

**COMMUNICATIONS
ALLIANCE LTD**



**Emergency Call Service Determination -
Proposed amendments to ensure mobile phones
can access the Triple Zero (000) emergency call
service**

COMMUNICATIONS ALLIANCE SUBMISSION

9 OCTOBER 2024

CONTENTS

INTRODUCTION	2
---------------------	----------

SUMMARY	3
Objective of the amendments to the ECS Determination	3
Implementing the amendments to the ECS Determination	3
Denial of access should be on the device, not the service	3
A central “blacklist” of devices is required	4

ISSUES FOR COMMENT	5
---------------------------	----------

1. OBJECTIVES AND REQUIREMENTS OF THE DIRECTION	5
2. Mobile phone definition	6
3. Section 62: Identification of mobile devices that cannot access the emergency call service – new customers	7
4. Section 63: Notification requirements and restriction on supply – new customers	11
5. Section 64: Identification of mobile devices that can no longer access the emergency call service – existing customers	11
6. Section 65: Notification requirements and restrictions on supply when a mobile device can no longer access the emergency call service – existing customers	12
7. Section 66: Requirement to update payment assistance policy	13
8. Section 67: Exception – foreign travellers in Australia	14
9. Feasibility and cost	15
10. Additional/preferable requirements	16

INTRODUCTION

Communications Alliance (CA) welcomes the opportunity to provide this submission in response to the ACMA consultation on the *Emergency Call Service Determination - Proposed amendments to ensure mobile phones can access the Triple Zero (000) emergency call service*.

CA understands the *Australian Communications and Media Authority (Emergency Call Service Determination) Direction 2024*¹ (Ministerial Direction) requires ACMA to amend the *Telecommunications (Emergency Call Service) Determination 2019* (ECS Determination), which has led to this consultation on the proposed *Telecommunications (Emergency Call Service) Amendment Determination 2024 (No. 1)* (Amendment Determination).

Communications Alliance

Communications Alliance is the primary communications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, platform providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to be the most influential association in Australian communications, co-operatively initiating programs that promote sustainable industry development, innovation and growth, while generating positive outcomes for customers and society.

The prime mission of Communications Alliance is to create a co-operative stakeholder environment that allows the industry to take the lead on initiatives which grow the Australian communications industry, enhance the connectivity of all Australians and foster the highest standards of business behaviour.

For more details about Communications Alliance, see <https://www.commsalliance.com.au>.

¹ <https://www.legislation.gov.au/F2024L01103/asmade/text>

Summary

Objective of the amendments to the ECS Determination

CA understands the intent from the Minister for Communications is to cease the supply of all carriage services to mobile phones that are known not to be able to access the emergency call service.

The Carriers that operate mobile networks (Mobile Network Operators or MNO's) continue their work to implement this intent.

As industry has been working through the intent, there are several implications that have emerged from examination of the draft Amendment Determination.

This submission expands on these issues, which include:

- regarding the requirement to ascertain a device's camp-on capability, time is required to formalise an ongoing device testing regime before the requirement to deny access to devices that cannot camp-on to an alternate network comes into force;
- the potential for a public register of mobile phones that do not meet the proposed changes to the ECS Determination ("blacklist") to be managed by the ACMA; and
- concerns with the ability to implement the exception for international visitors.

Implementing the amendments to the ECS Determination

As we outline in more detail in the answers to the ACMA's consultation questions, MNOs and CSPs will not be aware of the device a customer is using (or planning to use) until that device attaches to the network. This is due to the ability of customers to bring their own devices (BYOD) on many plans available in the market. This means the MNO or CSP cannot assess which mobile phones to deny network access to (i.e. cease offering all carriage services) in advance of the mobile phone attaching to the network (i.e., "before supplying a carriage service"). While it is possible to deny network access once the device has attempted to attach to the network, this has implications for the customer experience, as they may have only just purchased a mobile plan, only to discover at that point that the device they plan to use is unacceptable.

