

Identity checks for pre-paid mobile phones

Discussion Paper at

http://www.acma.gov.au/acmainterwr/assets/main/lib100285/id_checks_prepaid.pdf

Australian Privacy Foundation submission to ACMA

April 2006

CONTENTS

<u>The Australian Privacy Foundation</u>	1
<u>Challenge to underlying assumption</u>	2
<u>Emergency Services case not strong</u>	3
<u>Reference to privacy principles</u>	4
<u>Unfortunate reference to ‘national identification system’</u>	5
<u>Proposed process (as set out in section 6.2)</u>	5
<u>Benefits</u>	7
<u>Costs</u>	8
<u>Future options (as set out in section 8)</u>	8
<u>Compliance with Privacy law</u>	9
<u>Overseas comparisons</u>	10
<u>Conclusion</u>	11

The Australian Privacy Foundation

1. The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. Relying entirely on volunteer effort, the Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend 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 information about the Foundation and the Charter, see www.privacy.org.au

Challenge to underlying assumption

2. We submit that the ACMA, and the government, should take this opportunity to review the *need* for identification, rather than assuming that it is justified and therefore requires improved collection and verification processes. We note that other countries to which we normally compare Australia, such as Canada and New Zealand, have only recently expressly rejected the need for identification for pre-paid mobile phone accounts, and only 8 of 30 OECD member countries currently require ID (see section on overseas comparisons below).

3. The Discussion Paper clearly identifies that the issue of incomplete or inaccurate customer records is one that derives purely from the *secondary* uses of the information by government authorities.

4. The paper states:

“As pre-payment eliminates the need for regular accounts or invoices to be mailed to the customer, there is minimal commercial need to collect and maintain accurate identity or address information for pre-paid customers.” (DP 2.2)

5. We submit that in fact, the telecommunications (carriage) service providers (CSPs) themselves have *no need at all* for this information in order to provide the purchased services, although they may have a commercial interest in it for marketing, customer support, research etc.

6. Were it not for the legal requirement to collect customer information, CSPs could either not collect any customer information, or make provision optional. This would be consistent with National Privacy Principle 8, which states

“Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.”

7. We accept that NPP 8 does not apply in the circumstances of pre-paid mobile phone services, as the collection of customer identification information is, currently, required by law, for public interest reasons. Nevertheless, we suggest that consideration of this issue should recognise that this is a departure from an important privacy principle. This supports the need for a re-assessment of the justification for the requirement, as argued above.

8. If the case is established for continuing the requirement, then the detailed arrangements should be designed to minimise privacy intrusion and should only require information that will actually be of direct utility in relation to the other public interests.

Emergency Services case not strong

9. The difficulties relating to emergency services, asserted in section 4.5 of the DP, may be overstated. Surely, when emergency services receive a call from a mobile, it is always necessary to confirm at least the location of the caller – it would never be safe to rely on the pre-recorded address of the customer of that service.

10. It is not immediately obvious why more accurate and complete records of customer names and addresses would assist emergency services.

11. The relationship between mobile phone user and the person who has opened the account is entirely unpredictable. And the chances of a call from a mobile phone being made from same geographic location as the registered account holder's address are remote, and again entirely unpredictable. It follows that any usable information about the caller and their location, for emergency response, will need to be verified by the emergency service operator. Little if any time would be saved by the ESO having access to subscriber details as confirming them would take as long as collecting them afresh. It would be of limited value, and potentially dangerous, for emergency services to commence any action on the basis of pre-registered information, which may or may not be relevant.

12. The registered information could of course be valuable to law enforcement agencies in tracing, *after the event*, who has made a particular call (whether emergency or other). But this is not emergency service response and should not be confused with it. Even where a law enforcement investigation relates to the use of an emergency service number - e.g. in cases of arson, or bomb threats etc, it is at that point a law enforcement response not an emergency services response.

13. Any public interest case for an identification requirement to assist law enforcement should be justified and debated on its merits without being confused with emergency service issues.

14. The Discussion Paper states (at 5.2) that ACMA has considered the option of 'the removal of the Determination altogether' but provides no justification for not considering the option further. In light of the position in Canada and New Zealand, where the governments have expressly ruled out an identification requirement for pre-paid mobile accounts (see below), we believe that a justification is essential.

