Kevin Pulo
[redacted]

8 October 2024

The Manager
National Interests Section
Australian Communications and Media Authority
PO 13112 Law Courts
Melbourne Victoria 8010

Dear Sir/Madam,

This is my submission to ACMA's call for public consultation regarding the draft amendments to the Telecommunications (Emergency Call Service) Determination 2019.

My submission relates primarily to Questions 3-12 of the consultation paper. Direct answers to these questions are in a dedicated section.

Summary

My main comment is that the draft amendments implicitly presume that "identifying whether a mobile phone can access the Emergency Call Service (ECS, aka E000)" is something that carriage service providers (CSPs) are able to easily and accurately do - whereas in fact, performing this task accurately is not an easy task for CSPs, and furthermore the 3G shutdown has demonstrated that CSPs are generally only interested in taking the easy approach, and are unwilling to use accurate solutions. Specifically, the easy approach is the heavy reliance on IMEI whitelisting, which has numerous problems that I outline in the details below.

The above presumption of the draft amendments stems in large part from the language used by subsection 6(2) of the "ACMA (Emergency Call Service Determination) Direction 2024" issued by the Minister for Communications on 21 August 2024. I understand that ACMA is obliged to implement the Direction, and is not at liberty to modify or adjust it. However, I believe it is possible and appropriate for ACMA to amend the Emergency Call Service Determination (ECSD) in a way that avoids the below-described problems (which mostly arise from IMEI whitelisting), while still complying with the Minister's Direction. This is by clarifying the meaning of "identify" as it appears in the objectives relating to "identifying mobile phones which cannot access E000".

More specifically, the ECSD should include provisions which acknowledge that different methods of performing such identification have different levels of accuracy, and require CSPs to only use methods with accuracies that meet reasonable community expectations. For example, consider a method which determines that a particular set of handsets cannot access E000, and this is shown to be demonstrably false (for example, by such handsets actually making successful E000 calls). It is likely that a reasonable person would deem such a system to be unacceptably inaccurate, and so for this reason, a method should not be permissible under the ECSD. IMEI whitelisting is an example of such an approach.

Background - IMEI whitelisting and 3G shutdown

The draft ECSD requires CSPs to "identify" whether mobile phones are able to access the ECS. However, due to the extremely diverse landscape of modern mobile phones, and the technical nature and complexities of 4G/5G voice services, making this "identification" at the mobile network layer requires considerable effort.

This *"ECS identification"* is more difficult than determining the 4G VoLTE compatibility of a handset, or *"VoLTE identification"*. During the 3G shutdown, the CSPs have demonstrated that they are unwilling to take the effort to perform VoLTE identification accurately and correctly. Instead, they have taken the significantly cheaper and easier option of relying solely on lists of compatible handset models, as determined by the IMEI - that is, IMEI whitelists.

Using IMEI whitelists for VoLTE identification is a very coarse determination, which can be incorrect in many cases. There are two types of inaccuracies:

- *False negatives* are handsets that can support VoLTE, if correctly configured (including potentially updating the phone's operating system software), but are instead identified as "does not support 4G VoLTE".

- *False positives* are handsets that should support VoLTE (e.g. and perhaps did at launch or purchase), and have been VoLTE identified as "supports 4G VoLTE / will work after 3G shutdown", but in fact cannot make 4G VoLTE calls (e.g. perhaps because handset configuration settings have been changed by the end-user).

The only "solution" provided by the CSPs to false negatives is to replace the handset, which is wrong and wasteful because the handset actually works fine, whereas no solution at all is offered for false positives.

The CSPs could instead use better evidence than IMEI whitelists (e.g. checking for VoLTE provisioning on the service, checking if VoLTE calls have been successfully placed/received by the service, etc), but have chosen not to do so. This is likely because such more accurate methods are more difficult - and therefore more expensive - to implement, making them less commercially palatable.

For end-users in the false negatives group, who have successfully reconfigured their handset to use VoLTE, this is mostly an annoyance of continuing to receive incorrectly notifications telling them that they need a new phone.

End-users in the false positives group are more seriously affected, because they will only discover that their phone isn't actually able to make voice calls after the 3G shutdown, and after having been incorrectly advised by their CSP and/or AMTA that this would not occur.