Denial of access should be on the device, not the service

CA understands the intent of the proposed amendments is to ensure consumers are unable to use their mobile phone where that phone has been identified as being unable to access the emergency call service. The amendments specify that this should be done by ceasing the supply of all carriage services to mobile phones that are known not to be able to access the emergency call service. However, there may be other technical solutions that can result in the user not being able to access the emergency call service which is the same effect as ceasing the supply of the carriage services. For example, device blocking has the same result in that the consumer is not able to use their mobile phone. This is also a better solution as the consumer can then immediately start using the service as soon as they swap their SIM to a compatible phone which is a better customer experience than having to contact their provider and reactivate their service. Ostensibly, this delivers the intention of the proposed

amendments, namely, that people with a device that cannot make an emergency call are denied the ability to use that device at all.

This is important, because if denial occurs at the service level, there are two critical consequences:

1. Deactivation or suspension of *the service* requires the service to then be reactivated once the end user has obtained a replacement phone, so they can resume using the service. On the contrary, if the *device* is denied access to the network (blocked), as soon as the end user puts their existing SIM/eSIM in a new device that does support emergency calling, they are fully operational.
2. As noted above, MNO's and CSPs only become aware of the device a customer is using (or planning to use) once that device attaches to the network. Thus, for a CSP (i.e., MVNO) to deny access to the service, the MNO would firstly have to inform the CSP that their customer is using a device that is not capable of accessing the emergency call service, and then the MNO would have to deactivate the service. Resumption would also follow the same convoluted path, where the MNO would have to inform the CSP that the device their customer is now using to attempt to attach to the network is ok, so the CSP can remove the suspension on the service.

Communications Alliance members consider the amendments should be drafted flexibly so that other solutions that have the same effect as ceasing to supply the service (i.e. that the consumer cannot use their mobile phone) can be implemented.

A central "blacklist" of devices is required

MNOs currently have in place arrangements to share information with each other about mobile phones that are identified as not supporting access to the ECS. A publicly available list/register of mobile phones should be formalised to capture mobile phones that are known to be unable to access the emergency call service, either whilst the customer is on their home network, or camped-on to another operator's network - a so-called "blacklist" of unacceptable devices. This would also allow Australian MNOs and CSPs to be aware of devices they should not sell and would allow consumers who choose to purchase their own device through online channels (BYOD) to know which devices they should not purchase.

CA members expect further work will be needed on longer term arrangements regarding independent testing and maintenance of an independent register/list of devices.

This suggested "blacklist" of mobile phones would require:

- management by the ACMA, as an independent, technical regulator;
- it to be publicly available, so the public can inform themselves about the status of their own mobile phone model;
- a dynamic register, that gets updated, if/when a device is identified as no longer being able to access the emergency call service, or as network capabilities change;
- time to develop, populate and test the implementation, processes and training around the use of such a register; and
- future proofing, for example 4G networks will cease operation many years from now to make way for an expansion of 5G and 6G services, and like mobile phones now that only operate on a 3G network, there will be mobile phones that only operate on a 4G network, that have been an approved device for years but will have to change status, to move onto the register of blacklisted mobile phones.

Issues for comment

1. Objectives and requirements of the direction

Question 1: Do the proposed amendments to the ECS Determination fulfil the objectives and content requirements of the direction? If not, please explain why, and describe any alternative or additional approaches that could be used to meet the objectives and requirements of the direction.

CA believes ACMA has done a commendable job of trying to fulfil the objectives and content requirements of the Ministerial Direction in order to finalise the amendment to the ECSD. That said, we have three key, overarching recommendations for the ACMA's consideration in drafting the amendment to the ECS Determination.

Firstly, we consider the Amendment Determination should only apply to a standard telephone service (STS) which is used to access the emergency call service (ECS), and not to *all* carriage services.

The reasoning for this is:

- (i) the inherent relevance of mobile phones in the Ministerial Direction means it applies to calls to emergency service numbers (ESNs) 000 and 112. This is because communication via the only other ESN (i.e. 106) is for teletypewriters (TTYs) and mobile networks are not set up to carry the Baudot codes used by TTYs over the air interface.
- (ii) the applicability to calls to ESNs 000 and 112 means the Ministerial Direction is intended for voice communications only, as there is no arrangement for other communication methods like SMS to 000.
- (iii) the applicability to voice communications makes it appropriate to focus the Amendment Determination on the STS, and not block all carriage services as currently worded as the non-voice carriage services are not relevant to ECS access.

