EXPLANATORY STATEMENT

Approved by the Australian Communications and Media Authority

Telecommunications Act 1997

Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017

Authority

The Australian Communications and Media Authority (**the ACMA**) makes the *Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017* **(the Determination)** under subsection 99(1) of the *Telecommunications Act 1997* **(the Act**).

Subsection 99(1) of the Act provides that the ACMA may make written determinations setting out rules that apply to service providers in relation to the supply of specified carriage services or content services, which are called service provider determinations. Subsection 99(3) of the Act provides, relevantly, that the ACMA must not make a service provider determination unless the determination relates to a matter specified in the regulations. The relevant enabling regulations are the *Telecommunications Regulations 2001*.

Section 33 of the *Acts Interpretation Act 1901* relevantly provides that where an Act confers a power to make a legislative instrument, the power shall be construed as including a power exercisable in the like manner, and subject to the like conditions (if any), to repeal, rescind, revoke, amend or vary any such instrument. The Determination repeals and replaces the *Telecommunications (Service Provider – Identity Checks for Prepaid Public Mobile Carriage Services) Determination 2013* (**the 2013 Determination**) with modifications to improve the efficiency and effectiveness of the identity-checking arrangements for prepaid mobile carriage services (**prepaid mobile services**).

The Regulation Impact Statement that informed the making of the 2013 Determination foreshadowed that it would be reviewed two years after it had been made by the ACMA (in October 2013). The ACMA completed its review of the 2013 Determination in August 2016 along with the assistance of a joint industry and government agency working group (**the WG**). The review was concerned with improving the effectiveness and efficiency of the regulatory arrangements and to address some of the practical issues that have arisen as CSPs have transitioned away from sighting identification at the time of sale to other methods of identity verification.

As part of the review process, the WG developed 17 recommendations for consideration by the ACMA. Those recommendations are set out in the report of the WG, which can be accessed at http://acma.gov.au/sitecore/content/Home/theACMA/revised-identity-checking-requirements-for-prepaid-mobile-services. The ACMA supported all 17 recommendations. Of those 17 recommendations, eight involved changes to the 2013 Determination. The Determination gives effect to those eight recommendations.

Purpose and operation of the instrument

Regulatory arrangements for prepaid mobile services have been in place since 1997. The requirements were put in place to inhibit the use of anonymous prepaid mobile services, so that law enforcement and national security agencies (**law enforcement agencies**) can gain accurate information and evidence about users, should they need to do so.

The Determination sets out the regulatory framework for the supply of prepaid mobile services by carriage service providers (**CSPs**).

Under the Determination, and subject to limited exemptions, a CSP who supplies a prepaid mobile service to a person (the customer), must not activate the service unless the CSP has complied with:

- the rules set out in Part 4 of the Determination, which require the CSP to obtain certain identifying information about, and to verify the identity of, the customer; or
- a compliance plan that has been approved by the ACMA under Part 5 of the Determination.

The objects of the Determination are set out in section 2.1 of the Determination and, in summary, are:

- to assist law enforcement agencies to identify customers in relation to prepaid mobile services;
- to protect the privacy of individuals by ensuring that CSPs obtain, record and keep only the minimum amount of information that is reasonably necessary; and
- to provide CSPs with a range of methods which can be used to verify the identity of customers.

A provision-by-provision description of the Determination is set out in the notes at **Attachment A**.

The Determination is a legislative instrument for the purposes of the *Legislation Act 2003* (**the LA**).

Documents incorporated by reference

This Determination incorporates the following Acts and legislative instruments (including by the adoption of definitions), or otherwise refers to them:

- the 2013 Determination;
- the Act;
- the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*;
- the *Australian Charities and Not-for-profits Commission Act 2012*;
- the *Banking Act 1959*;
- the *Competition and Consumer Act 2010*;
- the *Corporations Act 2001*;
- the *Defence Act 1903*;
- the *Family Law Act 1975*;
- the *National Consumer Credit Protection Act 2009*;
- the *Telecommunications (Conditions for Allocation of Numbers) Determination 1997*;
- the *Telecommunications (Interception and Access) Act 1979* (the **TIA Act**); and
- the *Telecommunications Numbering Plan 2015*
- the *Telecommunications (Service Provider – Identity Checks for Pre-paid Carriage Services) Determination 1997*;
- the *Telecommunications (Service Provider — Identity Checks for Pre-paid Public Mobile Telecommunications Services) Determination 2000*.

The Acts and legislative instruments listed above may be obtained from the Federal Register of Legislation (http://www.legislation.gov.au). The Acts listed above are incorporated as in force from time to time, in accordance with section 10 of the *Acts Interpretation Act 1901*, subsection 13(1) of the LA and section 589 of the Act. The legislative instruments listed above are incorporated as in force from time to time, in accordance with section 1.7 of the instrument and subsection 14(1) of the LA and section 589 of the Act.

Consultation

Before the Determination was made, the ACMA was satisfied that consultation was undertaken to the extent appropriate and reasonably practicable, in accordance with section 17 of the LA.

The ACMA consulted with industry stakeholders and the general public on the making of the Determination. Between 7 November 2016 and 4 January 2017, the ACMA conducted a public consultation process inviting submissions on the proposed changes through the release of a draft instrument and a consultation paper on the ACMA's website.

As required under subsection 99(4) of the Act, the ACMA also consulted the Australian Competition and Consumer Commission.

The consultation paper outlined the following proposed changes to improve the efficiency and effectiveness of the 2013 Determination:

- broadening the application of some of the verification methods (for example, the financial transaction method) and increasing the range of credit cards and identification documents that can be used for verification;
- streamlining the record-keeping requirements and the obligations that apply to CSPs providing mobile services to individuals who have been affected by an emergency;
- consolidating the verification methods into a single part of the proposed Determination through the use of tables;
- allowing industry to submit joint (in addition to individual) alternative compliance plans for approval by the ACMA; and
- removing the secure postal delivery method as agreed by the WG.

