Submission on the Review of national arrangements for the protection and management of identity information

26 October 2018

Introduction

The Australian Mobile Telecommunications Association (AMTA) and Communications Alliance (CA) (the Associations) welcome the invitation to provide comments to the Department of Home Affairs' review of the national arrangements for the protection and management of identity information. This review provides a welcome opportunity to test whether current arrangements for identity management, and the regulatory obligations imposed on the telecommunications industry, are still fit for purpose and delivering the desired outcomes required for consumer protection in relation to privacy and identity theft or misuse.

What purpose is an identity?

Historically, service providers in the telecommunications industry have relied on some kind of identity check to establish a customer's profile and deliver a service. This enables services providers to know who their customer is so that they can contact them as necessary in order to provide them with a service. Service providers traditionally will also conduct some form of credit check on a customer before providing them with a service. However, changes in technology and how we do business, mean that in some cases, a traditional identity or credit check may not be a business requirement for all service providers. For example, a customer with a prepaid mobile service will not need to be billed and contact may be by email, app or text and so the service provider will have no business reason for collecting or verifying the customer's name or residential address [noting, as explained below, that prepaid mobile services are regulated by the *Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017* (the Prepaid ID Check Determination) which does require service providers to capture and verify a customer's evidence of identity].

Obligations to capture identity

Why does the Telecommunications sector have to capture a person's identity information?

Under the *Telecommunications Act 1997* and associated regulations, Carriage Service Providers[1] (CSPs) have regulatory obligations related to capturing identity information and in some cases, verification of evidence of identity information:

1) CSPs must capture the name, address and associated details including type of service, directory listing preferences, service category for the purposes of providing this information to the Integrated Public Number Database (IPND) in accordance with the associated ACMA IPND Scheme and registered Industry Code (C555); and
2) CSPs must comply with the requirements of the Prepaid ID Check Determination (in place in various forms since 2001) to capture and verify a customer's evidence of identity information before providing them with a prepaid mobile service.

In practice, most CSPs make use of the Government's Document Verification Service (DVS) as the primary method of verifying evidence of identity information provided by customers activating a prepaid mobile service, however, the regulation also allows for several other methods of identity check to be used and many CSPs do rely on other methods to varying extents.

[1] The term 'carriage service provider' is defined in section 87 of the Act to include a person who supplies, or proposes to supply, a listed carriage service to the public using a network unit owned by one or more carriers or a network unit in relation to which a nominated carrier declaration is in force. (Explanatory Memorandum)

Clearly, both of the above regulatory obligations do not actually require that the customer's identity is validated, rather, the customer's evidence of identity information is validated as it is presented by the customer. We note that the current regulations do not prevent an individual presenting stolen evidence of identity information for validation, and that a DVS check will simply verify that a driver's licence (or other evidence of identity) is valid without verifying that the licence belongs to the individual presenting it, usually online or over the phone.

These regulatory obligations impose significant costs on telecommunications service providers without delivering the requisite benefit of a robust system in terms of collection or verification of identity information.[2]

A way forward

The need for a robust system of collection and verification of identity information has long been advocated for by law enforcement and national security agencies.

While industry may not always have a business requirement to either collect or verify a customer's identity, we adopt the pragmatic view that the Government's objective will remain that there should be a regulatory obligation on CSPs to collect and/or verify customer identity information.

However, we strongly suggest that where the CSP has no business requirement to verify or store customer information, the regulation should not require them to verify or store that information just to meet a regulatory obligation, for example, providing information to the IPND or compliance with the Prepaid ID Check Determination. Rather, we suggest that service providers in these circumstances could facilitate customer verification against an external Government or trusted third party system if required. This would enable CSPs to avoid the risk and costs associated with verifying[3] and storing customer information which can be quite onerous for smaller service providers. For example, some service providers do not hold credit card data, but facilitate a customer to generate a token directly with a banking institution, allowing the service provider to only hold the token returned to them and not the credit card details.

Such an approach to identity verification and storage of information, that relies on a Government or trusted third party provider, would be more secure than having identity information distributed throughout industry service providers in circumstances where it is otherwise not required for business purposes.

Therefore, we suggest that any improvements that are made to national arrangements for the protection and management of identity information should include consideration of the following key points and principles:

1) A new national identity framework ought to replace existing arrangements and ensure that no parallel arrangements continue to exist.

2) National arrangements need to be truly national and consistent across state jurisdictions.

3) The legislative framework should be clear in its purpose and objectives and not impose overly onerous or costly obligations on industry.

[2] The costs associated with use of the Government's DVS can be prohibitive for many CSPs
[3] Ibid.

4) Where industry has a regulatory obligation to collect and verify customer identity information, any Government system or arrangements for doing so should be made accessible to industry, for example, as the DVS was made available to the telecommunications service providers to enable compliance with the Prepaid ID Check Determination. We also note that the cost of accessing any system needs to be made reasonable so that it does not prohibit service providers from doing business.

5) Arrangements should not require service providers to verify or store customer information themselves when there is no business requirement to do so; rather the arrangements should enable CSPs to facilitate verification against a Government or trusted third party system.

6) Regulatory requirements should always request the minimum amount of identity data necessary for a particular customer for any particular purpose; likewise any requirement to capture and store customer identity information as provided to the service provider.

7) Customers should be enabled by the framework to establish their identity only once and subsequently be able to rely on the established identity in transactions with other entities and organisations – both public and private sector. Noting that customers who are the victims of identity theft or misuse will also need a robust and accessible pathway to re-claim their identity information and prevent further misuse. Therefore, there should always be scope for the customer to be able to establish/re-claim their identity via multiple pathways.

8) Customers should be empowered under the framework to be able to access and manage their identity information as reasonably required.

9) Customers must be able to trust that their privacy will be adequately protected under the framework.

10) All members of the community must be able to easily access, trust and use the framework; noting that this will always prove a challenge for some members of the community that either lack access to evidence of identity information or do not possess such information, as well as more vulnerable members of the community who will necessarily rely on the assistance of others to establish and use identity information.

Conclusion

The Associations support the review of the national arrangements for the protection and management of identity information. With so many changes to technology and business practices in recent years and with the telecommunications industry planning to roll-out 5G mobile services as early as 2019, it is timely to review the current legislative and regulatory framework around identity and test whether it is still fit for purpose and able to deliver the requisite consumer outcomes and privacy protections.

We believe the principles and suggested points outlined above should all be considered closely by the review team and look forward to further engagement with the review process.

Please contact Lisa Brown, Public Policy Manager, AMTA at lisa.brown@amta.org.au or 02 8920 3555 if you have any questions in relation to this submission.