IMEI whitelisting and ECSD

Returning to the context of the ECSD, this demonstrates that - in the absence of being compelled otherwise - the CSPs are highly likely continue using the coarse IMEI whitelisting approach when making the ECS identification. However, in stark contrast to the 3G shutdown, the outcomes for end-users are much more severe where the ECSD is concerned.

False negative end-users

False negative end-users - that is, end-users who have and are using a device that is 100% functional, including being able to access E000 - will receive notifications from their CSP which incorrectly claim that their handset is unable to access E000, and that their entire service (voice, messaging and data) will be imminently terminated, unless the end-user gets a whitelisted phone model.

The draft ECSD contains no provisions at all for this circumstance. CSPs are not required to have a process for end-users to challenge the accuracy of the CSP's ECS identification, let alone any criteria for what might be considered acceptable proof of a handset's ability to access the ECS. In the absence of such criteria, affected end-users are incentivised to convince their CSP that their handset works and is compliant, including the most obvious demonstration of placing a non-emergency call to E000. This aspect of the draft ECSD is a moral hazard, i.e. while the intention is to improve the ECS, there may be unintended consequences that in fact end up degrading the ECS.

Since all CSPs are bound by the ECSD, if they all use IMEI whitelisting, then moving to a different CSP is not a solution for affected end-users. And, since IMEI whitelisting is relatively cheaper and easier, any CSPs using more accurate approaches will be at a commercial disadvantage, meaning that market forces will incentivise them to switch to IMEI whitelisting, if permitted. Therefore, prohibiting CSPs from using IMEI whitelisting (and similar approaches) is necessary.

False positive end-users

Meanwhile, the draft ECSD achieves nothing for false-positive end-users, who will suddenly be unable to access ECS during an emergency. Clearly there should be provisions which at least incentivise CSPs to minimise the occurrences of this scenario. While no system is perfect, the use of ECS identification methods that are known to be coarse and have significant inaccuracies should be avoided, while there should also be ways for end-users to directly test their own devices (without actually calling E000), and/or a process for CSPs to handle the possibility of incorrect ECS identifications.

Mobile phone usage assumptions

The draft ECSD makes assumptions about how mobile phone handsets are used, which precludes various use cases. For example:

- Using a surplus mobile phone purely as a 4G hotspot (in addition to the end-user's "actual" mobile phone that they use for voice services). Requiring end-users in this scenario to purchase a 4G data-only service would be anti-competitive (see also the anti-competitive section below).

- Using a mobile phone, with a battery that doesn't hold any charge, and so is always plugged into power, and remains next to a landline which has reliable access to E000. (e.g. a business phone number that needs to be maintained.)

In cases such as these, the circumstances are such that there is no actual loss of access to the ECS. This means that completely preventing these use cases (by the ECSD requiring service to be denied or withdrawn) is an overreach.

Only the end-user can know the details of any such mitigating circumstances. Therefore, there should be provisions for end-users to inform their CSP of such mitigating circumstances.

This could also include allowing end-users to opt-out of the E000 requirement for the service, although this might require additional safeguards to ensure that end-users (and not just those who are financial hardship customers) do not opt out of ECS merely to avoid the inconvenience / expense of fixing their current handset or obtaining another handset.

IMEI whitelisting is anti-competitive

If CSPs are permitted to use IMEI whitelists as the basis for ECS access identification, then this will have a significant stifling effect on competition within the market for mobile phones. This is because it would effectively give CSPs complete control over which mobile phone handsets can be used on Australian mobile phone networks. This would clearly be anti-competitive.

For example, CSPs could refuse to offer service for "BYO handsets", instead requiring end-users to purchase a handset from the CSP. This would amount to a government sanctioned form of mandatory network locking, separate from the actual "network locked" status of the handset.

