** and **Michael Turner** (Ashurst Risk Advisory) explore the Government's ambitious privacy reform agenda.[1]

Introduction

The Australian Government has released its eagerly anticipated Response to the Privacy Act Review Report, looking to make Australia's privacy laws fit for purpose in the digital age. Media and communications are in the front line of many coming reforms, acknowledging the sector's central role in the information age. The Government has agreed or agreed in-principle with the vast majority of the Privacy Act Review Report's 116 recommendations. However, there is still significant scope for interested parties to help shape and refine the reform proposals. Be prepared for quick and targeted consultation – legislation is expected to be introduced in 2024.

In this article, we dive into these reforms and more, exploring:

- highlights for the media and communications sector;
- practical steps you need to take now to prepare for coming reforms (and why) (Part 1); and
- some key reforms that will transform Australia's digital landscape – highlighting some key issues for media and communications sector (Part 2).

Highlights for the media and communications sector

Media and communications organisations will need to manage targeted sector-specific reforms as well as wide ranging whole-of-economy reforms. These reforms arise in the context of a clear international trend to place greater responsibility on businesses to protect the safety and privacy of individuals.

This means more than updating policies – work needs to begin now to plan and build the systems and capabilities to thrive in a more transparent, more user-centric, and more tightly regulated data economy. Key takeaways for the media and communications sector include:

- **Journalism exemption –** The Government has indicated its agreement to keep the exemption for media organisations acting "in the course of journalism" but is proposing to require media organisations' compliance with "adequate" media privacy standards, as well as data security, data destruction and data breach notification requirements. Should this proposal come to fruition, media organisations will need to plan for standards compliance (in particular, complaints handling) and focus on managing all their data (including data covered by the journalism exemption).
- **New rights of action –** The Government has indicated its agreement to create a new direct right of action for Privacy Act breaches, and the long-awaited statutory tort for serious invasions of privacy – which may give rise to new avenues for individuals to object to uses of their personal information, and in the context of the statutory tort, extending to media organisations even where they are acting in the course of journalism (subject to further targeted consultation).
- **Data retention laws –** As part of proposed reviews of data retention obligations, the telecommunications sector in particular can help the Government look at mandatory data retention obligations through a more cyber- and privacy-informed lens, where the question is not "how can the data be retained", but rather "should the data be retained". However, coming reviews will not duplicate the Government's separate independent review of the *Telecommunications (Interception and Access) Act 1979* (Cth).
- **Engagement with reforms** – The Government is looking to industry to help shape future reforms – with a busy reform agenda, be prepared to engage strategically on key issues.

Part 1: Practical steps to take today

The first step is to baseline today's organisational capabilities. This means asking the right questions to identify gaps and capability uplift opportunities, and to understand which of those capabilities matter the most.

There are five critical questions you should be asking today.

1. Is your governance framework up to the challenge?

Hallmarks of an adequate framework include clearly delineated risk management roles and responsibilities, accurate privacy risk reporting and escalation, clear and actionable internal policies to guide operational staff, as well as compulsory and impactful privacy training.

This must be a collaborative effort, for example using cross-collaboration forums and dedicated Management Committees - particularly ones involving cross-disciplinary stakeholders (including an organisation's Chief Information Security Officer, Chief Risk Officer, General Counsel, and Head of Privacy).

2. Is risk assessment built in?

Designate specific milestones or points within the project management lifecycle for assessing risk and integrating Privacy by Design advice – do not assume it will just happen. This ensures that privacy is a core aspect of project development and execution and reduces the risk of costly remediation.

Apply this approach consistently in areas such as Privacy Impact Assessment, Cyber Security, and Third-Party Risk Assessment, ensuring a comprehensive and integrated risk management strategy across all organisational projects and initiatives.

1 This publication is a joint publication from Ashurst Australia and Ashurst Risk Advisory Pty Ltd, which are part of the Ashurst Group. Some members of the Ashurst group (including Ashurst Risk Advisory Pty Ltd) do not provide legal services.

3. Do you have visibility across your data estate?

Make sure you have a centralised view of the location, volume, and types of personal information held. This needs to provide visibility of how data is managed across its entire lifecycle from the point of collection or generation through to deletion, enabling you to identify and remediate current risks and track changes in risk over time.

Without visibility of your data estate, it is impossible to govern your data effectively.

4. Are you prepared for a data breach?

Key to data breach preparation is codifying clear roles and responsibilities within a comprehensive data breach response plan. The plan should detail processes for each stage of breach response, including detection and identification, containment, recovery, notification, as well as review and improvement stages.

