



**Australian  
Privacy  
Foundation**

mail@privacy.org.au  
www.privacy.org.au

# Review of the Telecommunications (Emergency Call Services) Determination

Consultation draft at  
[http://www.acma.gov.au/WEB/STANDARD/671220/pc=PC\\_310543](http://www.acma.gov.au/WEB/STANDARD/671220/pc=PC_310543)

## Submission to ACMA

**September 2009**

### ***The Australian Privacy Foundation***

The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. Since 1987, the Foundation has led the defence of the right of individuals to control their personal information and to be free of excessive intrusions. The Foundation uses the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed. For further information about the Foundation and the Charter, see [www.privacy.org.au](http://www.privacy.org.au)

We note that we have a long history of participation in telecommunications policy development, particularly during the period of Code development by then ACIF, and through submissions to departmental, agency and parliamentary enquiries. We have made several submissions which touch specifically on the subject of mobile phone location and related issues of the IPND (see <http://www.privacy.org.au/Papers/indexPolicies.html#TelecommsDNC>).

Regrettably, since Communications Alliance succeeded ACIF the opportunities for participation have been much reduced, and we, along with our colleagues at CTN (now ACCAN) have also been concerned about the closed nature of many ACMA consultations – e.g. through its Law Enforcement and Emergency Services Advisory Committees, which have no effective civil society input.

We do however welcome the opportunities for input when they are offered, as in this case.

### ***Submission***

We note that ACMA is required by s.147(2)(1) of the *Telecommunications (Consumer Protection and Service Standards) Act 1999* to have regard to the objective that any ECS Determination is consistent with IPP 11 and NPP 2 of the *Privacy Act 1988* concerning disclosure of personal information. It would have been useful to have seen in the Consultation paper an assessment of how the proposed changes meet this requirement, and also the need to ensure that service providers can comply with other relevant privacy principles – in particular the collection and anonymity principles (NPP 1 and NPP 8 respectively).

This would have been consistent with the Privacy Commissioner's guidance on Privacy Impact Assessment. In the absence of any such assessment, we have identified some privacy issues with the proposed changes. These go beyond the question of mere compliance with privacy principles – important though that is – to wider issues about intrusion and proportionality.

## **Draft Determination section 15 - Type 2 VOIP Services**

We welcome the policy decision to allow the providers of Type 2 VOIP providers the option of making their customer aware that access to ECS is not available *where it is technically not possible*. To have made provision of access to ECS mandatory would have severely restricted the range of VOIP services available. Given that a consequence of ECS access would normally be a loss of privacy, this would have been undesirable. We believe strongly that consumers should have the choice of anonymous communications provided they are fully informed of any ‘downside’ such as non-availability of ECS.

However, we remain unclear as to why any Type 2 VOIP service would *not* be able to connect to ECS numbers. Surely the issue is whether providers of these services are able to meet the full range of obligations that attach to provision of ECS access, such as customer identification and provision of location details? Is it the intent of the policy that simply because a provider cannot technically meet the full range of obligations, it is not *permitted* to allow its users to access ECS numbers, even where this is technically possible? If this is the case it would be an unreasonable denial of potentially life saving service, and grossly irresponsible. We seek clarification as to whether this is the case, and if so how it can possibly be justified. If, as we suspect, such a policy intent is driven primarily by law enforcement interests, then this should be explained and justified rather than purporting to be based on the needs of response to ECS calls.

## **Sections 40-42 – Provision of customer information to the IPND Manager**

We understand the intention of these provisions is simply to align the obligations of the providers of mobile carriage services with those of the other two types of service provider, in relation to the provision of ‘best available’ customer address information. There appears to be no change in either the customer identification requirements or the standard details to be provided to the IPND Manager. As you may be aware, the Foundation has concerns about the policy position in relation to both those matters, and the extent to which it has been driven by the perceived needs of users of the IPND other than Emergency Services responding to calls to ECS numbers – including law enforcement agencies and commercial interests. Given the lack of certainty about the relevance of a subscriber address to the location of a call in many, if not most, mobile calls, we question the proportionality of the case for address information based on ECS needs. However, provided the policy on these matters is unchanged, we will reserve our arguments for another occasion.

For further contact on this submission please contact  
Nigel Waters, Board Member  
E-mail: [Board5@privacy.org.au](mailto:Board5@privacy.org.au)

*Please note that postal correspondence takes some time due to re-direction – our preferred mode of communication is by email, which should be answered without undue delay.*