

Manager
Community and National Interests
ACMA
Via email: cnit@acma.gov.au

April 2006

Re: Improving Identity Check Processes for Pre-paid Mobile Services

Thank you for the opportunity to comment on the above discussion paper.

About CTN

The Consumers' Telecommunications Network (CTN) is a national peak body of consumer and community organisations, and of individuals representing community interests, who participate in developing national telecommunications policy. CTN advocates policies for better access, quality of service and affordability of telecommunications facilities for all residential consumers.

CTN's members are national and state organisations representing consumers from non-English speaking backgrounds, deaf consumers, indigenous people, low income consumers, people with disabilities, young people including children, pensioners and superannuants, rural and remote consumers, women and consumers in general.

Overview

There is a need to reconsider what exactly the Determination is trying to achieve and whether a rigorous pre-paid identity check regime is the best means of doing so. CTN's view is that whilst the proposed identity checking process is superior to the current means of collecting information, there is no clear argument that the provision of the information will solve current or future problems. It must also be kept in mind that there are any number of reasons a consumer may use a pre-paid service- amongst them being an inability or ineligibility for a post-paid service, and that access to a service must not be restricted.

Data Integrity

If customer identity information needs to be collected in order to populate the Integrated Public Number Database (IPND), there is a need to ensure the quality and integrity of that data. Allowing sales people at the Point-Of-Sale (POS) or at the Carriage Service Provider (CSP) providing the service to collect that information will create the possibility for the information to be used for purposes other than it was collected. This is an issue identified in the paper, but the emphasis seemed to be on the fact the information was collected by agents for the CSP, rather than the CSP

itself. The difference is irrelevant. If information provision is compulsory, we'd like to see a mechanism developed that allows the end user to directly input to the IPND, rather than providing the information to the CSP (if the objective is, as understood, to populate the IPND).

We note that under the ACIF Customer Contracts Code and Standard Form of Agreement Determination that CSPs are required to advise their customers in writing about changes to their contractual terms. However this could include by text message, or even a mere public notice in a newspaper. Accordingly, these requirements should not be interpreted as a requirement on CSPs to keep up-to-date address records of their customers.

Data Security

There seemed to be an underlying suggestion that information collected by a CSP is somehow more secure than information provided at the POS. The simplest way to secure information is to not require people to provide it in the first instance without good reason. Secure data collection procedures to reduce the chance of mishandling customer information. In particular there seems to be a problem that the information collected at POS is not being used to inform the IPND. Given this, there should not be any ability to collect that information.

If CSPs are ultimately responsible for the collection of this information, this needs to be clear. It would also seem to prohibit collection at the POS, as it would surely contravene the National Privacy Principles. A bigger question, however, is whether they should be collecting it at all.

Rationale About the Requisite Collection of Information

We are confused and concerned that the emphasis of the "need" to collect information is for emergency service use. We are aware through our work on the Emergency Services Advisory Committee (ESAC) that emergency service organisations work on the assumption that the IPND data from a mobile phone caller is not necessarily relevant and accordingly ask the caller their location. After all, mobiles are not fixed services, and there is no assumption that a call from a mobile phone will be originating from the registered address of the user. It is an entirely different service to that of the fixed service.

It is likely an end user will know their home address if that is where they are calling from. If they don't know the location they are calling from, there is little value in requiring the correct address details in the IPND, as it will not assist in finding the location of the user. The need to collect this information needs to be reconsidered in light of the realities of what the collection of the information will be used for.

Collection of information at Point of Sale

We have concerns about the information gathering process at the point of sale, but this does not necessarily mean that it is more appropriate to collect information from an end user when they initiate the service. The information provided at the POS by the purchaser is not necessarily going to be correct, and there is an obvious preference to minimise the potential for incorrect information to be recorded. Historically it appears that IPND data is fraught with errors- and pre-paid data is notably inferior to that collected for post-paid services and fixed lines.

Proposed Identity Verification Process

Step 2 of the suggested identification process is much less rigorous than we anticipated. In fact, there is nothing to really compel the end user to give correct details. Meeting the Evidence of Identity documents will be quite a bureaucratic process for the consumer. The onus should not be moved to the end users, simply for the benefit of unburdening business.

It is notable that if the consumer's identity has been previously verified, then the reactivation of the same service doesn't require an identity check. We support the retention of this exemption. However, what we do not support is the exemption for identity-checks for customers who pay for services using a credit or debit card. We do not believe that is a sufficient means of establishing identity- and after all, from a national interest perspective this would seem to be an obvious vulnerability that would allow persons trying to hide their identity to do so successfully.