Practising response processes in simulated crisis scenarios for leadership teams and boards is another critical, yet often overlooked, part of data breach response preparation.

5. Do you understand your automated decision-making?

Knowing how and where automated decision-making is used (and keeping this information current) will be a new challenge for many organisations, so this requires strong organisational transparency and traceability in data flows and business processes.

It will be impossible to explain automated decision-making to a customer or regulator unless you have detailed and current knowledge about your data and business operations – adopting a risk-based approach to identifying the areas that matter most.

Part 2: A deep dive into the reforms

Few of the 116 proposals in the Privacy Act Review Report are "off the table." The Government has:

- **Agreed 38 proposals –** including important changes to make regulatory investigation and enforcement simpler, and to bring transparency to automated decision-making. These changes are likely to become law faster and potentially with limited or no transition periods – and more limited "targeted" stakeholder consultation.
- **Agreed in-principle 68 proposals –** the bulk of the proposals, which will require further stakeholder consultation and impact analysis, including in the development of guidance and transition periods.
- **Noted (and did not agree) 10 proposals –** some of these may be addressed by other means. For example, we may see targeted codes or standards implemented faster than broader economy-wide law reforms.

Language used in the Government response often differs from the original Privacy Act Review Report. In some cases, this might be simply to make the response easier to read. However, differences may signal how the Government will take proposals forward, explaining why so many proposals are "agreed in-principle" (rather than "agreed").

Agreed in-principle: Direct right of action and statutory tort

A direct right of action for breaches of the Privacy Act, and a statutory tort for serious invasions of privacy (which is broader than the protections under the Act) are likely to significantly expand liability exposure especially from data breaches and increase the risk of class action suits. The direct right of action could result in any order the court sees fit, including any amount of damages (potentially beyond the maximum penalties under the Privacy Act).

A statutory privacy tort applying outside the Privacy Act would be more accessible than existing causes of action such as breach of confidence or defamation, particularly when claimants are able to take advantage of the new individual rights discussed below. It may also open up an avenue for claims against organisations or individuals who are not otherwise bound by the Privacy Act – or for activities covered by exemptions, such as the journalism exemption.

The Government will need to balance the public interest in privacy with the public interest in a free press in the development of a statutory tort. Media organisations have expressed concerns that the new tort will have a "chilling effect" on public interest journalism. In response, the Government has flagged that it will consult with the media industry before implementing the new tort. Consultations are expected in the course of 2024, alongside other targeted consultations.

Generally agreed: Retain the journalism exemption, with increased oversight and data security obligations

The Government has agreed to keep the current exemption that applies to media organisations acting "in the course of journalism" – but only where organisations follow an adequate media privacy standard. The Government has also agreed in-principle that data security, data destruction and data breach notification obligations will apply to media organisations, including where the journalism exemption would otherwise apply.

To take advantage of the journalism exemption, media organisations will need to follow privacy standards overseen by the Australian Communications and Media Authority (**ACMA**), Australian Press Council (**APC**) or Independent Media Council (**IMC**)), or standards that otherwise "adequately" deal with privacy. While this largely reflects the current regime, the new element to this requirement is that the OAIC will develop criteria, in consultation with industry, to determine what is "adequate" and publish a template media privacy standard. How complaints are handled is likely to be a key part of what is considered "adequate".

This oversight on privacy standards will preserve current sector-based oversight (by the ACMA, APC and IMC) and provide a lever to extend oversight into less regulated areas (such as online content).

While media organisations can still use their own privacy standards, the OAIC's criteria on what is "adequate", and its template privacy standard, will set important baselines. Early engagement in consultations is vital, including for organisations that do not align with the ACMA, APC or IMC requirements, and do not intend to use the OAIC template.

The Privacy Act Review Report did not recommend applying a "public interest" test to the journalism exemption, noting challenges and uncertainty in deciding what is public interest journalism. However, developing criteria to determine an "adequate" privacy standard and a template standard could have a very real impact on how journalism is conducted.

In addition, the Government has said it will consider further how to support smaller news media engaged in public interest journalism, suggesting that at least for smaller media organisations we may still see a distinction drawn, or further protections being provided.

The Government agreed in-principle to limit the journalism exemption so that that media organisations will be required to keep personal information secure, to destroy it when it is no longer needed and to report eligible data breaches to the OAIC (within new, tighter timeframes – see more below).