A second overarching clarification is that the **denial of access** to an STS (or as the Amendment is currently drafted, to a "service" or "carriage service") should be at the device level, not at the service level. This is important, because if denial occurs at the service level, there are two critical consequences:

1. Deactivation or suspension of *the service* requires the service to then be reactivated once the end user has obtained a replacement phone. In practice what this means is the end user will need to contact their service provider (not using either their old or new phone because the service is deactivated). This will result in a frustrating customer journey. On the contrary, if the *device* is denied access to the network (blocked), as soon as the end user puts their existing SIM/eSIM in a new device that does support emergency calling, they are fully operational.
2. Where the service is supplied to the customer by a CSP (MVNO), the MNO is not able to suspend/deactivate "the service"; only the CSP can. As we set out later in this submission, MNOs, *but not* MVNOs, can identify devices where the make/model has previously been identified as not being able to make emergency calls. In combination, these two limitations mean that if the ECS Determination is amended to require the suspension/deactivation of a service, there is a very convoluted process whereby the MNO would first have to identify the end user is attempting to use a device identified as not being able to make emergency calls, then the MNO would have to inform the MVNO who would then suspend the service. There is no automated notification of this information; it is done on an ad hoc basis, meaning

some end users may experience a delay before being denied a service, whereas others may be denied a service far more quickly.

The amendments should be drafted flexibly so that other solutions that have the same technical or operational effect as ceasing to supply the service (i.e. that the consumer cannot use their mobile phone) can be implemented. We note the Minister's Direction provided the ACMA with discretion to define any terms not defined in the Direction.

Thirdly, for "new customers", as contemplated by s.62 and s.63 of the draft Amendment, flexibility needs to be included in the amendments as where a consumer has not purchased a mobile handset from an MNO/CSP, it is not possible to determine whether the handset can access the ECS *prior* to the end customer being supplied a service. As we explain in response to Q7 and Q8, a mobile network operator will become aware of the mobile phone an end user is using only after the device has attached to the network, not before. Therefore, it is not possible for either an MNO or MVNO to prevent the supply of a service in advance of the device being known; the only possible customer journey is where the customer purchases, activates (including prepaid verification checks) and *pays* for the service, and then once the mobile phone they're planning to use connects to the network, will it be known what that device is.

Absent consideration and adoption of a flexible approach to address these three key recommendations, CA believes the Amendment Determination is likely to be unenforceable. Adoption of these recommendations will help meet the intention of the Ministerial Direction. These recommendations are further explored in answers to later questions.

2. Mobile phone definition

Question 2: Is the ordinary meaning of mobile phone sufficient noting that the direction does not intend to inadvertently capture other communication devices such as internet of things devices or medical alert devices? If not, please explain what the definition of mobile phone should be and provide reasons.

No, the "ordinary meaning" of mobile phone is not sufficient.

The direction may not intend to "*inadvertently capture other communication devices such as internet of things (IoT) devices or medical alert devices*" but that might still happen.

For example, some smartwatches may be like an IoT device, while other smartwatches, which are not a mobile phone, could be used in making an emergency call to ESN 000 via a mobile phone.

Another example is an eCall service, which allows a vehicle to initiate emergency communication via different methods, all using a public mobile telecommunications service. Some send a SOS message to a call centre that initiates an out of area emergency call to ESN 000. Others initiate a voice call directly to ESN 000.

Therefore, it would be helpful to clarify the Amendment Determination with a definition for mobile phone.

CA suggests a definition for "mobile phone" could be something like:
"*... mobile phone means customer equipment capable of voice communications when connected to, or intended for, use in connection with a standard telephone service using a mobile network. For clarity, it excludes devices such as Internet of Things (IoT) devices, smartwatches, medical alert devices and fixed broadband gateways capable of using a mobile network as an interim back-up solution.*"

3. Section 62: Identification of mobile devices that cannot access the emergency call service – new customers

Question 3: Can a carriage service provider currently identify whether the mobile phone that a customer proposes to use to access its network is configured to be able to access the emergency call service before service is supplied to that mobile phone?