Even a less extreme version of this scenario, where CSPs notionally allow "BYO handsets", but only from a CSP-controlled list of acceptable models, is severely problematic. This is because it prohibits end-users from sourcing and using a handset of their choice that is 100% compatible with the carriers' networks, but isn't on the list of "acceptable models". This needlessly restricts consumer choice and free market dynamics, with flow-on effects such as increasing the barriers to entry for new mobile phone makers, further entrenching the large incumbent manufacturers, increasing prices for end-users, encouraging monopolistic behaviours, etc. This is not in the public interest or the best interests of end-users.

CSPs have no incentive to oppose this increase in market control that they would stand to receive, since they in fact stand only to benefit from it. Therefore, CSPs should be regulated so as to not use IMEI whitelists and similar approaches for ECS identification.

Information provision requirements

The draft ECSD includes requirements for CSPs to provide information about alternative compliant mobile phones.

During the 3G shutdown, the CSPs have used a coarse approach where the only seriously suggested remedy presented to end-users is to buy a new phone (note: the suggestion is usually either to "buy" or other obtain a "new" phone, not merely to "obtain a suitable handset"). No real consideration is given to the possibility of (re-)configuring, (software) upgrading, or otherwise investigating how end-users can make their existing handset compliant with VoLTE.

This has prompted criticisms that the CSPs have treated the 3G shutdown as a way of selling more mobile phones to end-users ("selling more" in the sense of "unnecessarily").

Without some countervailing incentive, the draft ECSD encourages CSPs to continue using only coarse and inaccurate methods for ECS identification, followed by a sales pitch of their own handsets that customers can purchase. Even if end-users are able to obtain and use compliant handsets from a third party, if the CSP messaging is presented poorly, is has the potential to mislead end-users into thinking that a handset from the CSP is required, rather than merely convenient. Again, CSPs are commercially incentivised to behave in this manner. This means that the draft ECSD promotes what basically amounts to a shakedown (and, worse, a government-mandated shakedown under the guise of safety requirements).

ECS testing services

There is currently no way for end-users to test or verify whether their handset is actually able to call E000. This is true irrespective of the details of the mobile phone model, configuration/settings, carrier, or CSP.

The only currently definitive way to know whether or not a particular handset can successfully call E000, is to make an actual ECS call. This is an obvious problem, because doing so during an emergency is not appropriate (because a negative outcome can have dire consequences), and doing it at other times (non-emergencies) is also not appropriate (because it can prevent the ECS from working for actual emergency calls).

The draft ECSD does not address this issue, despite it being central to the question of identifying handsets that cannot call E000. Neither end-users nor CSPs can reliably identify affected handsets without such a testing service. This problem has existed, and the industry has been aware of it, since the initial introduction of 4G and VoLTE. Despite this, the industry in general (mobile phone manufacturers, carriers, and CSPs) have not taken any action to introduce any such end-user accessible testing. As such, it would be appropriate for ACMA in its role as regulator, to add provisions to the ECSD requiring CSPs to establish such a testing service. Some example provisions are listed in the section below.

Due to limitations with how the ECS is implemented at a technical level, it is true that a testing service is not straightforward to achieve (e.g. it is not possible to have a "001" "test emergency" number). However, it is not completely impossible to do this, despite the previous claims of some CSPs (i.e. Telstra).

The issue is mostly that doing this in a safe and reliable way requires more effort (and therefore more expense) than the CSPs are willing to invest. As such, when the CSPs say that this is "impossible", what they actually mean is "not commercially viable", or "not in our commercial interests". However, the whole point of regulation is to force enterprises to adopt practices that may be commercially unpalatable, but nevertheless are outweighed by significant public benefits. Reliable access to the ECS is such a case.

Potential provisions

Basically, CSPs should be very strongly incentivised to use the most accurate methods of ECS identification possible, and disincentivised from using coarse and inaccurate methods.

Unfortunately, the draft ECSD has the exact opposite incentives, where CSPs are rewarded (or at least not punished) for having poor accuracy, while end-users (who have little control, power, or leverage in these matters) must instead bear the full weight of inaccuracies.

The draft contains no concept that CSPs may make inaccurate or incorrect ECS identifications, let alone any provisions for how such situations should be handled, putting end-users at the mercy of the CSPs. Again, the behaviour of CSPs during the 3G shutdown strongly suggests that their approach will be to ignore such inaccuracies, and instead simply attempt to force (i.e. blackmail) affected end-users into purchasing new handsets.

