

Attorney-General's Department  
4 National Circuit  
BARTON ACT 2600  
Australia



10 January 2022

By email only: [privacyactreview@ag.gov.au](mailto:privacyactreview@ag.gov.au)

Australian Payments Network (AusPayNet) welcomes the opportunity to respond to the Attorney-General's Department's review of the *Privacy Act*. AusPayNet recognises that a well-functioning digital economy requires convenient and secure payments mechanisms for individuals and organisations to build trust in the industry and supports initiatives to achieve such an outcome.

### AusPayNet Membership and Role

AusPayNet is the industry association and self-regulatory body for the Australian payments industry. We manage and develop procedures, policies and standards governing payments in Australia. Our purpose is to enable competition and innovation, promote efficiency, and control and manage risk in the Australian payments ecosystem. AusPayNet currently has over 140 members, including financial institutions, operators of Australia's payment systems, merchants, and financial technology companies.

### Introduction

AusPayNet supports the Department's objectives to better empower consumers, protect their data, best serve the Australian economy and address the *Privacy Act's* interaction with other Commonwealth regulatory frameworks. AusPayNet thanks the Department for considering its feedback<sup>1</sup> on the Issues Paper published on 30 October 2020. In this submission, AusPayNet will restate feedback that remains important and supportive of its preferred options of those the Department has proposed in the follow-up Discussion Paper published on 25 October 2021. AusPayNet will also highlight and incorporate its responses from other recent consultations which have an impact on the *Privacy Act*.

### Context: Digital Identity, Consent and Customer Experience in Payments

Since the Issues Paper and our submission, the pressing need for digital identity solutions and the sharing of personal information has been evident in various use cases involving identification, authentication and authorisation (including in payments), necessitating both a consent framework and a regulatory framework. These needs are noted on page 90 of the Treasury's final report on its Review of the Australian Payments System.<sup>2</sup> The report stated that:

---

1 Australian Payments Network Limited, Submission to the Attorney-General's Department's Review of the Privacy Act 1988 (Cth) 29 November 2020 <<https://www.ag.gov.au/sites/default/files/2021-02/auspaynet.PDF>>.

2 Commonwealth Treasury, 30 August 2021, 'Review of the Australian Payments System – Final report', Accessed 14 December 2021 <<https://treasury.gov.au/publication/p2021-198587>>

“Many aspects of the payments ecosystem are already wholly digital and there is a strengthening connection between the sharing of information and the payment of money... Currently, the Government is considering recommendations to extend the scope of the [Consumer Data Right] CDR to empower consumers to also share instructions to make payments (known as payment initiation), as well as their data. Those recommendations required standardisation compatible with those applicable in the payments ecosystem and an *integrated* consumer experience between the sharing of data and the initiation of payments... Similarly, the work undertaken to strengthen and modernise the management of *identity credentials* to combat *fraud* and build trust is fundamental to the future of our payments ecosystem.”  
(emphasis added)

In support of this, AusPayNet restates its earlier suggestion that the decision to share personal information should rely on legal obligation in the first instance, and on consent only where necessary. This approach will enable integrated and end-to-end payment services while avoiding consent fatigue.

Since payments activities can take place across multiple sectors, AusPayNet also reiterates its recommendation that the new Act be focussed on privacy and data protection at a fundamental level, and not propose sector-specific requirements. The goal is to establish the underlying principles which would apply to all sectors. A streamlined regulatory landscape will create a better environment for compliance. In its submission to the Department of Home Affairs’ consultation on ‘*Strengthening Australia’s cyber security regulations and incentives*’ which also included a review of the *Privacy Act*, AusPayNet noted that setting consistent expected behaviours will make it easier for all companies – especially small and medium enterprises with lesser resources – to understand and comply.<sup>3</sup>

Consistent privacy regulations will also enable the development of interoperable products and services for improved customer experience in payments. In response to the Digital Transformation Agency’s release of the Trusted Digital Identity Bill,<sup>4</sup> AusPayNet explained the critical importance in digital identity of interoperability, being the ability to transfer and render useful data and other information across systems, applications and devices. Interoperability supports end-user choice and convenience, by enabling users to make digital transactions, independent of any other user or company, and avoiding siloes or walled gardens. An example of the benefit of interoperability is the enablement of the “Tell Us Once” initiative by the New South Wales Government.<sup>5</sup> The initiative creates a secure platform for transactions across government clusters, allows customers to save and reuse personal information, and reduces cost of data synchronisation.

In addition, AusPayNet suggests that the Department’s proposal 18 be strengthened for the correction of personal information. AusPayNet reiterates its suggestion of a clear obligation on the business payment service user to ensure that their beneficiary lists are up to date, to avoid incorrect or failed payments. AusPayNet has responded accordingly to the Australian Security and Investment Commission’s (ASIC) consultation paper 341 ‘*Review of the ePayments Code: Further Consultation*’, which is aimed at addressing

---

3 Australian Payments Network Limited, Submission to the Digital Transformation Agency’s Consultation on Trusted Digital Identity Bill 27 October 2021 <<https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/australian-payments-network.pdf>>.

4 Department of Home Affairs, 1 October 2021, ‘Consultation on the exposure draft of the Trusted Digital Identity Bill and related legislative instruments’, Accessed 14 December 2021 <<https://www.digitalidentity.gov.au/have-your-say/phase-3>>

5 NSW Department of Customer Service, Government Made Easy – Creating ‘Tell Us Once’ Transactions with Government, 1 November 2021 <<https://www.digital.nsw.gov.au/article/government-made-easy-creating-tell-us-once-transactions-with-government>>.

issues such as mistaken internet payments.<sup>6</sup> Treasury has since confirmed that it agrees with mandating the ePayments Code<sup>7</sup>; it is therefore pertinent for the review of the Privacy Act to be harmonised with that of the ePayments Code.