The ACMA received nine submissions from representatives of industry, law enforcement agencies and consumer interests. The ACMA considered all relevant issues raised by the submissions when making the Determination. In response to the consultation, the ACMA updated the Determination to:

- clarify certain definitions in Part 1 of the Determination;
- amend the list of Category A documents in Part 1 of the Determination to allow foreign military personnel to obtain prepaid mobile services in Australia by allowing their military identity cards to be used as evidence of identity on access-controlled defence sites;
- amend the definition of emergency in Part 3 of the Determination so that it is no longer linked to the definition under the Act and to expand on the type of emergency events that are captured such as fire, flood, storm, earthquake, explosion or terrorist act;
- expand the exemption provisions in Part 3 of the Determination that currently apply in emergency situations (like bush fires and floods) to victims of family violence where they are unable or unwilling to return to their principal place of residence as a result of family violence;
- remove the requirement for CSPs to record additional information in relation to entities such as Australian Business Number, Australian Company Number and Australian Registered Business Number in Part 4 of the Determination;
- ensure that there is no inconsistency between Part 6 of the Determination and the requirements imposed on CSPs under Part 5-1A of the TIA Act in relation to data retention;

- further streamline the record-keeping requirements in Part 6 of the Determination by removing the requirement to record the last four digits of a credit card when it is shown to a CSP as part of a visual identity check[1]; and
- amend Schedule 1 to make the descriptions of the two financial transaction methods more consistent.

The following key issues were also raised during the consultation process but not supported by the ACMA:

- That the draft Determination did not sufficiently broaden the scope of trusted credit cards.
- That the ACMA should introduce a timeframe to phase-out visual identity checks at the time of sale.

Regulatory impact assessment

A preliminary assessment of the proposal to make the instrument was conducted by the Office of Best Practice Regulation (**OBPR**), based on information provided by the ACMA, for the purposes of determining whether a Regulation Impact Statement would be required. OBPR advised that the proposed regulatory change in this instrument was minor or machinery in nature and verified that no further regulatory impact analysis was required (OBPR reference number 20982).

Statement of compatibility with human rights

Subsection 9(1) of the *Human Rights (Parliamentary Scrutiny) Act 2011* requires the rule-maker in relation to a legislative instrument to which section 42 (disallowance) of the LA applies to cause a statement of compatibility with human rights to be prepared in respect of that legislative instrument.

The statement of compatibility set out in **Attachment B** has been prepared to meet that requirement.

[1] Where a credit card is used as part of a visual check, it must be sighted with another specified identity document (such as a driver licence or Medicare card). Under the 2013 Determination, the CSP was required to record the last four digits of a credit card number yet was not required to record any numbers from the other identity documents. Given this inconsistency, the Determination does not include the same requirement in relation to credit cards.

Attachment A

Notes to the *Telecommunications (Service Provider — Identity Checks for Prepaid Mobile Carriage Services) Determination 2017*

Part 1 – Preliminary

Section 1.1 Name of Determination

This section provides for the instrument to be cited as the *Telecommunications (Service Provider — Identity Checks for Prepaid Mobile Carriage Services) Determination 2017.*

Section 1.2 Commencement

This section provides for the instrument to commence at the start of the day after it is registered on the Federal Register of Legislation.

Section 1.3 Authority

Section 1.3 provides that the Determination is made under subsection 99(1) of the Act.

Section 1.4 Repeal of the *Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2013*

This section provides that the 2013 Determination is repealed.

Section 1.5 Definitions

This section defines a number of key terms used throughout the Determination and notes that a number of other expressions used in the Determination are defined in the Act.

Section 1.6 References to carriage service provider

This section provides that a reference to a CSP obtaining information from a customer; verifying the identity of a customer; or activating or deactivating a prepaid mobile service, includes a reference to an authorised party doing those things for, or on behalf of, the CSP.

Section 1.7 References to other instruments

This section provides that in the Determination, unless the contrary intention appears:

- a reference to any other legislative instrument is a reference to that other legislative instrument as in force from time to time; and
- a reference to any other kind of instrument is a reference to that other instrument as in force from time to time.

Section 1.8 References to category A and category B documents

This section defines what is a category A document and what is a category B document. These two categories of documents are what a CSP can sight for the purposes of verifying the identity of a customer as part of a visual identity document check, as required by section 4.4 of the Determination and item 8 of Schedule 1 to the Determination. Under those provisions, the number and categories of documents that must be sighted by the CSP will depend on how the purchaser chooses to pay for the prepaid mobile service and whether (or not) activation of the service will result in the purchaser having 5 or more activated prepaid mobile services.

Part 2 – Objects and application of Determination

Section 2.1 Objects of Determination

Section 2.1 sets out the objects of the Determination.

Section 2.2 Application of Determination

Subsection 2.2(1) provides that subject to subsection 2.2(2), the Determination sets out the rules that apply to CSPs in relation to the supply of prepaid mobile services.

Subsection 2.2(2) provides that the rules in the Determination will not apply to a CSP in relation to a supply of a prepaid mobile service to a person if it previously supplied the service to the person and, the service has not been deactivated, and, in relation to that previous supply, the CSP complied with the requirements set out in any of the:

- the Determination; or
- the *Telecommunications (Conditions for Allocation of Numbers) Determination 1997*; or
- the *Telecommunications (Service Provider – Identity Checks for Pre-paid Carriage Services) Determination 1997*; or
- the *Telecommunications (Service Provider — Identity Checks for Pre-paid Public Mobile Telecommunications Services) Determination 2000*; or
- the 2013 Determination.

If, for example, a purchaser or service activator was previously supplied with a prepaid mobile service by a CSP who had complied with the relevant requirements at the time (being those stipulated in one of the instruments listed in subsection 2.2(2)) and wants to recharge their prepaid mobile service, the rules set out in the Determination do not apply in relation to the further supply of the service by the CSP. However, the rules would apply if the service was deactivated and the customer was seeking to reactivate it.

Section 2.3 Requirements that must be satisfied before service is activated

Subsection 2.3(1) provides that, subject to subsection 2.3(2), a CSP who supplies a prepaid mobile service to a person must not activate that service unless the CSP has complied with the rules set out in Part 4, or complied with an approved compliance plan made under Part 5.