Where a consumer has not purchased the mobile phone handset from the provider that answer to this question is no. In answering this question, a **Carriage Service Provider (CSP)** can be considered to be a Mobile Virtual Network Operator (MVNO) who sells mobile services (i.e., a mobile plan, possibly in conjunction with a mobile phone or other device), but does not operate a mobile network. A **Carrier** is the MNO.

Section 62 is potentially unenforceable because there is no way for all CSPs to comply with this requirement. The primary reason is a customer is free to choose the mobile phone they wish to use and therefore the MNO or CSP cannot be certain what mobile phone is in use with a service. In those cases, it is only possible for a MNO or CSP to know the mobile phone a customer is using *once that phone attaches to the network*, i.e., there is a SIM in the phone and it is authenticated onto a mobile network.

While some CSPs sells mobile phone handsets to be used with a service, many CSPs offer a 'SIM only' or a 'bring your own device' (BYOD) service such that the CSP has no visibility of the end user's choice of mobile phone. In those cases, the CSP has no way to identify what device is used with the service. Where the CSP supplies a mobile phone in conjunction with a service, they would know whether the device has been found to be unable to access emergency services if an industry-wide "blacklist" was compiled and made publicly available. This "blacklist" could initially be compiled with assistance from the MNOs, and augmented over time by an independent testing program, such as the one currently being consulted on by the University of Technology Sydney (UTS) (under contract to the DITRDCA). Such a list should be maintained by the Government, and we propose the ACMA would be best placed to maintain this list over time.

Where a n MNO is supplying a mobile phone in conjunction with a service, that MNO would be better placed to identify if their supplied mobile phone can access the ECS on that MNO's network. Where an MNO offers BYOD services, once the phone has attached to the network, the MNO could use the mobile phone's Type Allocation Code (TAC – see answer to Q7 for more details) to determine whether the mobile phone is on a "blacklist".

Question 4: Can providers currently identify whether a mobile phone that a customer proposes to use is configured to be able to access the emergency call service on the mobile networks of other providers before service is supplied to that mobile phone?

See answer to Q3 above in response to the requirement for a device to have authenticated (attached) to a network *before* the make and model can be determined.

Setting aside these timing issues, MNOs do undertake extensive testing of the models of mobile phones that are sold through their owned and operated channels. These testing processes typically include consideration of whether a device can 'camp on' when the handset is in a Limited-Service State. Devices must comply with the relevant Australian Standard which includes access to ECS requirements.

However, for devices that have not been sold through these channels, there is currently no mechanism for a positive determination on whether all makes and models available worldwide are able to camp on.

Industry understands that it is the intention of the Direction to require that MNOs remove from their networks, devices that are currently known not to be able to access emergency call services either via the provider's own network or via an alternative network.

The testing required to identify the capability of handsets beyond those already tested by the MNOs directly, is currently being consulted on by the University of Technology Sydney (UTS) (under contract to the DITRDCA). Over time, this testing will identify those additional devices that are unable to camp on. As above, the ACMA should maintain a register of such devices.

The policy intention and the ongoing testing work can be better reflected in s63 and s65 of the Amendment Determination by requiring action by a service provider when it "becomes aware" that a mobile phone is not able to access emergency call services. This would replace the current 'has identified' wording. 'Becomes aware' can also allow for situations where a mobile phone configuration is identified via MNO testing or advised by a manufacturer.

Question 5: If the answer to either of Questions 3 and 4 is no, what additional information would be needed to give effect to such a requirement? Is that information currently available?

Additional information is not available and will not "give effect to such a requirement" because a CSP has no way to know what mobile phone an end user chooses to use.

As noted above, the UTS testing process will provide further information on handsets not directly tested by MNOs. We have proposed wording above that will enable the ongoing results of this testing process to flow through into action by MNOs under the ECS Determination.

Question 6: If a mobile phone is configured to be able to access the emergency call service using both the network of the carriage service provider supplying carriage service to it, and the networks of other providers supplying carriage services to the public, can a carriage service provider that is supplying service to the mobile phone identify whether that mobile phone will 'camp-on' to another network if required? If not, please explain why and indicate what additional information would be required to enable a carriage service provider to identify the 'camp-on' capability of a mobile phone.