## Responses to the Department's Proposed Options

### Proposal 12. Pro-privacy default settings.

12.1 Introduce pro-privacy defaults on a sectoral or other specified basis.

- **Option 1** – Pro-privacy settings enabled by default: Where an entity offers a product or service that contains multiple levels of privacy settings, an entity must pre-select those privacy settings to be the most restrictive. This could apply to personal information handling that is not strictly necessary for the provision of the service, or specific practices identified through further consultation.
- **Option 2** – Require easily accessible privacy settings: Entities must provide individuals with an obvious and clear way to set all privacy controls to the most restrictive, such as through a single click mechanism.

AusPayNet acknowledges that the proposed options resemble opt-out (option 1) and opt-in (options 2) decisions. In its earlier feedback, AusPayNet supports the modern principles of Privacy by Design and data minimisation. Both principles suggest that data can be anonymised when no longer required to be identified to a specific person. On this basis, AusPayNet supports Option 1 on pro-privacy settings as the default setting.

We note though that the current wording is unclear and can also be read as the entities' provision of *default settings* (option 1) and provision of an obvious *technical feature* for customers to change the settings at a later stage (option 2). With this interpretation, both the default setting and technical feature can be made available and are not mutually exclusive. For example, an individual who has downloaded an ecommerce app will find that the app is first set to not share information of his/her purchases with friends and family (option 1). The individual can easily navigate to and change the settings to share the information with family only and can also change his/her mind to set all privacy controls back to the most restrictive setting of not sharing with them or anyone (option 2).

Based on the above, AusPayNet recommends introducing both pro-privacy default settings and easily accessible privacy setting technical features across all sectors.

<sup>6</sup> Australian Payments Network Limited, Submission to the ASIC's Consultation Paper 341 'Review of the ePayments Code: Further Consultation' 2 July 2021 <<https://download.asic.gov.au/media/k4xd2lrj/cp341-submission-auspaynet.pdf>>.

<sup>7</sup> Commonwealth Treasury, 8 December 2021, 'Transforming Australia's Payments System', Accessed 14 December 2021 <<https://treasury.gov.au/sites/default/files/2021-12/p2021-231824.pdf>>

### **Proposal 26. A statutory tort of privacy**

**26.1 Option 1:** Introduce a statutory tort for invasion of privacy as recommended by the ALRC Report 123.

**26.2 Option 2:** Introduce a minimalist statutory tort that recognises the existence of the cause of action but leaves the scope and application of the tort to be developed by the courts.

**26.3 Option 3:** Do not introduce a statutory tort and allow the common law to develop as required. However, extend the application of the Act to individuals in a non-business capacity for collection, use or disclosure of personal information which would be highly offensive to an objective reasonable person.

**26.4 Option 4:** In light of the development of the equitable duty of confidence in Australia, states could consider legislating that damages for emotional distress are available in equitable breach of confidence.

AusPayNet notes that the introduction of a statutory tort will also necessitate a legal test to determine if there has been a breach. Such a test will, in turn, require a fit-for-purpose consent framework to determine if the personal information was shared with permission.

Under the Department's proposal 9.1, consent is to be defined in the new Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action. We agree that modern data protection law has shown that consent is effective when it relates to a clear and specific request. This is recommended for simple and definitive activities. A different consent mechanism will be needed for complex situations. Specific and unambiguous consent may not be possible and can be disruptive to a chain of payment activities happening almost instantaneously. The proposed definition is also not aligned with the direction of the current discussions in creating digital identity solutions (see for example our earlier comments on the "Tell Us Once" initiative) in seeking to provide convenient and secure payment processes, without the need for consumers to repeat their information and consent. This means the current definition, while useful for simple and definitive payment activities, is inapplicable for complex or ongoing payment activities.

Similarly, the CDR is currently not enabled for multi-dimensional, fine-grained consent. It does not have the granularity of dimensions required for action initiation or the ability to add new dimensions (such as creditor, debtor, amount, currency, frequency and date) in order to provide full control and visibility to the consumer and the Accredited Action Initiator.

In lieu of a well-established and accepted consent framework in a complex payment system, AusPayNet is of the opinion that options 1 and 2's introduction of a statutory tort is premature and will cause confusion. AusPayNet holds the same position in its earlier submission that as payment service providers and merchants in Australia implement e-commerce security protocols over the next few years, it will be important to ensure that the capture and provision of consent and authentication data meets the requirements of the new Act. AusPayNet remains keen in bringing together the Department and an expert group to ensure this is the case.

AusPayNet understands that options 3 and 4 appear more targeted at addressing the harms caused by the breach of privacy on social media and to fulfilling the policy objectives of the exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 under consideration at the

same time. These options dealing with “offensive” conduct and “emotional distress” are out of scope for AusPayNet.

### Conclusion

AusPayNet appreciates the opportunity to respond to the consultation and to contribute our insights from the perspective of the payments industry and the wider digital economy context. We welcome a streamlined regulatory environment for privacy, focused on data protection at a fundamental level while enabling new interoperable and technology neutral approaches to digital identity and the sharing of personal information generally. AusPayNet welcomes the opportunity to engage further with the Attorney General’s Department and share the progress of our work on the issues raised in this submission.

[Redacted signature area]

Yours sincerely

[Redacted signature]

[Redacted name]

**CEO, Australian Payments Network**