Submission in response to the Parliamentary Joint Committee on Intelligence and Security

Review of Identity-Matching Services Bill 2019 and the Australian Passports Amendment (Identity-Matching Services) Bill 2019

6 September 2019

Introduction

1.1 Optus appreciates the opportunity to provide input into the review of the Identity-Matching Services Bill 2019 ('the ID-Matching Bill') by the Parliamentary Joint Committee on Intelligence and Security (PJCIS).

1.2 From Optus' perspective, the ID-matching Bill and the associated Australian Passports Amendment (Identity-matching Services) Bill 2019 together provide the basis for a significant next step in the vitally important task of improving public confidence and enhancing the capability of Australia's identity validation processes. Continuing to build Australia' capability is important for a range of economic and security related reasons.

… it is vital for Optus that it maintains and seeks to enhance its identity validation processes….

1.3 The SingTel Optus Pty Ltd group companies in Australia ("Optus") serve over 11 million customers per day with a broad range of communications services, including mobile, national, local and international telephony, fixed and mobile broadband, subscription and IP television, and content services. In summary, Optus is a provider of critical national communications infrastructure and services to the Australian community.

1.4 As a telecommunications provider with commercial and legal obligations to be able to identify and verify the identity of the customers and potential customers who seek to use its services, it is vital for Optus that it maintains and seeks to enhance its identity validation processes. These processes need to be robust, fit for purpose, and future proof. Further, they need to be subject to suitable security and integrity controls suited to the status of the personal information which they handle.

1.5 Legislation enacted by Parliament in recent years has sought to ensure that Australia's security and law enforcement agencies have ongoing access, in approved and authorised circumstances, to relevant communications data and communications content. The integrity and utility of this obvious priority of the Parliament in turn relies on the ability of carriers and carriage service providers to accurately validate the identity of their customers and prospective customers during the process of establishing accounts for their communications services and subsequent customer service interactions.

Identity theft and identity fraud

1.6 Identity theft and identity fraud is an increasing problem affecting the Australian economy and customers of communications services. Such illegal activity can result in far-reaching consequences for individuals, ranging from having to change ID documents, phone numbers and email addresses, through to more serious consequences such as having money stolen from their bank accounts, having loans taken out or crimes committed using their name, or having their personal security compromised.

1.7 Both Optus and its customers have been, and continue to be, impacted by the increasing instances of ID theft and fraud. Optus faces a responsibility to continue to explore ways to improve and enhance its customer identity validation techniques and capability.

National Identity Security Strategy

1.8 The coordinated Government approach contemplated by the Intergovernmental Agreement to a National Identity Security Strategy (the National ID Strategy) and being

implemented by changes such as the ID-Matching Bill, appear to be critical steps to build confidence in Government ID management and validation techniques for the Australian economy into the future.

1.9 As is noted in the Explanatory Statement to the ID-Matching Bill (p.3), "the identity management systems of government agencies that issue Australia's core identity documents…play an important role in preventing identity crime".

1.10 Optus is a current user of the Government's Document Verification Service (DVS). Its use of the DVS enables validation of the ID documents that customers provide when signing up to Optus services. However, the current DVS system only validates if an ID document exists with the relevant agency and if some of the ID information (name, etc) matches, but it cannot currently verify that the person whose photo appears on the ID document that has been provided to us is the same person whose photo appears on the actual ID document held by the relevant state, territory or federal agency that issued the ID document.

1.11 The lack of a current facial verification service is a big limitation in the current ID matching systems. Optus believes that the enhancements being proposed via the National ID Strategy and the ID-Matching Bill will assist Government to build better ID validation techniques through the sharing of ID information (including facial verification) between state, territory and federal agencies, and this will lead to better outcomes and enhanced protections for Australian consumers and the businesses that rely on Government ID verification tools.

Optus supports the key provisions of the Bill

1.12 Optus endorses the provisions of the ID-Matching Bill which:

(a) enable the establishment of the interoperability hub for relaying electronic communications between bodies and persons for the purposes of requesting and providing identity-matching services;

(b) enable the establishment of a system, with suitable controls, for biometric comparison of facial images with facial images;

(c) support the information sharing, and establishment of capability to store and link the various State Government and Commonwealth Government information and identity sources;

(d) support the development of identity matching services which include supporting requests, from a local government authority or non-government entity, relating to an individual for the purpose of verifying the individual's identity; and

(e) ensure that safeguards to protect an individual's personal information are placed on the use of identity matching services by non-government entities. Optus notes those safeguards include the consent provisions described.

1.13 As a result, Optus recommends that the PJCIS support the advancement of this Bill with suitable priority to provide the legislative framework to allow the development of these vital identity matching services as soon as practical.

Ends.