These problems could be alleviated or improved by adjusting the draft ECSD in a variety of potential ways. For example:

ECS identification accuracy related

- Requiring CSPs to use ECS identification methods that meet reasonable community expectations of acceptable accuracy.

- Prohibiting the use of IMEI whitelisting or similar methods of identifying non-compliant handsets.

- Requiring CSPs to provide similar model replacement phones at no cost to the end user (i.e. like-for-like models, as opposed to replacing a high-end with a cheap feature phone).

- Mandating the use of dynamic network monitoring methods of identifying non-compliant handsets (as opposed to static whitelists).

- Specifying that CSPs must provide a process by which end-users can challenge and/or rectify any incorrect ECS identifications.

- Allowing end-users to inform their CSP of mitigating circumstances regarding their access to the ECS.

- Allowing end-users to opt-out of the ECS. This would be similar to the Customer Service Guarantee (CSG) Waivers used by VOIP landline providers. However, as in the earlier section, it could require additional safeguards.

- Providing legal recourse for end-users whose service is terminated or refused by CSPs on the basis of inaccurate or incorrect ECS identification. For example, by making the CSP liable for direct and indirect losses incurred by end-users in such circumstances. (Or, if the ECSD is not authorised for such provisions (due to its status as a regulation), then perhaps by a provision which makes such service terminations/refusals be a breach of the ECSD.)

- Mandatory reporting by CSPs of instances of false positives, i.e. where the CSP incorrectly failed to identify handsets that cannot call E000, and the end-user was unable to place an emergency call as a result. This could also potentially include being a breach of the ECSD, if it resulted from the CSPs use of an inaccurate ECS identification method.

- Mandatory reporting by CSPs of instances of false negatives, i.e. where the CSP identified a handset as being unable to call E000, but this then found to be incorrect. Again, this could potentially be a breach of the ECSD if it resulted from an inaccurate ECS identification method, and/or caused the service to be terminated/refused (when it should not have been).

ECS test service related

- Requiring CSPs to provide an end-user accessible ECS test service on their networks.

- Requiring CSPs to provide detailed technical documentation to end-users, which permits them to verify the correctness of their VoLTE and associated settings.

- Requiring CSPs to develop, produce, acquire, or otherwise provide access to a mobile app which checks that the mobile phone's configuration, settings, and operating system are sufficient for access to the ECS.

- Requiring CSPs to provide (or provide access to) individualised verification services of handset configuration settings. This could be provided in-person for those CSPs with in-store facilities, or by third parties which provide such in-person services, or via video-conferencing facilities.

- Requiring CSPs to provide (or provide access to) in-person actual ECS testing services for handsets. For example, this could be by using a specially-configured femtocell inside a Faraday cage, which would allow the handset to place a test call to E000, but purely simulated within the femtocell, and not by making an actual non-emergency call to the real ECS.

Information provision related

- Requiring the notifications (in sections 63 and 65) to state that they may not be accurate, and providing information about how the end-user can check the accuracy for themselves, and what to do if they find that the ECS identification is incorrect.

- Requiring CSPs to provide information about how end-users can determine - prior to any purchase - the ECS identification or ECS suitability of any arbitrary phone model. This could consist of detailed technical information, but it could also involve the use of a specially developed phone app, which checks and reports on the phone's configuration settings, for example.

- Requiring CSPs to provide information about suitable phones that are commensurate with the features of the customer's existing phone, i.e. it is not helpful to tell a high-end user about basic phones, or a basic phone user about high-end phones. This helps prevent up-selling, where CSPs deliberately only mention phone models that are either incredibly basic (merely to satisfy the "low cost or no cost" provision of draft subsections 63(2)(c) and 65(3)), or more featureful (and expensive) than the user requires.

- Requiring CSPs to provide information about suitable phones that are available from their competitors (including competing CSPs), third party retailers, and second-hand retailers.

Consultation paper questions

- **Questions 3 and 4:** No, currently CSPs cannot identify if a proposed handset will be able to access the ECS prior to connecting to the service (on their own network, or other networks).

