New streamlined identity-checking requirements for prepaid mobile carriage services

Submission to ACMA

June 2013

Australian Privacy Foundation

email: mail@privacy.org.au

website : www.privacy.org.au

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

Please note that APF does not have a single postal address – we prefer communication by e-mail. If a postal address is required please contact the signatory.

Publication of submissions

We note that we have no objection to the publication of this submission in full. To further the public interest in transparency of public policy processes, APF strongly supports the position that all submissions to public Inquiries and reviews should be publicly available, except to the extent that a submitter has reasonable grounds for confidentiality for all, or preferably part of, a submission.

Introduction

APF welcomes the opportunity to respond to this Consultation. We have made submissions to past policy reviews in this area. The Consultation paper clearly outlines the proposed changes and identifies most of the relevant issues, although there are a few points where we think further clarification is required before we can offer a final opinion.

Identification requirements for communications services are controversial, particularly in light of longstanding community concerns about cybersecurity, identity crime and data security breaches. Recent publicity about government surveillance has also led to demands, which we support, for greater transparency about the extent of monitoring of communications, and the safeguards that apply. This consultation cannot be divorced from that wider debate and context.

We also note that the route by which identification details will be made available to law enforcement and national security agencies (and to a range of other users) is via the Integrated Public Number Database (IPND). The government is currently conducting a review of the IPND, to which we have made multiple submissions. It is very unfortunate both that the IPND review and this consultation on mobile phone identification requirements are being conducted independently, and that both of those policy developments are being progressed in the absence of an overall review of telecommunications privacy, which was recommended by the ALRC in its 2008 Report *For Your Information – Australian Privacy Law and Practice*. The government has delayed its response to the telecommunications privacy recommendations of the ALRC for more than 5 years, and in the meantime the community is unfairly asked to make judgments about elements of the 'big picture' without an overall principled context.

In commenting on the proposed Determination, we do not concede the threshold issue of whether a statutory requirement for customer identification is, on balance, justified. We think a strong case can be made that the identification regime (in this policy area as in many others) imposes major privacy intrusions on the vast majority of law-abiding end-users without giving a level of assurance about the accuracy and completeness of the resulting records that might justify the imposition. We note that other major jurisdictions including the USA and the UK do not require identification for mobile phone accounts[1].

One contributor to this imbalance in the mobile phone context is the vagueness of the concepts of service activator vs end-users – we suggest that it will continue to be very easy for mobile phones to be acquired for use in association with criminal purposes through the use of unknowing intermediaries. We submit that the definition of a service activator needs to be given more thought and more rigorous analysis applied to the detail of the regime relative to its objectives.

We are also concerned that the Determination appears to be based on unquantified problems with the existing regime – we believe that all significant policy changes should be 'evidence based'. The absence of any analysis of the scale and nature of any such problems is troubling, and calls into question the need for the changes.

We accept however that the current state of the law imposes an identification requirement, and that this Determination proposal is not the best forum for debating the justification. We will therefore confine ourselves below to comments on the methods of identification and associated safeguards.

We note that ACMA has clearly identified the privacy interest and has sought to balance this with other public interests, within the constraints imposed by the statutory requirement for identification.

Alternative means of verifying identity for pre-paid mobiles

The introduction of alternative means has one very positive effect in privacy terms in that it will remove the need for third party retailers to collect and record identification details from individuals purchasing a mobile phone SIM card. If the alternatives are taken up, then there should be a major reduction in the amount of personal information being stored, often in insecure environments, and incidentally known to employees of third party businesses who have no 'need to know'. This will be an undeniable benefit, but has to be balanced against any negative privacy impacts of the alternatives.

[1] The Economist, 4 May 2013, page 54

Option (a) – use of the online government verification services, such as the DVS, is superficially attractive, but only once it has been accepted that the DVS (and any similar systems) should be made available for use by the private sector in the first place. This is a separate issue on which the APF has strong views (see our website for numerous DVS related papers), but for the purposes of this consultation, we will assume that access has been agreed. Some of the features of the proposed use of DVS, such as its operation on a blind check 'yes-no' basis, and the associated limits proposed on recording of certain identifiers, are welcome. The Determination should ensure that *any* on line government verification service has to have these safeguards.