This will add a layer of complexity to data management and liability for media organisations. They will need to tread a fine line between having sufficient oversight of a journalist's data to be able to ensure that the security, destruction, and data breach notification obligations are able to be met, while preserving the integrity and confidentiality of journalism activities.

The Government has agreed in-principle that media organisations will not need to notify individuals of a data breach where the public interest in journalism outweighs the interests of individuals being notified. Media organisations will need governance in place to be able to make this assessment under pressure, and in short timeframes.

Agreed in-principle: Notifiable Data Breaches

The Government has agreed in-principle to tighten timeframes for data breach notifications, and to apply the regime to media organisations engaged in journalism.

Currently, an organisation must notify the OAIC as soon as practicable after it becomes aware that there are reasonable grounds to believe an eligible data breach has occurred. The Government has agreed in-principle that notification should happen within 72 hours at the latest, with the ability to notify further information progressively as details emerge, aligned to cyber incident notifications for critical infrastructure.

Organisations must also notify affected individuals as soon as practicable. Again, the Government has agreed in-principle that organisations can notify information progressively. This may in practice mean organisations will be under pressure to give more limited notifications earlier, before full details are understood.

A tighter focus on reporting timeframes may increase the risk of adverse public relations and customer outcomes for entities in having to publicly disclose data breaches before they have been fully investigated. As recent incidents have demonstrated, knowing a data breach has occurred can be very different from understanding exactly what data or individuals are impacted, to what degree, and what should be done in response.

Agreed in-principle: Review of data retention laws

The Government has agreed in-principle to review laws that require retention of personal information – this is in addition to commitments made in the National Strategy for Identity Resilience, and the recently released 2023-2030 Cyber Security Strategy.

The telecommunications sector in particular can help the Government look at mandatory data retention obligations through a more cyber- and privacy-informed lens where the question is not "how can the data be retained", but rather "should the data be retained". However, this review is not intended to overlap with the Government's separate independent review of the *Telecommunications (Interception and Access) Act 1979* (Cth).

Agreed: Regulatory flexibility, enforcement, and penalties

The Government has agreed to give the regulator more flexibility and a stronger regulatory toolkit – likely to drive more investigation and enforcement action. As last year's reforms demonstrated, changes to regulatory and enforcement powers can happen quickly, without further consultation or transition periods.

The expanded regulatory toolkit includes a binding codes and standards framework similar to those of the eSafety Commissioner, broader powers around emergency declarations, broader investigative powers, the ability to conduct public inquiries and reviews, and broader information sharing powers following data breaches.

A promised strategic review may bring new resourcing, an industry funding model, contingency funds for litigation costs orders and an enforcement special account to fund high-cost litigation. Organisations will be under pressure to demonstrate compliance with existing obligations while building capacity to comply with new obligations in the pipeline.

The Government has also agreed broader consequences for non-compliance – including:

- **Penalties:** clarifying how last year's massive new penalties for serious interferences with privacy will apply, and introducing mid and lower tier penalties for less serious or administrative non-compliances.
- **Broad new orders and declarations:** allowing courts to make any order they see fit once a civil penalty for interference with privacy is established, and for the OAIC to direct entities to identify, mitigate and redress actual or foreseeable loss or damage.

We may see an increase in very high value penalties, as well as more capability to pursue a broader range of smaller targets. The OAIC has been challenged recently in Senate budget estimates on whether it will pursue penalties for data breaches and has recently brought action in the Federal Court seeking penalties against a healthcare provider as a result of a data breach. We may also see civil penalties used to drive compliance with the OAIC's investigation and information gathering activities.

Agreed: Automated decision-making

The Government has agreed to all proposals on substantially automated decision-making, sending an extremely strong signal that the issue is high on the legislative agenda, and that legislation is likely to closely reflect the Privacy Act Review Report positions.

Although automated decision-making is often discussed alongside artificial intelligence, they are not the same: automated decision-making can include business rules or processes used to make decisions, as well as more complex artificial intelligence models.

The reforms will require **transparency** about personal information used in automated decision-making, and **meaningful explanations** of automated decisions.

The reforms apply to decisions that both:

- are **substantially automated** (framed this way to prevent entities using a negligible human approval or "rubber-stamp" to avoid the requirements); and
- have a **legal or similarly significant effect** on an individual's rights.