The alternative identity verification process has the potential to undermine the new regime. Access to a telecommunications device for young people is highly important. Pre-paid services are useful because they do not require a contractual commitment- it gives the user control over their spend. If a referee was required, are they also responsible for the calls made on that service? They cannot be. There needs to be much more clarity of the role of a referee. References to guarantors who have lawful rights are not helpful here and create even more confusion.

Access to services is key in our view, and we do not support moves to restrict this access on the grounds that identity cannot be ascertained. We note that the activation of the service still hinges on the CSP being satisfied that the customer has been identified. This seems at odds with the need to actually have correct address information. There seems to be a disproportionate emphasis on the name of the customer, rather than the other details for which the information is provided (such as populating the IPND). Surely for consistency there would need to also be verification of address, as well as validation of the identity? And yet this is not required, highlighting another serious inconsistency in the proposal.

All the emphasis is placed on the provision of information at the POS or activation of a service, yet there are no requirements that information be updated at regular intervals throughout the use of the service. Again, this inconsistency would surely

undermine the whole effectiveness of the proposed regime, particularly given the fact that nearly 51% of the population use a pre paid service. We also wish to point out that pre-paid services are a very useful budgeting tool for many people. It is important that there are no disincentives created for customers wanting a pre-paid service.

We also note that CSPs are required to deactivate a service if it has reason to suspect the identity information it holds is incorrect. Based on discussions with industry members, we believe that some CSPs are systematically ignoring this requirement. If there is a problem to be solved, ACMA needs to understand the extent of the problem and the role CSPs have in ensuring they have the correct information. We ask that ACMA write to each of the CSPs about their policy and clarify details about the number of breaches it has found. If CSPs are responsible for the collection and maintenance of correct information then their adherence to this requirement needs much closer regulatory scrutiny.

Other relevant issues

We'd like to see some additional provisions for customers to obtain a refund if they are not connected to a telecommunications service they have purchased due to problems verifying identity. Similarly, all packaging of pre-paid services needs to clearly indicate that proof of identity will need to be provided before a service can be activated.

We think it's important that the context of other developments be considered in making any changes. In the case of national security concerns, we are of the view that other powers may make the collection of identity information for pre-paid users irrelevant. In particular we'd expect the recent telecommunications interception legislation amendment which gives law enforcement agencies access to phone calls and text messages to provide information pertaining to national security. Similarly there is the potential for mobile location information technology in the future to give law enforcement agencies information that is far more relevant (and current) than what was collected when a pre-paid mobile service was activated.

We note that in 2004 the then Australian Communications Authority issued a discussion paper looking at how customer information from the IPND is used. Consumer groups have long been concerned that information from the IPND has been misused- and yet here we have a regime demanding even more personal information that is not actually required in order to provide the service, other than to meet the needs of the initial Determination. We'd like to see the uses of the IPND back on the agenda, so we have some confidence that customer information that people have no choice in providing is not being abused.

Conclusion

We remain unconvinced about how this proposed pre-paid identity check regime will deliver any national interest outcomes. There is no more than a cursory reference to

repealing the Determination made in the discussion paper, which would seem inappropriate given the unsteady premises upon which the rationale for a new identity check regime is based. This needs to be given serious consideration.

We do not see that the address location of a consumer will necessarily help emergency services locate that person. Nor do we see how linking the consumer's address as the time of service activation will assist in achieving national security because there is no ongoing requirement to ensure that information is current. Nor do we see that the IPND information is likely to be more accurate given the lack of coordination between receipt of the customer information and the eventual entry into the IPND.

CTN has long held the view that consumers should not be compelled to provide more personal information than is reasonably required, and address details for pre-paid mobile users falls into this category. Whilst we are still awaiting an update on the use of IPND data, we will continue to challenge any requirements that require customers to provide personal information when that data is vulnerable.

We hope these comments are of use to you. Should you wish to discuss this response in more detail please contact myself or Sarah Wilson at the Consumers' Telecommunications Network on 02 9572 6007 or at ctn@ctn.org.au.

Yours sincerely,

A handwritten signature in black ink, reading "Teresa Corbin". The signature is fluid and cursive, with a long horizontal flourish at the end.

Teresa Corbin
CTN Executive Director

This submission was prepared by Teresa Corbin, CTN Executive Director, and Sarah Wilson, CTN Policy Officer. It has been approved out of session by the CTN Council.