No. As covered in response to earlier questions, a CSP cannot know what mobile phone an end user chooses to connect to a carriage service and therefore cannot identify the 'camp-on' capability of a mobile phone used to access the ECS.

In addition, there is no obligation for an end user to:

- (i) inform their CSP of which mobile phone the end user intends to use, and
- (ii) update the CSP any time they choose to use a different mobile phone.

As noted above there is currently a consultation underway by UTS for testing requirements to assist MNOs in identifying the 'camp-on' capability of mobile phones. An ACMA administered and published "blacklist" of mobile phones that have been tested and are known to be unable to 'camp-on' would enable service providers to take action based on the results of this testing process.

Question 7: What information do (or can) providers know about a mobile phone when it has connected to a provider's network?

Once a mobile phone has connected to a mobile network, the International Mobile Equipment Identifier (IMEI) of the device can be identified. The first eight digits of the IMEI are the Type Allocation Code (TAC), which is a unique code to the make and model of the device. Using the TAC, an MNO can look up the capabilities of the device in a database, for example, the GSMA TAC database,² or once established in Australia, a "blacklist" of devices known to be incapable of accessing the emergency call services on any of the networks (either directly or via camp on).

Two key elements the GSMA database does not contain are: 1) whether the device is configured to fall back to a 2G or 3G network to make emergency calls (known as "Circuit Switched Fall Back", or CSFB); and 2) Whether the device is able to camp-on to other mobile networks (other than its home network) when in Limited Service State. On the second point, while device manufacturers will claim compliance with GSMA IR.92,³ given the raft of permutations of device and network configurations, the only way to be sure that a device will successfully camp-on to make an emergency call, is through individual device/network combination testing.

Question 8: Can providers:
(a) identify the make/model number of a mobile phone once it has connected to its network?
(b) share information with each other to identify mobile phones that cannot access the emergency call service on mobile networks?

While an MNO can identify the make/model of a mobile phone *once* it is connected to the network, this information is not available to a CSP / MVNO selling mobile services on top of a mobile network. This is because the identity (TAC) of the mobile phone associated with a mobile service is not currently delivered to CSPs / MVNOs.

An MNO receives the IMEI of the mobile phone as a usual part of attaching to or registering on the MNO's mobile network. The MNO can use the TAC (in the IMEI) to identify the make/model (using the TAC) of a mobile phone once it has connected to its network.

Note that an IMEI is potentially personally identifiable information and sharing it with other entities might be subject to obligations in the *Privacy Act*. However, TAC information can be shared with the ACMA for the purposes of creating an industry-wide "blacklist" of devices known to be unable to access the emergency call services on networks.

This blacklist can be progressively updated with the results of further testing undertaken either directly by the MNOs or via the UTS testing work. This "blacklist" would be used by service providers to ensure ongoing compliance with the ECS Determination.

² GSMA Type Allocation Code (TAC) database: <https://www.gsma.com/solutions-and-impact/industry-services/device-services/gsma-device-attribute>

³ GSMA IR.92, ver 20.0. https://www.gsma.com/newsroom/gsma_resources/ir-92-ims-profile-for-voice-and-sms-20-0/

Question 9: Based on information that is available or will be available to providers on 1 November 2024, indicate the number or proportion of mobile phones to which providers currently supply service, that providers may no longer be able to supply service to because of the requirements in the draft amendments to the ECS Determination. Please explain your response indicating which provision/s is relevant to your answer.

This information has already been provided to the government outside this consultation process.

Question 10: What are the minimum reasonable steps that a carriage service provider should take to identify whether a customer's mobile phone can access the emergency call service on their network and the networks of other carriage service providers?

Consistent with answers to earlier questions, a CSP has no way of knowing "*whether a customer's mobile phone can access the emergency call service*". Other than information supplied by the MNO to the CSP, CSPs have no visibility of the device (make / model) that their customer is using. Transfer of information from an MNO to a CSP is done using a static list on an ad-hoc basis and is only accurate at the point in time when the list is compiled. End users periodically replace devices, meaning the list "ages" quickly and becomes inaccurate. Indeed, if an MNO supplied a CSP with a list of devices that are known not to be able to make emergency calls, and the CSP actioned that list by contacting their customers asking them to change their phone, then the list could reasonably be predicted to "age" very quickly, as customers replace their phones.