Subsection 2.3(2) provides that the rule in subsection 2.3(1) does not apply if an exemption under Part 3 applies or subsection 4.2(2) applies in relation to the prepaid mobile service.

Section 2.4 Obligations when using an authorised party

The effect of section 2.4 is that if a CSP uses an authorised party to sell or give away prepaid mobile services, the CSP is ultimately responsible for complying with the requirements of the Determination. This section requires CSPs to ensure that the actions of authorised parties which they use support the CSP in meeting the requirements under the Determination.

Subsection 2.4(1) provides that if a CSP uses an authorised party to sell a service, or to invite a person to use a prepaid mobile service at no charge to that person, the CSP must comply with section 2.4.

Subsection 2.4(2) provides that the CSP must ensure that the authorised party acts in a manner that enables the CSP to comply with its obligations under the Determination.

Subsection 2.4(3) prohibits a CSP from engaging in conduct where:

- its authorised party sells a service to a person (the **third party**) or invites a third party to use a prepaid mobile service at no charge to that person;
- neither the CSP nor the authorised party obtains the necessary information from, and verifies the identity of the person; and
- the CSP or the authorised party activates the prepaid mobile service.

Part 3 — Exemptions from rules

Part 3 is intended to allow individuals who are adversely affected by an emergency or family violence to have access to prepaid mobile services as soon as reasonably practicable in the circumstances. Provided that the CSP complies with the requirements in Part 3, the CSP is exempt from complying with the general requirements set out in section 2.3.

3.1 Supplying prepaid mobile carriage services during emergencies

Section 3.1 exempts a CSP from the requirements set out in section 2.3 if the CSP proposes to supply a prepaid mobile service to an "emergency-affected individual" and all of the circumstances set out in subsection 3.1(2) apply.

An "emergency-affected individual" is defined in subsection 3.1(3) as an individual who is unable to inhabit or access their principal place of residence as a result of an emergency.

The term "emergency" is defined in subsection 3.1(3) as an actual or imminent event (such as fire, flood, storm, earthquake, explosion or terrorist act) that causes widespread disruption to a community – rather than to an individual – and requires a significant and coordinated response. This definition may cover small-scale events, such as bush fires that might affect only a few properties in a defined geographic area, as well as large scale disasters. Such events or disasters are not limited to natural disasters or weather related events but may also be man-made – for example, terrorist acts. The definition may also cover an event irrespective of whether that event has been officially declared as a state of emergency.

Under subsection 3.1(2), a CSP does not have to comply with section 2.3 in relation to the supply of a prepaid mobile service if:

- the CSP itself distributes end-user equipment (such as SIM cards) to a person whom the CSP reasonably believes to be an emergency-affected individual and obtains the name and residential address of the emergency-affected individual unless it is not reasonably practicable to do so; or
- the CSP distributes end-user equipment to an authorised party or an emergency assistance organisation on the condition that the authorised party or emergency assistance organisation:
    - only distributes the equipment to a person whom the party or organisation reasonably believes to be an emergency-affected individual; and
    - obtains and records the name and residential address of the emergency-affected individual unless it is not reasonably practicable to do so.

If the CSP has arranged for the end-user equipment to be distributed by an authorised party or emergency assistance organisation, the CSP must obtain the name and business address of the party or organisation and (if obtained by the party or organisation) the name and residential address of the emergency-affected individual who is provided with the equipment. The Determination does not prescribe how the CSP must obtain the information. This gives the CSP some flexibility in deciding the most convenient way of fulfilling that obligation. The CSP may, for example, decide to obtain the information from the party or organisation via email or a spreadsheet. In addition, the Determination does not require the CSP to verify any of the information so obtained.

A prepaid mobile carriage service supplied to an emergency-affected individual under Part 3, can only remain activated for a maximum of 30 days, unless the ACMA approves a longer period in writing. Such an approval by the ACMA may apply to an individual prepaid mobile service, or to a class of prepaid mobile services.

An individual who was supplied with a prepaid mobile service which has been deactivated in accordance with the 30 day requirement may request that the deactivated service be activated. The CSP is not obliged to accept such a request. However, before activating any new service, the CSP will be required to comply with the rules set out in Part 4, or comply with an approved compliance plan made under Part 5.

3.2 Supplying prepaid mobile carriage services to family violence-affected individuals

Section 3.2 exempts a CSP from the requirements set out in section 2.3 if a CSP proposes to supply a prepaid mobile service to a family violence-affected individual and all of the circumstances set out in subsection 3.2(2) apply.

The term "family violence" has the same meaning as in section 4AB of the *Family Law Act 1975* (**the FLA**). Relevantly under subsection 4AB (1) of the FLA, "family violence" is defined to mean "violent, threatening or other behaviour by a person that coerces or controls a member of the person's family (the ***family member***), or causes the family member to be fearful". Under subsection 4AB(2) of the FLA, examples of behaviour that may constitute family violence include (but are not limited to):

- an assault; or
- a sexual assault or other sexually abusive behaviour; or
- stalking; or
- repeated derogatory taunts; or
- intentionally damaging or destroying property; or
- intentionally causing death or injury to an animal; or
- unreasonably denying the family member the financial autonomy that he or she would otherwise have had; or
- unreasonably withholding financial support needed to meet the reasonable living expenses of the family member, or his or her child, at a time when the family member is entirely or predominantly dependent on the person for financial support; or
- preventing the family member from making or keeping connections with his or her family, friends or culture; or
- unlawfully depriving the family member, or any member of the family member's family, of his or her liberty.

A "family violence-affected individual" is defined in Part 3 as an individual who has been affected by family violence and, as a result, is unable or unwilling to inhabit or access their principal place of residence.

Under subsection 3.2(2), the CSP is exempt from complying with section 2.3 if the CSP distributes end-user equipment to a "family violence assistance organisation" on the condition that the:

- end-user equipment is provided to a person, who, in the reasonable belief of the family violence assistance organisation, is a family violence-affected individual; and
- the family violence assistance organisation obtains and records the name and residential address of the family violence-affected individual unless it is not reasonably practicable to do so.