The Government has said this "legal or similarly significant effect" could cover or access to basic necessities such as food and water, or denial of consequential services or

support, such as financial and lending services, insurance, employment opportunities and health care services. However, in Europe, decisions in ride-sharing apps have been found to meet this threshold – including assigning rides; calculating prices; rating drivers; and calculating fraud probability scores.

The Government has also clarified that information provided to individuals should not reveal commercially sensitive information – a key concern under Europe's current automated decision-making transparency rules and more extensive proposals for the regulation of artificial intelligence.

A broad range of other proposals will impact automated decision making, from changes around permitted uses of information, to more granular consents, to new requirements for privacy impact assessments for high-risk activities.

Agreed in-principle: Fair and reasonable – a new keystone of the Australian privacy framework

In welcoming the Privacy Act Review Report, the OAIC pointed to the new "fair and reasonable" requirement as shifting the burden of safeguarding privacy from individuals to organisations, describing it as a "new keystone of the Australian privacy framework".

The proposal will require any collection, use and disclosure of information to be fair and reasonable in the circumstances – even where an organisation has obtained consent.

The Government has described the test in terms of a balancing act – making sure impacts on individuals and the public interest in protecting privacy are considered alongside an organisation's interest in carrying out its activities or functions. This balancing of interests is similar to the ability to use information for a "legitimate interest" under European privacy law, with the important difference that the Australian "fair and reasonable" test will apply to all handling of personal information, including with consent.

This new test will apply another overlay to existing principles-based rules and will likely add further uncertainty and complexity. Organisations will need good visibility of their data handling practices, an active assessment and review process, and transparency in policies and collection notices to have comfort that data handling practices and new innovations are not open to challenge.

New: Personal information of unknown individuals

In a key departure from the Privacy Act Review Report recommendations, the Government has flagged that it considers an individual will be reasonably identifiable where they are able to be distinguished from all others, "even if the identity of the individual is not known" – for example, tracking shopping or internet browsing by the user's IP address, mobile device or using cookies. This concept refers to the ability to single out a person even if identity details (such as their name) are not known.

The Privacy Act Review Report concluded that this information should **not** be covered by the definition of personal information, and instead limited additional protections should apply to de-identified information (a proposal that the Government noted but did not agree with).

In its response to the Privacy Act Review Report, the Government stated that information should be regulated as personal information under the Act if it (by itself, or in combination with other information):

- presents a risk of identification or re-identification that is higher than low or remote; **or**
- is sufficient to be linked to an individual (distinguishable from all others), even if their identity is not known.

This change could have significant implications for what data is regulated. Data sets used and traded by businesses and researchers might currently be de-identified to the point that there is a low or no risk of re-identification, but that data might still contain enough information to distinguish an individual from all others – there's a very real risk that this data may be covered by Privacy Act protections in the future. For the media industry in particular, this may have a significant impact on the operations of key players within the AdTech ecosystem, and in particular on how ad publishers (such as AVOD, digital platform and website operators) serve ads to their audiences.

Agreed in-principle (mainly): Direct marketing, targeting, and trading

We will likely see a much stricter regime for all these activities, ensuring the individual has some degree of control over them.

- **Targeted advertising?** While the Government "noted" (and did not agree) to an unqualified right to opt out of targeted advertising, digital businesses should not breathe a sigh of relief just yet. The Government has said that it will consider how to give individuals more choice and control – for example through layered opt-outs or industry specific codes. Targeted interventions such as industry specific codes might come into play faster than would occur for broader economy-wide law reform.
- **Opt-outs for direct marketing – but what is marketing?** The Government has agreed in-principle that individuals should have an unqualified right to opt out of direct marketing – but flagged the need to refine the definition. Changes should be harmonised with the Spam Act and Do Not Call Register Act. Organisations will not only need stronger mechanisms to track direct marketing consents and opt-outs but streamlined processes to identify which activities will be considered direct marketing, targeting, or spam.
- **Consent for data trading**: Trading includes the disclosure of personal information for a benefit, service, or advantage. This would seem to have significant scope to affect legitimate disclosures of personal information which would not fall within the normal concept of "trading".

Applying these rules to information about individuals who are not known (as discussed above) may be extremely complex – for example, managing opt-outs or consents of unknown individuals. Further consultation on exactly what each of "marketing", "targeting" and "trading" covers will help clarify who is more tightly regulated, and who is not.

Agreed in-principle: Consent, transparency and control

The Government has agreed in-principle that consent must be **voluntary, current, specific, and unambiguous** – a codification of current OAIC guidance. These requirements will have far-reaching implications in practice.

