Pre-paid mobile identity-check **processes being reviewed**

ACMA is reviewing the way telephone companies collect identity information about their pre-paid mobile phone customers.

This information can help emergency service organisations respond quickly to time-critical emergencies and also help identify people who make hoax calls to emergency services. It can also be used to assist law enforcement and national security agencies in investigating crime, including prosecuting people who make life-threatening calls.

The information is stored in the Integrated Public Number Database (IPND), an industry-wide database of all listed and unlisted public telephone numbers. The current information collection processes are not providing data of sufficient quality and consistency.

Other possible improvements to the identity-checking process, which may reduce industry costs and provide a simpler process for consumers, are also being examined. These include removing the identity-checking process from retail outlets such as supermarkets and petrol stations, and requiring mobile phone companies to collect and verify the information at the time the pre-paid mobile service is activated.

The rules applying to supply of pre-paid public mobile telecommunications services are set out in the *Telecommunications (Service Provider – Identity Checks for Pre-paid Public Mobile Telecommunications Services) Determination 2000*, which provides for three alternative methods of identity checking:

- a point-of-sale process where carriage service providers collect information about purchasers of pre-paid services, including name and address, at the time the service is purchased or
- a post-sale process where they verify collected identity information or
- a process where a carriage service provider could comply with an ACMA-approved compliance plan.

In response to increased concerns worldwide about identity security and the anonymous use of pre-paid mobile phones, several countries have announced the introduction of an identity-checking regime for pre-paid mobile phones similar to the Australia system. Other countries have announced tightening of identity-security arrangements that may have similar benefits.

Pre-paid mobile phone services enable users to pay in advance for the costs of their mobile phone calls. As credit is reduced, the user has the option of purchasing another pre-paid service or recharging the credit for their existing service. Post-paid services typically involve a fixed-term contract with bills sent to the customer at regular intervals.

In 2001–02, pre-paid services accounted for approximately 32.5 per cent of the mobile phone service market in Australia. At the close of 2004–05, pre-paid services accounted for approximately 51 per cent of the 16.5 million mobile services in operation in Australia and represented the major area of growth in the mobiles market. This strong growth can be expected to continue, particularly as pre-paid mobile services are enhanced with the addition of value-added services previously only available to post-paid customers.

All telecommunications carriage service providers are required to provide information for the IPND under Part 4 of Schedule 2 to the *Telecommunications Act 1997*. The IPND is managed by Telstra as a condition of its carrier licence. It contains customer data including a public number and associated information such as the customer's name and address and the name of the service provider. This data may only be accessed and used for certain 'approved purposes' such as providing directory services, producing public number directories, and assisting law enforcement agencies or emergency service organisations.

Telecommunications service providers must ensure the IPND Manager receives correct information about their customers for the effective operation of the 000 emergency call service. They are also required to provide assistance to law enforcement and national security agencies. A vital part of this is to maintain accurate records of their customers' personal details.

As part of its review, ACMA released a discussion paper, *Identity Checks for Pre-paid Mobile Services*, for which submissions close on 28 April 2006. For more information about the review, contact ACMA's Community and National Interests section by email cnit@acma.gov.au or telephone 03 9963 6800.

New standards for **narrowcast television** services

To prevent the broadcast of programs that directly recruit or solicit donations for terrorist organisations and terrorist activities, ACMA has determined new program standards for subscription and open narrowcasting television services. The new standards reflect existing Commonwealth anti-terrorism laws and will ensure that ACMA can act more effectively if inappropriate material is broadcast.

The standards state that open and subscription narrowcast television services must not broadcast programs that can reasonably be construed as:

- directly recruiting persons to join, or participate in, the activities of a terrorist organisation; or
- soliciting or assisting in the collection or provision of funds for a terrorist organisation.

The definition of 'terrorist organisation' in the standards is linked to the list of terrorist organisations prescribed in the Commonwealth Criminal Code Regulations 2002.

The standards place the obligation on television narrowcasters to ensure that prohibited programs will not be broadcast. Program content that is part of a bona fide report, comment on a matter of public interest or political opinion is not prohibited. This exception is intended to ensure that freedom of expression is not unduly restricted.

The current television narrowcast codes of practice already limit the ability of narrowcasters to broadcast views that are likely to incite or perpetrate hatred towards, or vilify particular groups, and they provide adequate safeguards on these matters.

Determining standards was preferred to codes amendment because a standard enables stronger, more expeditious enforcement mechanisms to be used in the event of a breach and does not require the complainant to complain to the broadcaster first.

ACMA decided to impose standards following an investigation into the broadcast of Al Manar programming by Television and Radio Broadcasting Services (TARBS) in 2004. Al Manar is a channel based in Lebanon and was being delivered by TARBS, a service provider based in Australia, which offered subscription narrowcasting services.

While the investigation was terminated before findings were made owing to the cessation of the TARBS business, the investigation had revealed that programs on the Al Manar channel included material directed towards soliciting funds and promoting the activities of terrorist organisations by calling for donations and publishing their website addresses.

Work on the investigation highlighted a gap in the regulatory framework. Under the relevant class licence condition, narrowcasters only commit an offence and breach the class licence condition if they intend to use a broadcasting service to commit the offence or are reckless in their knowledge of whether the service is being used to commit the offence.

In most cases, narrowcasters will not have the intention or direct knowledge required for such an offence. They are not necessarily directly involved in program production, may acquire their content from third parties and may not have viewed the programs that they broadcast.

The new standards address this gap by prohibiting programs that directly recruit participants or solicit donations for terrorist organisations, regardless of a narrowcaster's intention or knowledge about the program content.