The CSP cannot directly provide end-user equipment to a family violence-affected individual.

The CSP must obtain the name and business address of the family violence assistance organisation, and if obtained, the name and residential address of the family violence-affected individual. The Determination does not prescribe how the CSP must obtain the information. This gives the CSP some flexibility in deciding the most convenient way of fulfilling that obligation.

A prepaid mobile service supplied to a family violence-affected individual under Part 3 can only remain activated for a maximum of 30 days, unless the ACMA approves a longer period in writing. As is the case under section 3.1, such an approval by the ACMA may apply to an individual prepaid mobile service, or to a class of prepaid mobile services.

An individual who was supplied with a service which has been deactivated in accordance with the 30 day requirement may request that the deactivated service be activated. The CSP is not obliged to accept such a request. However, before activating any new service, the CSP will be required to comply with the rules set out in Part 4, or comply with an approved compliance plan made under Part 5.

Part 4 — Rules for obtaining information and verifying the identity of customers

4.1 Application of Part 4

Section 4.1 provides that Part 4 sets out the rules with which a CSP must comply with in relation to obtaining identifying information from, and verifying the identity of a customer of a prepaid mobile service for the purposes of paragraph 2.3(1)(a).

4.2 Requirements to be satisfied before service is activated

Subsection 4.2(1) provides that unless the exception at subsection 4.2(2) applies, before activating a prepaid mobile service, the CSP must obtain information about the customer in accordance with section 4.3 and verify their identity in accordance with section 4.4 in relation to a customer who is a purchaser, or section 4.5 in relation to a customer who is a service activator.

Subsection 4.2(2) provides two exceptions to the rule in subsection 4.2(1).

The first relates to where the CSP has activated the prepaid mobile service at the same time as, or immediately before, the provider receives confirmation that the service activator's specified financial account is active in accordance with paragraph (2)(c) and subitem (4) of item 4 of Schedule 1. This would apply where the CSP's systems enable activation of the prepaid mobile service at the same time that, or immediately before, it receives confirmation that the account is active when the CSP has successfully set up a direct debit arrangement with the service activator.

The second exception relates to where the CSP has temporarily activated the prepaid mobile carriage service in accordance with paragraph (2)(c) of item 5 of Schedule 1. This recognises that where a CSP uses the "Time-delayed financial transaction" method, it may take up to two business days for it to confirm that the service activator's account is active.

4.3 Information to be obtained from the customer

Section 4.3 requires the CSP to obtain certain information from the customer of a prepaid mobile service. The information that must be obtained varies depending on whether the customer is a purchaser or a service activator.

If the customer is a purchaser, the CSP must obtain the information mentioned in item 1 of Table 2. The information obtained includes the number of other activated prepaid mobile services supplied to the purchaser. A CSP may acquit this requirement by asking the purchaser to confirm how many other activated services they have.

If the customer is a service activator, the CSP must obtain the information mentioned in item 2 of Table 2. The information obtained includes the date of birth of the service activator. A CSP is not

required to collect date of birth information in relation to a customer who is a purchaser. The Regulation Impact Statement that informed the making of the 2013 Determination introduced the requirement to obtain the date of birth of a service activator. A similar requirement was not imposed for purchasers as there was recognition that this would have a regulatory impact on CSPs given that it would result in changes to CSPs' IT systems.

4.4 Verification of the identity of a customer who is a purchaser

Section 4.4 sets out how the CSP must verify the identity of the customer for a prepaid mobile service where the customer is a purchaser.

The CSP must ask the purchaser whether activation of the service will result in the purchaser having five or more activated prepaid mobile services. However, the Determination does not require the CSP to obtain proof of the information obtained in this regard.

Item 1 of Table 3 relates to a purchaser who pays for the service otherwise than by credit card or debit card – for example, by cash, cheque, a payment facility such as PayPal, or stored value card – and where the activation of the service will not result in the purchaser having five or more activated services. In this circumstance, to verify the identity of the purchaser, the CSP must see one category A document, or two category B documents, each of a different kind, identifying the purchaser.

Where the activation of the service will not result in the purchaser having five or more activated services and where the purchaser pays for the service using a credit card or debit card, the CSP is not required to take any additional steps to verify the identity of the purchaser.

Item 2 of Table 3 sets out the verification requirements where the purchaser informs the CSP that the activation will result in the purchaser having five or more activated services. In this circumstance, the CSP must see two category A documents, each of a different kind, or one category A and two category B documents, each of a different kind, identifying the purchaser.

Category A and category B documents are identified in section 1.8.

Paragraph 4.4(3)(a) requires the CSP to be satisfied that any document shown to it which includes an expiry date has not expired.

Additionally, under paragraph 4.4(3)(b) if the purchaser is showing the CSP a foreign military identification card, the CSP is only able to accept this form of identification if it is provided to the CSP on an access controlled defence site.

4.5 Verification of the identity of a customer who is a service activator

Section 4.5 sets out how the CSP must verify the identity of the customer for a prepaid mobile service where the customer is a service activator. Subsection 4.5(2) requires a CSP to use an approved method of identity verification to verify the identity of a service activator. The approved methods are specified in column B of Schedule 1.

Part 5 — Alternative methods for obtaining information and verifying the identity of customers

5.1 Application of Part 5

Part 5 sets out the requirements for the preparation, approval and amendment of a compliance plan for the purposes of paragraph 2.3(1)(b) and the circumstances in which an approved or amended compliance plan may be revoked. Part 5 is intended to provide CSPs with additional flexibility and promote innovation in developing alternative approaches to identity verification.

5.2 Applications from carriage service providers

Section 5.2 provides that a CSP may apply to the ACMA for approval of, a compliance plan, and, if the CSP wishes to amend the approved compliance plan, it may apply to the ACMA for approval of the amendment.