Taking this lack of visibility of the device a CSP's end user customer is using in the context of blocking access to a mobile service, it is important to understand that this lack of visibility also means the CSP will not know when their end customer has been blocked from accessing the network. The mechanism that will be used to deny an individual person (an "end user") access to a mobile network can only be **implemented at the network level**. Devices that attempt to attach to a mobile network can be assessed (using the device's TAC) against a "blacklist" of devices (known to be unable to make emergency calls, including camp-on calls), and if the device's TAC is on a known "blacklist", then it is possible to block the device, using one of a few different mechanisms to deny access.

A CSP selling a mobile service on top of a mobile network will have absolutely **no visibility** that the device their customer is using has been blocked.

Once blocked, the end user cannot use that device to contact their service provider (or anyone else for that matter) by voice, text or data (i.e., they cannot look up information on the service provider's website, because the device is blocked from attaching to the network).

The CSP cannot do anything to improve the existing process. CSPs, and to a large extent, MNOs as well, will simply have to field calls from their customers (using something other than their blocked phone) and "piece together" what has occurred.

4. Section 63: Notification requirements and restriction on supply – new customers

Question 11: Should any groups of carriage service providers be exempt from the obligations? Or should there be different obligations on certain sub-sets of carriage service providers? If so, please explain.

Yes. Section 63 is potentially unenforceable because, consistent with answers to earlier questions, a CSP cannot identify a mobile phone under s63(1) which means s63(2) is not applicable.

If the Amendment Determination is not updated, any CSP that only offers "SIM only" or BYOD services should be exempt because an implicit part of the service offering is that an end user chooses their mobile phone independently of the CSP, so the CSP will have no knowledge of the mobile phone an end user may prefer to use.

5. Section 64: Identification of mobile devices that can no longer access the emergency call service – existing customers

Question 12: Can a carriage service provider identify whether a mobile phone that it is supplying carriage services to can no longer access the emergency call service? If not, what, if any, additional information would providers need to identify such phones?

Section 64 is potentially unenforceable because, consistent with answers to earlier questions:

- A CSP cannot "identify whether a mobile phone that it is supplying carriage services to can no longer access the emergency call service"; and
- Additional information would not help CSPs to identify such phones because it is the MNO that identifies the mobile phone through the IMEI once the phone attaches to the network.

An MNO may be able to identify that a mobile phone can no longer access the ECS on its own mobile network, but the existing drafting of s64 may have unintended consequences.

Scenarios where a mobile phone can no longer access the ECS on its home mobile network include:

- Permanent cessation of certain network function(s) e.g. closure of a 3G mobile network.
- Temporary lack of network function(s) that may be within control of the MNO e.g. planned maintenance or upgrades.
- Temporary lack of network function(s) that may not be within control of the MNO e.g. natural disasters.
- End user action that means a mobile phone is unable to maintain an attachment to a mobile network, including:
 - Changing the configuration of the mobile phone to 'flight mode' to comply with CASA obligations⁴
 - Driving in a rural or remote area with inconsistent mobile coverage,
 - Entering an area with no mobile coverage e.g. an underground carpark, in a national park

⁴ <https://www.casa.gov.au/operations-safety-and-travel/consumer-and-passenger-advice/onboard-passenger-safety-and-behaviour/using-your-electronic-devices-flights>

- Powering off the mobile phone e.g. to conserve phone battery charge.

The proposed wording of s64 currently makes no distinction in relation to the above scenarios.

Given the urgent timeframe in the Ministerial Direction for implementation by 1 November 2024, which is close to the rescheduled shutdown date for 3G networks of 28 October 2024, it would appear that the policy intent is for this obligation to apply to the first scenario i.e. permanent cessation of certain network function(s), like the closure of a 3G mobile network.

CA submits that ACMA should amend the wording of s64 accordingly to avoid possible unintended consequences.

6. Section 65: Notification requirements and restrictions on supply when a mobile device can no longer access the emergency call service – existing customers

Question 13: Does this raise any issues for end-users that should be considered?

Yes, there are a number of potential consequences that should be considered, although these are best addressed by the CSP when engaging with their Customers. The CSP will have knowledge of the preferred method of communication for Customers and other matters which may need to be considered when contacting them (e.g. financial hardship, Domestic and Family Violence etc).