Option (b) – use of financial accounts, is in our view problematic. In principle, we are opposed to the use of 'nominal' transactions unrelated to any financial commitment for an entirely different purpose; i.e. identity verification. We would be very surprised if all stakeholders in the policy settings and regulation of financial services were comfortable with this proposal. It also raised unanswered questions about how any costs associated with nominal financial transactions will be apportioned.

Option (c) – the use of approved email addresses – specified as edu.au and gov.au addresses – is interesting innovation but we would have thought open to a range of criticisms, and potential weaknesses. What is the level of confidence in the integrity of the domain administration systems that allocate tens of thousands of such addresses? ACCAN has raised other issues in relation to this option which need to be addressed.

Option (d) – an existing post-paid account with the same CSP, would appear sensible and non-controversial in that no additional privacy intrusion is involved (although privacy issues remain in relation to the customer identification requirements associated with post-paid accounts).

Option (e) – signed courier delivery – seems unlikely to be popular, and would also appear to be open to ready abuse by persons temporarily occupying premises for the purposes of acquiring mobile phone accounts (amongst other things).

Most of the options have a common problem in that they rely, to a greater or lesser extent, on trust in another link in the chain of 'evidence of identity'. That is why we think that this Determination pre-empts the wider discussion that needs to take place about identity management in general and its relationship to government surveillance.

We note that ACCAN has raised a range of issues relating to equity and access and support their concerns. There is a risk that the provision for a wide range of alternative methods of identity verification could result in very unfair and unequal treatment of different groups of consumers.

We also support ACCAN's submission that the list of matters to be taken into consideration by the ACMA when considering a compliance plan under part 6 should expressly include the protection of consumer information.

Identification details required

We note that the proposed Determination introduces a new requirement for collection of date of birth (DoB), and justifies this on the grounds that it is useful to law enforcement and national security agencies in assisting them to accurately distinguish between individuals with similar names. The availability of any additional information may result in some cases where individuals do not unnecessarily come under suspicion or experience further intrusion, but this needs to be balanced against the additional intrusion into the privacy of all mobile phone holders inherent in the new requirement for DoB – a detail which the CSPs have no legitimate business interest in collecting.

CSPs will no doubt be interested in using the newly acquired DoB for general market research, and potentially to target individuals for marketing. We submit that CSPs should not receive any 'windfall' commercial advantage from information which they are required by law to collect – there should be a prohibition on secondary use of DoB for any purpose other than providing it to the IPND Manager.

As ACCAN has noted, it is unclear whether the requirement for DoB will extend to those CSPs which continue to rely on point of sale verification, and that if it does, it raises a serious privacy concern about DoB details – a key to potential identity crime - being in the hands of thousands of third parties.

Record keeping requirements

The proposed record keeping requirements are in most respects just consequential on the policy decision to mandate the identification requirement in the first place. It is unclear if CSPs choosing to use Option (b) will be allowed (or required) to record account numbers – there is a suggestion later in section 3.4 that a transaction code will be allowed (mandated?) in place of credit/debit card numbers, but is this only in relation to the point of sale option? We submit that that safeguard should be mandated for all verifications based on financial account details. Section 7.3 appears to only restrict the recording of specific items and the copying of documents containing those items. We submit that there should be an express prohibition on CSPs keeping copies of *any* documents shown as evidence of identity – it should only be necessary for the 'verification transaction details' listed in Column C of the table in Schedule 4 to be kept (subject to our submissions above about the appropriateness of some of these details).

The obligation in requirement in s 7.1(3) that records be kept as long as the service is active should also expressly require that those records should be destroyed once the service is no longer active.

Arrangements for emergencies and disasters (and for DVS outages)

We note the sensible provision for relaxation of identification requirements in emergencies and disasters. Presumably to ensure that such relaxations do not compromise the overall objectives, it is proposed to limit the validity of any relaxation to 30 days. We submit that this is far too short a period –

it is completely unreasonable to expect someone who has been the victim of a natural disaster or major emergency to have their access to their replacement communications cut off so soon after the event.

There clearly needs to be provision for DVS outages given that option (a) is likely to be the highest volume channel for verification. We would suggest that in these circumstances, a 30 day temporary use exception might be appropriate.

For further information please contact:

Nigel Waters, Board Member
Australian Privacy Foundation
board5@privacy.org.au
APF Web site: http://www.privacy.org.au

Please note that APF's preferred mode of communication is by email, which should be answered without undue delay. APF does not have an organisational postal address. If postal communication is necessary, please contact the person named above to arrange for a postal address.