5.3 Applications from a group of carriage service providers

Section 5.3 provides that a group of CSPs may apply to the ACMA for approval of a joint compliance plan, and, if the group of CSPs wishes to amend the approved joint compliance plan, they may apply to the ACMA for approval of the amendment. The joint compliance plan applies to the group of CSPs that applied for its approval. An amendment to an approved joint compliance plan applies to all of the CSPs that the joint compliance plan applies to.

5.4 Form of application

Section 5.4 requires that an application for approval under sections 5.2 or 5.3 must be in writing and contain the information specified in subsection 5.4(b) or 5.4(c), as the case may be.

5.5 Approval of compliance plans

Subsection 5.5(1) requires the ACMA to decide to approve or not approve an application from a CSP or a group of CSPs for approval of a compliance plan.

Subsection 5.5(2) requires that the ACMA must consider the views of the Communications Access Co-ordinator[2] (**CAC**) on whether the compliance plan will satisfy the information needs of law enforcement agencies and whether the compliance plan meets the objects of the Determination that are set out in section 2.1.

5.6 Approval of amendment of approved compliance plan

Subsection 5.6(1) outlines the process that must be followed by the ACMA where it receives an application from a CSP or a group of CSPs to amend an approved compliance plan. The ACMA must decide whether the proposed amendment would result in a significant change to the approved compliance plan.

Subsection 5.6(2) requires that the ACMA must approve the proposed amendment to the compliance plan if it decides under subsection 5.6(1) that the proposed amendment would not result in a significant change.

Subsection 5.6(3) requires that if the ACMA decides under subsection 5.6(1) that the proposed amendment would result in a significant change, the ACMA must consult the CAC on whether the compliance plan will satisfy the information needs of law enforcement agencies, before deciding whether to approve or not approve the amendment to the compliance plan or joint plan.

Subsection 5.6(4) requires that before making a decision, the ACMA must consider the matters mentioned in subsection 5.5(2). These matters include considering the views of the CAC on whether

[2] The Communications Access Co-ordinator is an officer of the Attorney-General's Department, and acts on behalf of all national security and enforcement agencies (see section 6R of the TIA Act).

the compliance plan will satisfy the information needs of law enforcement agencies and whether the compliance plan meets the objects of the Determination that are set out in section 2.1.

5.7 Requests for further information and timeframes for making decisions

Section 5.7 sets out the process for requesting further information and the timeframes for making decisions on applications for approval of a compliance plan or an amendment to a compliance plan.

Subsection 5.7(1) allows the ACMA to make a request for further information in relation to an application for approval of a compliance plan or amendment to an approved compliance plan to the applicant CSP or group of CSPs.

Subsection 5.7(2) requires the ACMA to make a decision to approve or not approve a compliance plan or amendment to a compliance plan within one month after the later of either receiving the written views of the CAC or after receiving further information from the applicant.

Subsection 5.7(3) provides that if the ACMA fails to make a decision within the decision-making timeframe, the ACMA is taken to have not approved the compliance plan or amendment to a compliance plan.

5.8 Revocation of approved compliance plans

Subsection 5.8(1) sets out the circumstances in which an approved compliance plan may be revoked.

Subsection 5.8(2) provides that a CSP or a group of CSPs may revoke an approved compliance plan by giving the ACMA written notice of the revocation.

The compliance plan is taken to be revoked on the later of the ACMA receiving notice of the intention to revoke the compliance plan and the date of revocation (if any) specified in the notice to the ACMA.

Once an approved compliance plan has been revoked, the CSP or group of CSPs must comply with Part 4, unless an exemption provided by Part 3 applies.

Subsection 5.8(3) outlines the process that must be followed by the ACMA where it intends to revoke an approved compliance plan.

Before seeking to revoke an approved compliance plan, the ACMA must be satisfied, that the CSP or, in the case of a joint plan, one or more CSPs, have not complied with the approved compliance plan to a significant extent.

The ACMA must provide written notice to the CSP or group of CSPs of its intention to revoke the approved compliance plan.

Subsection 5.8(4) requires that the ACMA's notice of revocation must include the grounds for the proposed revocation and a statement that sets out the effects of subsections 5.8(5) to (9).

Subsection 5.8(5) provides that a CSP or group of CSPs may within 21 days of receiving a notice from the ACMA, give an objection notice to the ACMA objecting to the proposed revocation of the approved compliance plan.

Subsection 5.8(6) requires that the objection notice provided to the ACMA by the CSP or group of CSPs must include the grounds that the CSP or group of CSPs objects to the proposed revocation.

Subsection 5.8(7) provides that the ACMA may require further information in relation to the objection notice. In this circumstance, the ACMA may ask the CSP or group of CSPs in writing for additional information within 21 days of receiving the objection notice.

Subsection 5.8(8) requires the CSP or group of CSPs to provide information in response to the ACMA's request for further information within 21 days of the date of the request.

Subsection 5.8(9) requires that the ACMA must decide whether to revoke or not to revoke the approved compliance plan as soon as practicable, after the later of the period in which the ACMA could have asked the CSP or group of CSPs for further information, or if the ACMA requires further information, the end of the period in which the CSP or group of CSPs must give the information to the ACMA.

Subsection 5.8(10) requires that if the ACMA decides to revoke an approved compliance plan, the date of effect of the revocation is the date specified in the notice of the decision that is provided to the CSP or group of CSPs.

5.9 Notice of decisions by the ACMA

Subsection 5.9(1) requires that the ACMA must give written notice of the decision to approve, approve an amendment of, or revoke a compliance plan to the CSP or CSPs affected by the decision as soon as practicable after making the decision.

Subsection 5.9(2) requires that if the ACMA decides not to approve, or approve an amendment of, a compliance plan, or decides to revoke a compliance plan, the ACMA must set out its reasons for the decision made in the notice it provides to the CSP or group of CSPs.

Part 6 — Records

6.1 Carriage service provider to keep records of prepaid mobile carriage services supplied

Subsection 6.1(1) requires a CSP to keep records in relation to each prepaid mobile service supplied by the CSP. The records must be sufficient to enable the CSP's compliance with the Determination to be readily ascertained.

Subsection 6.1(2) requires the CSP to keep the records for as long as the service is activated.