The notification requirements should be flexible and non-prescriptive to allow CSPs to tailor them in various situations.

The note to subsection 65(3) (that “The information in subsection (3) could be provided via a link in the notification”) should also be removed. It does not add any value as CSPs again will be placed to consider how to contact their Customers.

The note in itself is of concern because this may open a new avenue for scammers to imitate notifications and send malicious false messages that prey on end users fear of cessation of service.

More broadly regarding the restriction of service, we have concerns regarding the intersection of blocking a service and the obligations provided under Financial Hardship and to victims of Domestic Family Violence.

Question 14: Is the rolling set of notifications to ensure that end-users have sufficient time to change mobile phones before their services are disabled appropriate? If not, why not?

Regardless of the duration afforded to consumers to upgrade or change devices, some consumers will leave it to the last minute. So, we recommend a short period of time, and note that many customers who are served notice under the proposed s.65 of the Amendment Determination, will still wait until after their device has been denied access to the network before they take any action.

Question 15: Should any other information be included in notifications to help the end-user to prepare for the disabling of their carriage services and prompt them to action?

There is no additional information that we can think of at this time.

Question 16: Noting that the disabling of service to an end-user's mobile phone will require the end-user to obtain another mobile phone, do providers have any data available or information relevant to the assessment of the likely cost of this requirement to end-users of mobile services?

Cost for end users will vary between different CSPs. Costs are also commercially sensitive information, so it is not shared with CA.

Please refer to individual submissions from CA members.

Question 17: Should the Determination specify the acceptable forms of notification, or leave this undefined to provide flexibility to carriage service providers to determine appropriate methods of notification?

The prior experience of unintended consequences of direct regulation (e.g. the Financial Hardship Standard preventing culturally appropriate practices) is evidence that the Amendment Determination should leave undefined the acceptable forms of notification.

7. Section 66: Requirement to update payment assistance policy

Question 18: Should any groups of carriage service providers be exempt from the obligations? Or should there be different obligations on certain sub-sets of carriage service providers? If yes, please explain.

Yes. Groups of carriage service providers that should be exempt from the obligations include:

- CSPs that offer 'SIM only' or 'BYOD' services i.e. they do not offer mobile phones.
- CSPs solely providing mobile services to Wholesale, Business, Enterprise and Government organisations where the relationship is directly with the organisation and not with the end user.
- Business to Business CSPs is a sub-set of provider which should be exempt from the obligation.

8. Section 67: Exception – foreign travellers in Australia

Question 19: Are carriage service providers able to confirm that a person requesting the supply of a mobile service is a foreign traveller to Australia and the period of time that such a person may intend to stay in Australia?

No. There are challenges in considering how to deal with international travellers and as currently drafted the exception is not likely to be relied upon because it relies on information not known to MNOs/MVNOs. We believe any provisions regarding international travellers should be drafted flexibly.

There are two categories of foreign travellers with regard to mobile telephones services – those who use their international SIM and roam onto Australian mobile networks and those who purchase a SIM for an Australian mobile network.

When entering Australia, international travellers can continue to use their existing handset and service from their domestic carrier under an international roaming agreement with one of the local service providers.

If a CSP is to rely on a proposed exception in the Determination it could allow for a presumption that these travellers are to remain in Australia for a limited period of time and that, the other provisions of the ECS do not apply. Otherwise, the proposed exception should be drafted flexibly to otherwise support the overarching public safety intent of the amendments and devices be blocked.

The other category of international travellers are those who purchase a local SIM for use in their existing handset. It is currently not possible for local service providers to distinguish these new service requests from those made by Australian domestic residents.

Some CSPs might be able to obtain that information at point of sale e.g. at a retail outlet in the arrivals hall of an international terminal, asking every customer, including those arriving permanently or for a long-term visit. However, in practice this will result in the exception not operating for this category of foreign traveller. There are too many variables in the user journey and providers will not be able to discriminate when it comes to mobile phone blocking if the need arises.