Seeking fresh consent may create customer friction and inadvertently drive away customers. The need to regularly seek fresh consents has been criticised in the context of

discussions about the Consumer Data Right, with recent amendments allowing business customers to give longer term standing consents.

As consent must be specific, it is unlikely organisations can obtain bundled consents covering broad purposes. We might also see longer and more detailed collection statements/notices, contributing to consent fatigue.

Depending on transitional arrangements, organisations might not be able to rely on consents collected in the past including implied, bundled or opt-out consents. Even if prior consents can be relied on, many organisations will find it complex or impossible to apply different sets of rules and controls to older data.

In another codification of OAIC guidance, the Government has agreed in-principle that privacy notices should be clear, up-to-date, concise, and understandable, with appropriate accessibility measures in place. Collection notices should also include specific matters (for example, if information is collected, used, or disclosed for high privacy risk activities).

Agreed in-principle: New individual rights

The Government has agreed in-principle a range of new individual rights and accompanying obligations for organisations to assist individuals to exercise their rights. These rights include:

- **Request an explanation** of information held, and what is being done with it.
- **Object** to collection, use or disclosure, and require an organisation to justify how its practices comply with the Privacy Act.
- **Right to erasure**: The Government response includes the additional possibility that data might be de-identified rather than deleted, a slightly different approach to the original Privacy Act Review Report. Organisations will also need to pass the erasure request to third parties who have received the data unless the effort to do so is disproportionate.
- **Request correction of online publications**: Expanding the existing right to correct personal information to online publications within the control of the entity.
- **Require search engines to de-index** certain online search results: an Australian-specific version of the "right to be forgotten".

These new rights will not be absolute. Instead they will be subject to exceptions, to balance the interests of individuals against those of the public, and other countervailing interests. There will also be protections against requests that are technically impossible, unreasonable, frivolous or vexatious.

Significant concerns about the potential administrative burden have not gone unnoticed. The Government has confirmed it will further consider the scope and application of these new individual rights in light of feedback about the administrative burden.

Agreed in-principle: Internal governance and accountability

Consistent with trends overseas, the Government's response signals more requirements to assess, monitor and record privacy activities and risks – looking to drive better internal governance, and require organisations to create and maintain the records the OAIC will need to investigate non-compliance. New internal accountability measures include:

- **Privacy Impact Assessments** for activities with high privacy risks: Assessing risk and impact requires better visibility of data collected, the purposes for which it is collected, what the data may be used and disclosed for, how data is actually used, as well as data governance that links these things together. This brings a requirement that already exists for Commonwealth Government agencies to private sector entities.
- **Record of purpose of collection, use and disclosure** at or before the time of collection (or for secondary purposes, before undertaking that secondary use or disclosure). The primary and secondary purposes information can be put to without consent will be significantly narrowed. The primary purpose will be the original purpose of collection from the individual (not the purpose of a later recipient) and secondary purposes must be directly related to that primary purpose.

While these changes may appear administrative, the complexity they could add to the business processes of an organisation cannot be understated. Similar requirements exist under the GDPR, which requires organisations to keep detailed records of processing activities.

A busy road ahead

The Government's response to the Privacy Act Review Report is just one part of an ambitious reform agenda aiming to make Australia's laws fit for purpose for the digital age – in addition to privacy reforms, the Government will be pushing important reforms as part of the 2023-30 Cyber Security Strategy, new Digital ID laws, a review of the Online Safety Act and the introduction of mandatory Online Safety Standards.

Key emerging themes across various reforms include:

- **Consultation, co-design, and cooperation** – the Government continually emphasises the importance of involving industry and civil society in shaping new rules. Industry is often given the opportunity to bring solutions for pressing social issues, which can result in binding or voluntary codes and standards.
- **Reliance on industry as the front-line of defence** – in an increasingly interconnected and complex digital landscape, the Government expects industry to do more to not only protect itself, but to protect individuals, supply chains and broader ecosystems. We are seeing increasing responsibilities for organisations to assess risks, interests and impacts as part of their business.
- **Heightened expectations** – Regulation and regulators expect more than ever before. While laws traditionally set minimum compliance thresholds, regulators and regulation increasingly look to drive better practices – to be deliberately disruptive to current practices.

Expect a very busy 2024 – in the privacy space and elsewhere – with the need to meet a tougher regulatory and compliance environment for existing laws, uplifts to comply with new laws, and consultations and engagement to help shape the future regulatory landscape.