6.2 Records for certain transactions

Subsection 6.2(1) requires CSPs to keep additional records in relation to a prepaid mobile service when the CSP has complied with section 4.4 in relation to a purchaser and the prepaid mobile service was purchased using a credit or debit card.

Subsection 6.2(2) requires the CSP to keep records that link the credit card or debit card to the carriage service number for the prepaid mobile service that has been purchased. The CSP has discretion as to how to record this number, depending on the circumstances. The note to section 6.2 suggests as an example that a transaction code generated in relation to the purchase of a prepaid mobile service using a credit card or debit card could be linked to the carriage service number of the service for the purpose of keeping a record required by subsection 6.2(2). Alternatively, if the CSP is required to record the credit card number in relation to the prepaid mobile service as part of its data retention obligations under Part 5-1A of the TIA Act, it could link the credit card number to the carriage service number. Part 5-1A of the TIA Act imposes strict controls on CSPs to ensure the confidentiality of information by requiring that the information is encrypted and protected from unauthorised interference or unauthorised access.

6.3 Record of compliance arrangements

Section 6.3 requires a CSP who supplies a prepaid mobile service to keep a written description of the arrangements that it has in place to comply with the Determination.

6.4 Restrictions on the recording and keeping of certain information

Subsection 6.4(1) restricts a CSP from recording and keeping the identifying number of a government document or a category A or category B document.

Subsection 6.4(2) provides that a CSP may record and keep the identifying number of a government document, or a category A or category B document in circumstances where it is required or authorised to do so by or under a law. The note under subsection 6.4(2) references Part 5-1A of the TIA Act. Under that legislation, CSPs have obligations to retain certain information. Subsection 6.4(2) makes it clear that, in the event that Part 5-1A of the TIA Act requires a CSP to record and keep the identifying number of a government document, or a category A or category B document, the Determination will not prevent it from doing so.

Subsection 6.4(3) provides another limited exception to the prohibition in subsection 6.4(1). Relevantly, the provision will not prohibit the recording of a government document for a "permitted purpose"; so long as the information is recorded only for such time as is reasonably necessary for the permitted purpose and where, immediately after the CSP verifies the service activator's identity, the CSP destroys the information where the recording is not otherwise prohibited by law.

The term "permitted purpose" is defined in subsection 6.4(5) to mean the purpose of verifying the identity of a service activator in accordance with section 4.5, or any other purpose which is ancillary or incidental to the provider's obligation to verify the identity of a service activator in accordance with section 4.5.

Subsection 6.4(3), and the definition of "permitted purpose" specifically, have been included to recognise that some IT systems used by CSPs may, in the course of the identity-checking process, record the identifying number of a government document for a temporary period. However, under paragraph 6.4(3)(c), a CSP that records the identifying number of a government document must, immediately after the CSP has verified the service activator's identity, destroy the number.

Subsection 6.4(3) recognises that CSPs may need to record the identifying number of a government document temporarily to "troubleshoot" – or assist – any customers that are experiencing difficulty in verifying their identity using the "Government online verification service" method at item 1 of Schedule 1.

Schedule 1 — Approved methods for verification of the identity of a customer who is a service activator

Schedule 1 describes the approved methods of identity verification in relation to a customer who is a service activator. A CSP must use one of these methods to verify the identity of a service activator, as required by section 4.5. The CSP must record the method that it uses to verify the identity of a service activator.

Item 1 – Government online verification service

The method described at item 1 of Schedule 1 sets out the process relating to a "Government online verification service" (for example, the Document Verification Service (**DVS**) managed by the Attorney-General's Department).

A CSP is taken to have verified the identity of the service activator if the service activator provides the requisite information from a government-issued document, the information is verified on the government online verification service, and the CSP records the method of identity verification as "government online verification service". Examples of government documents include a driver's licence, a Medicare Card or a passport. Depending on which document is provided, the CSP may be required to seek additional information such as an expiry date or date of birth.

When the DVS is used for the purpose of verification, it will confirm to a CSP that the details on a government identity document match records held by the government authority that issued it. The DVS checks if the details are still valid and not expired or cancelled. If the details come back as matched, then the CSP is taken to have verified the identity of the customer.

Item 2 – Existing post-paid account

The method described at of item 2 of Schedule 1 is the "Existing post-paid account" method. A CSP using this method to verify the identity of a service activator must confirm the details of an existing account for a post-paid service with the CSP. This may include a landline, post-paid broadband internet account or a post-paid telephone service. The CSP will seek the details of an existing post-paid account from the service activator such as the account number or telephone number. The CSP will also seek information that will help it determine that the service activator is the account holder, such as a password for the account. The CSP is taken to have verified the identity of the service activator when it determines that the post-paid account exists and that it belongs to the service activator and the CSP records the method of identity verification as "existing post-paid account".

Item 3 – White listed email service

The method described at item 3 of Schedule 1 is the "White listed email service" method. This method requires the CSP to confirm that the service activator holds an email address ending with ".edu.au" or ".gov.au". These email addresses are deemed to be trusted. Once the service activator provides details of a white listed email service, the CSP will send an email to the white listed email service containing instructions for the service activator to follow in order to determine if the white listed email service is active. Once the CSP determines that the account is active and the CSP records the method of identity verification as "white listed email service", the CSP is taken to have verified the identity of the service activator.

Item 4 –Real-time financial transaction

The method described at item 4 of Schedule 1 is the "Real-time financial transaction" method. This method requires the CSP to obtain the details of an existing specified financial account (an account with an authorised deposit-taking institution (**ADI**) or a licensed credit provider) from the service activator in their name. The CSP will use the details of the specified financial account to make a financial transaction to the service activator's financial account to determine if the account is active. The CSP must not financially disadvantage the service activator when so doing.

Transactions that are made in real-time are transactions that financial institutions respond to immediately, so the CSP is not subject to a waiting period. The CSP will receive confirmation that an account is active as soon as the transaction has been processed. A credit card transaction is an example of a real-time financial transaction.