Industry sees an education campaign undertaken by the Government, making travellers aware of Australian mobile phone obligations a better way to educate and inform the overseas market. The Government could also look to see what issues or learnings arose from jurisdictions such as the U.S when they undertook to close down 3G networks.

Question 20: Where a foreign traveller roams on more than one network in Australia, the proposed amendment would require all carriage service providers that handle roaming to comply with the notification requirement. Is this appropriate? If not, why not?

No. CSPs generally do not have a relationship with inbound international roamers. This might be relevant to a small subset of CSPs that offer services to foreign visitors, but, consistent with responses to earlier questions, CSPs do not know what mobile phone an end user may choose to use to connect to a mobile network.

While MNOs in Australia are cooperating to share information about mobile phones in Australia, they cannot know the same information about the mobile phones of inbound international roamers.

Question 21: Should the exception involving foreign travellers in Australia be limited to situations where the carriage service provider is being approached in Australia to supply services? This would exclude the requirements from applying to international roamers. If not, why not?

No, the exception should apply to all international roamers, including international dignitaries on an official Government visit, individuals visiting family or friends, or groups arriving for prearranged tours.

It is worth remembering that like the domestic population where only a small percentage of mobile phones will not be able to make emergency calls once the remaining 3G networks are closed, almost all foreign travellers arriving in Australia with a mobile phone that is capable of international roaming will be able to make an emergency call in Australia. Further, and as discussed in our answer to Q7, it is not possible to identify the type of mobile phone a foreign traveller is planning to use until the device attaches to the network. Thus, it is not possible to identify the small subset of foreign travellers with a mobile phone not capable of making emergency calls until the traveller turns on their phone in Australia.

For international visitors to Australia, a potential unintended consequence of sending foreign travellers notifications and denying access to mobile networks while they are in Australia, may be that every visitor who receives a notification about a low cost or no cost mobile phone will demand a free phone to replace their phone which complies with global technical specifications, and should be expected to function normally in Australia including making emergency calls, but has been denied service because it is a model that is not supplied in Australia and therefore has not been included on a suggested register of 'approved' mobile phones.

Similarly, if not exempted, inbound international roamers would also get the notification that offers low cost or no cost mobile phones even though they might not be expected to qualify under a financial hardship policy

Therefore, we support the exception proposed in s.67, although we note that there are challenges in implementing the exception, due to the difficulty in identifying the small subset of foreign travellers who have a mobile phone that is not capable of accessing the emergency call service.

Question 22: Is the 60-day period for foreign travellers to use carriage services on mobile phones that are not able to access the emergency call service appropriate? If not, why not, and what alternative timeframe would be appropriate?

The practical challenge with using the exception is not the chosen 60-day period, but rather how service providers can understand the travel intention of foreign arrivals. As above, we have proposed a deeming provision for inbound roamers. It is unlikely that the exception will be workable for travellers who purchase local SIM services, regardless of the proposed date range.

9. Feasibility and cost

Question 23: For carriers and carriage service providers, what are the likely costs and benefits of implementation for your organisation? (Please provide specific cost estimates in your response.) Are there alternative ways to achieve the objective of the direction that would be consistent with its terms and provide for lesser costs and/or greater benefits?

Implementation within each MNO and CSP will be tailored to suit the respective organisation's existing systems and processes.

Therefore, the likely costs and benefits for implementation is commercially sensitive information and it is reasonable for them not to share this information with CA.

Please refer to individual submissions from CA members.

10. Additional/preferable requirements

Question 24: The ACMA is seeking feedback on whether there are:

- Additional matters aligned to the objectives that should be included in the proposed amendments to the ECS Determination?
- Matters included in the proposed amendments to the ECS Determination for which alternative arrangements that should be considered?

Please provide evidence to support your position.

There are no additional matters aligned to the objectives that should be included in the proposed amendments to the ECS Determination.

One final item for consideration are phones that support multiple SIMs, including all eSIM capable mobile phones. We note that the Amendment Determination would require each CSP to notify the customer or end user separately, because each CSP cannot know if other CSPs have already informed the customer or end user. Thus, customers with multiple SIMs/eSIMs will receive individual notifications from their respective service providers, which is the correct and relevant approach.



Published by:
**COMMUNICATIONS
ALLIANCE LTD**

Level 25
100 Mount Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507