- **Question 5:** The only definitive way to currently know if a specific individual handset can access the ECS, is to place a call to the ECS, which is (a) not appropriate for non-emergency situations and (b) not possible prior to the device being connected to the network. However, as per my provision suggestions above, there are technical ways that CSPs could achieve this, but they require investment that, to date, has not been undertaken.

- **Question 6:** No, for the same reasons as the above answers to questions 3, 4, and 5.

- **Question 7:** CSPs primarily know the IMEI of the connected device. This is (effectively) a globally unique serial number, which allows the phone's make and model to be determined. However, this does not convey any information whatsoever about how the phone has been configured, its settings, the version of the operating system software (or any other software) installed, and so on.

The CSP can infer some information about how the phone has been configured, based on the network protocol communication that occurs between the carrier's network, and the phone. For example, the CSP can know which bands the phone communicates on, if VoLTE has been successfully provisioned, the connected APN, and so on.

- **Question 8(a):** Yes, the IMEI, which is present in network communications between the carrier's base stations and the phone, can be used to accurately determine the make/model of the mobile phone. However, as above, this information is insufficient for accurate ECS identification.

- **Question 8(b):** There does not seem to be any reason why this sharing of information should not be possible. However, sharing the information alone, without metadata of how it was obtained, its accuracy, or any dispute with the end-user about it, is not likely to be useful, and could be actively harmful for false negative end-users.

- **Question 9:** As explained above, it is not possible to have meaningfully accurate estimates of this. Even the CSPs cannot actually do this, because IMEI whitelisting is coarse and has numerous inaccuracies - and any estimates they provide will only be based on IMEI whitelists. Determining the number or proportion of false negatives and false positives requires careful inspection of individual handset configuration settings and/or network monitoring, which are apparently not currently undertaken by the CSPs. Again, the absence of any ECS test service is a vital flaw - if such a system existed, then it would be possible to meaningfully answer this question.

- **Question 10:** The minimum reasonable steps for ECS identification are to avoid reliance on IMEI whitelists, provide detailed technical documentation (or some other system, e.g. an app) for how end-users can validate the configuration and settings of their handset, and provide a process for end-users affected by incorrect ECS identification.

- **Question 12:** No, for the same reasons as in questions 3-8.

- **Question 13:** Yes. First, how will CSPs know that end-users have received and read the notifications? Should end-users have to acknowledge receipt of them? Should CSPs be required to escalate the notifications, to ensure that they have been received, read, and understood? Second, the notifications are not required to contain contact information, for the end-user to be able to discuss the notification with the CSP. This contact information should be required.

- **Questions 14 and 16:** Even these questions themselves presuppose that the only possible solution is for affected handsets to be replaced. As explained above, in some cases it is possible to reconfigure or software update the handset, in order to provide the necessary ECS access.

- **Question 15:** Yes, information should be provided on what will happen to their mobile number if the service is terminated. For example, will it be possible to port the number to a different CSP after the termination?

- **Question 17:** This should be left to CSPs. For example, some end-users do not even know how to check SMS messages, and do not place calls (so as to hear any automated message on outbound calls). CSPs should be free to escalate the notifications, e.g. by calling the end-user, sending them postal mail, email, etc.

Concluding remarks

I hope that the information presented in my submission is useful to ACMA. To summarise my main points:

- The draft amendments do not account for inaccuracies that may occur (both accidental and deliberate) when CSPs identify handsets that cannot call E000, especially those that arise from the current de facto approach of IMEI whitelisting.
- The ECSD amendments can, and should, do more to clarify this accuracy aspect of "identifying" such handsets, which would help to prevent or minimise a range of negative outcomes.
- There are various potential provisions available to ACMA to achieve this, with the main options centred around:
    - Requiring ECS identification accuracy that is in line with reasonable community expectations.
    - Specifically prohibiting or otherwise restricting the use of IMEI whitelists (and other similarly coarse approaches).
    - Providing recourse for end-users affected by inaccuracies, e.g. by requiring CSPs to have an appeals process, or the ability to handle each service individually (rather than with bulk rules), etc.

If you have any questions regarding my submission, please feel free to contact me via email.

Yours faithfully,

Kevin Pulo