After receiving a transaction code at the time of making the financial transaction confirming that the account is active and recording the method of identity verification as "real-time financial transaction", the CSP is taken to have verified the identity of the service activator.

Item 5 –Time-delayed financial transaction

The method described at item 5 of Schedule 1 is the "Time-delayed financial transaction" method. This method requires the CSP to obtain the details of an account with an ADI or licensed credit provider from the service activator in their name. The CSP will use the details of the specified account to make a nominal transaction to the service activator's financial account by way of account transfer to determine if the account is active. The CSP must not financially disadvantage the service activator when so doing.

After receiving a transaction code at the time of making the nominal transaction, the CSP will arrange for temporary activation of only one prepaid mobile service for a period of two business days. During that time, the nominal transaction should be processed and, if the account does not exist or cannot be confirmed, the transaction will be rejected or refunded and notified to the CSP's account. The CSP may confirm that the account is active if, during that time, the transaction is not rejected or refunded. After recording the method of identity verification as "time-delayed financial transaction", the CSP is taken to have verified the identity of the service activator. If the CSP does not confirm within two

business days that the service activator's account is active, it must deactivate the temporarily activated service within one calendar day.

Item 6 – Existing eligible prepaid (other) account (no direct debit arrangement in place)

The method described at item 6 of Schedule 1 is the "Existing eligible prepaid (other) account" method. An eligible prepaid (other) account is an account held by a service activator with a CSP for the supply of an eligible prepaid (other) service. Such a service is an activated prepaid mobile service supplied by a CSP to a service activator and has the following characteristics:

(a) it has been activated for 24 months or less from the time of activation;
(b) the CSP complied with section 4.5 in relation to the activation of the service by verifying the identity of the service activator using a method of identity verification other than that in item 6 of Schedule 1; and
(c) it is not an eligible prepaid (direct debit) service.

A CSP using this method to verify the identity of a service activator must confirm the details of an eligible prepaid (other) account with the CSP. The CSP will seek the details of an eligible prepaid (other) account from the service activator such as the account number or telephone number. The CSP will also seek information that will help it determine whether the service activator is the account holder, such as a password for the account.

The CSP is taken to have verified the identity of the service activator:

(a) when it determines that:
    (i) the eligible prepaid (other) account exists;
    (ii) the eligible prepaid (other) account belongs to the service activator; and
    (iii) activation of the service will not result in the service activator having five or more prepaid mobile services activated using the "Existing eligible prepaid (other) account" method for identity verification; and
(b) records the method of identity verification as "eligible prepaid (other) account".

Item 7 – Existing eligible prepaid (direct debit) account (direct debit arrangement in place)

The method described at item 7 of Schedule 1 is the 'Existing eligible prepaid (direct debit) account' method. An eligible prepaid (direct debit) account is an account for an eligible prepaid (direct debit) service which is an activated prepaid mobile service supplied by a CSP to a service activator where the CSP:

(a) has complied with section 4.5 in relation to the activation of the service; and
(b) has a direct debit arrangement in place with the service activator using the service activator's specified financial account.

A CSP using this method to verify the identity of a service activator must confirm the details of an eligible prepaid (direct debit) account with the CSP. The CSP will seek the details of an eligible prepaid (direct debit) account from the service activator such as the account number or telephone number. The CSP will also seek information that will help it determine whether the service activator is the account holder, such as a password for the account. The CSP is taken to have verified the identity of the service activator when it determines that the eligible prepaid (direct debit) account exists and that it belongs to the service activator and records the method of identity verification as "eligible prepaid (direct debit) account".

Item 8 – Visual identity document check

The method described at item 8 of Schedule 1 is the "Visual identity document check" method.

Subject to subitem 8(6), if the activation of the prepaid mobile service will not result in the service activator having five or more activated prepaid mobile carriage services, the service activator must show the CSP either:

(a) 1 category A document identifying the service activator; or
(b) 2 category B documents, each of a different kind, identifying the service activator.

Subject to subitem 8(6), if the activation of the service will result in the service activator having five or more activated prepaid mobile services, the service activator must show the CSP either:

(a) 2 category A documents, each of a different kind, identifying the service activator; or
(b) 1 category A document and 2 category B documents, each of a different kind, identifying the service activator.

Category A and B documents are identified in section 1.8.

Subitem 8(6) states that if a service activator shows a category A document that is a foreign military ID card, the service activator must show the document to the carriage service provider in an access-controlled defence site.

A CSP is taken to have verified the identity of the service activator if the CSP:

(a) confirms whether the activation of the service will result in the service activator having 5 or more activated prepaid mobile carriage services and then follows the applicable visual identity document check requirements depending on the number of services to be held by the service activator; and
(b) is satisfied that if a document shown to it by the service activator includes an expiry date, the document has not expired; and
(c) immediately activates the prepaid mobile service; and
(d) records the method of identity verification as "visual identity document check".

Attachment B

Statement of compatibility with human rights

Prepared by the Australian Communications and Media Authority under subsection 9(1) of the *Human Rights (Parliamentary Scrutiny) Act 2011*

Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017

Background

Subsection 99(1) of the *Telecommunications Act 1997* (the **Act**) provides that the Australian Communications and Media Authority (**ACMA**) may make written determinations setting out rules that apply to service providers in relation to the supply of either or both specified carriage services or specified content services, which are called service provider determinations. Subsection 99(3) of the Act provides, relevantly, that the ACMA must not make a service provider determination unless the determination relates to a matter specified in the regulations.

The relevant enabling regulations are the *Telecommunications Regulations 2001* (**the Telecommunications Regulations**).

Regulatory arrangements for prepaid mobile carriage services (**prepaid mobile services**) have been in place since 1997. The requirements were put in place to inhibit the use of anonymous prepaid mobile services, so that law enforcement and national security agencies can gain accurate information and evidence about users, should they need to do so.

The *Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017* **(the Determination)** revokes and replaces the *Telecommunications (Service Provider – Identity Checks for Prepaid Public Mobile Carriage Services) Determination 2013 (***the 2013 Determination***)* with modifications to improve the efficiency and effectiveness of the identity-checking arrangements for prepaid mobile services.

The Determination sets out the regulatory framework for the provision of prepaid mobile services.

Unless an exemption applies under Part 3 of the Determination, a carriage service provider (**CSP**) who supplies a prepaid mobile service to a person (the customer), must not activate the service unless the CSP has obtained certain identifying information about, and verified the identity of, the customer in accordance with:

- the rules set out in Part 4 of the Determination; or
- a compliance plan that has been approved by the ACMA under Part 5 of the Determination.

The Determination aims to:

- assist law enforcement and national security agencies (**the relevant agencies**) in identifying customers of prepaid mobile services for the purposes of their investigations by ensuring that carriage service providers (**CSPs**):
    - obtain and record specified information about those persons; and
    - if necessary, verify the identity of those persons;
- protect the privacy of individuals by ensuring that CSPs obtain only the minimum amount of information that is reasonably necessary to assist the relevant agencies and by imposing restrictions on the collection, recording and copying of personal information in the identity-checking process; and

- provide CSPs with a range of methods which can be used to verify the identity of customers.

Human rights implications

The ACMA has assessed whether the instrument is compatible with human rights, being the rights and freedoms recognised or declared by the international instruments listed in subsection 3(1) of the *Human Rights (Parliamentary Scrutiny) Act 2011* as they apply to Australia.

Having considered the likely impact of the instrument and the nature of the applicable rights and freedoms, the ACMA has formed the view that the instrument engages the following:

- The right to privacy in Article 17 of the *International Covenant on Civil and Political Rights* (**the ICCPR**).
- The right to freedom of expression in Article 19 of the ICCPR.

Right to privacy

Article 17 of the ICCPR provides:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

Article 17 of the ICCPR (like Article 16 of the *Convention on the Rights of the Child* and Article 22 of the *Convention on the Rights of Persons with Disabilities*) protects the right to freedom from unlawful or arbitrary interference with privacy. Certain provisions in the Determination could be considered to limit the right to privacy. However, the right to privacy is not an absolute right and a limitation is not incompatible with the right itself.

The Determination authorises the collection and use of personal information. However, to the extent that the Determination could be said to authorise an interference with privacy, that interference will be neither unlawful nor arbitrary. It will not be unlawful because the collection, use and destruction of personal information, which is provided for and circumscribed by the Determination, is authorised by the Telecommunications Regulations. It will not be arbitrary because the Determination specifies only the minimum amount of personal information that is reasonably necessary to assist with the legitimate objectives of law enforcement and national security. The Determination also imposes restrictions on the collection, recording, keeping and reproduction of personal information in the identity-checking process.

In addition to those safeguards, Part 13 of the Act is directed at protecting the confidentiality of (among other things) personal information held by CSPs. The disclosure or use of such information is prohibited except in limited circumstances, such as for purposes relating to the enforcement of the criminal law, assisting the ACMA to carry out its functions or powers, or providing emergency warnings. Part 13 also imposes a range of record-keeping requirements on CSPs in relation to authorised disclosures or uses of information. The Information Commissioner has the function of monitoring compliance with, and reporting to the Minister, in relation to these record-keeping requirements, and on whether the records indicate compliance with limitations imposed on disclosure and use of personal information held by CSPs.

Most CSPs are also subject to the *Privacy Act 1988* in relation to the personal information they handle in accordance with the Determination. The Determination is expected to enhance the privacy protections afforded to individuals in the following ways:

- customers of prepaid mobile services are provided with a range of choices about how their identity can be verified; and

- restrictions on the collection, recording and copying of personal information in the identity-checking process are imposed.

These safeguards, together with the other restrictions on the handling of personal information described above, indicate that the Determination is reasonable, necessary and proportionate to the objectives of law enforcement and national security.

Right to freedom of expression

Article 19(2) of the ICCPR (like Article 13 of the *Convention on the Rights of the Child* and Article 21 of the *Convention on the Rights of Persons with Disabilities*) protects the right to freedom of expression, including the right to seek, receive and impart information and ideas through any media of a person's choice. However, this right is subject to certain restrictions, including the protection of national security or public order. Protection of public order includes law enforcement.

Where a CSP prevents the use of a prepaid mobile service (because the CSP has been unable to verify a user's identity) under the Determination, this may affect a person's right to freedom of expression.

One of the objectives of the Act, and the Determination, is to prevent telecommunications networks and facilities from being used in, or in relation to, the commission of offences against the laws of the Commonwealth or of the States or Territories. This objective promotes law enforcement and the prevention of threats to national security.

Requiring persons who use telecommunications networks and facilities to disclose their identity is one basic and crucial way to minimise the risk of telecommunications networks being used in, or in relation to, the commission of offences. It also assists relevant agencies to identify and apprehend persons who do use, or attempt to use, telecommunications networks and facilities in, or in relation to, the commission of offences. The Determination is, in this respect, a reasonable, necessary and proportionate restriction on the freedom of expression.

Furthermore, the Determination is expected to enhance the freedom of expression of certain groups of people by expanding the range of ways in which they can verify their identity to acquire prepaid mobile services. The 2013 Determination included exemption provisions for customers affected by an emergency. These provisions have been enhanced to make it easier for CSPs to be more responsive in an emergency. Additionally, Part 3 of the Determination now allows CSPs to supply prepaid mobile services to victims of family violence where they are unable or unwilling to access their principal place of residence as a result of that family violence. This change will enhance the freedom of expression for victims of family violence. Victims of family violence may otherwise find it more difficult to access a telephone service, at what may be a particularly vulnerable time.

Foreign military identification cards have been included in the Determination as an acceptable form of identification but only when they are shown on an access-controlled defence site. This is because visiting foreign defence personnel, for example, those undergoing joint military exercises with the Australian Defence Force, might not have the requisite documents to meet the identity requirements in the Determination.

Conclusion

This Determination is compatible with human rights. Any interference with privacy is neither unlawful nor arbitrary. The restrictions imposed on freedom of expression are reasonable, necessary and proportionate to give effect to the legitimate objectives of law enforcement and national security.