Reference to privacy principles

15. The Discussion Paper includes (at 5.1) as a desirable outcome of the review:

- Improved privacy protections for consumers:
 - i) improved accuracy of customer information in the IPND (in line with National Privacy Principle 7 [*note, this reference should be to NPP3 – data quality, not NPP 7*];
 - ii) secure data collection procedures to reduce the chance of mishandling customer information (in line with National Privacy Principle 4);

16. We suggest that this is an overly simplistic view of privacy protection. The National Privacy Principles need to be considered as a total package and in the context of the underlying objective of giving individuals more control over the way in which personal information about them is held and used.

17. Accuracy and completeness are not ends in themselves - they are designed to support 'fitness for purpose'. A secondary purpose, such as the compilation of the IPND and its use by law enforcement agencies, should *not* be the driver of appropriate quality standards. If the data is of sufficient quality for the primary purpose – which in this case is the provision of a telecommunications service to a customer, then that should suffice, with any secondary users having to live with whatever inaccuracies may be present. This analysis would also apply to information about post-paid fixed line customers, where the service providers need the information to supply the service and to bill the customer.

18. However, in the case of pre-paid mobile telecommunications services, the public interests behind the requirement for the IPND are the primary (and only) purpose of collection, and it is therefore appropriate for the data quality principle, NPP 3 [*not NPP 7 – see above*] to be applied in relation to that purpose. (There is a separate issue about notification under NPP1 which is discussed below).

19. It does not follow, however, that the public purpose of the IPND requires the level of 'certainty' about customer details that the current Determination, and the proposals, aspire to. Identity management is an inherently 'messy' process dealing with the different names and addresses which legitimately attach to some people, and becomes even messier attempts are made to use details collected for one purpose for other unrelated purposes. We suggest that while there may be some collateral benefit to individuals from enhanced identification feeding into the IPND, NPP3 cannot be used as a justification for the changes.

20. The security principle, NPP 4, also does not stand alone – it aims to ensure an appropriate protection against possible risks, including unauthorised access, use and disclosure. Clearly, the implementation of the principle is a risk management exercise – the contribution that improved accuracy and completeness of customer data may make to security needs to be balanced alongside both the cost (both financial and to individual’s privacy in a wider context), and the risk. No empirical evidence is provided in the Discussion Paper about the extent of inappropriate use or disclosure of IPND data resulting from inaccuracy or incompleteness.

Unfortunate reference to ‘national identification system’

21. The reference in 5.2 to a ‘national identification system’ is unfortunate. No such system has yet been officially proposed – indeed the Attorney-General has announced that a review of the case for such a system will be undertaken, but not in the immediate future. The government appears divided on the merits of a national identity card, and initiatives such as this should avoid in any way pre-judging the eventual policy decision.

22. In the meantime, it is more accurate and appropriate to use the expression, also in 5.2, of ‘initiatives to improve Australia’s identity security framework’, which are clearly in train. This may seem like a marginal semantic difference, but has major significance from a privacy perspective. The APF and many other groups consider that much more debate is needed before accepting that ‘improvements in identity security’ is an appropriate objective, and even if it is, certainly reject the view that a ‘national identification system’ is necessarily required.

Proposed process (as set out in section 6.2)

Step 2. – Collection

23. The current Determination requires information about either the purchaser (where obtained as part of the purchase at point of sale) or the end-user (where obtained by a call after the purchase). The logic of this distinction is not clear. It would seem to lead to CSPs records arbitrarily being about either the purchaser or the end-user (but not both) – either could be passed on for inclusion in the IPND, leading to further potential for incorrect or irrelevant data.

24. The proposed new requirements do not make any distinction between purchaser and end-user – the requirements relate to the ‘customer’ – a term which is undefined. If it is intended to abandon the arbitrary distinction then this is probably desirable, but it would help if the consequences of this change was explained.

25. It is suggested that the CSP should require the customer to specify whether the service is for use of a business. This is not only none of the CSPs' business, but is also not mandatory for the IPND, which only holds 'business' or 'charity' status of a telephone service 'if known' to the provider (see Schedule 1 to the current Determination).

26. Since the CSP does not need to know it, it follows that there should be no requirement to provide this information. With fixed line services and post-paid mobile services, identifying business or charitable use is currently optional – usually to obtain some preferential terms or additional services.

27. Many customers decline to specify whether their intended use is for personal or business purposes, partly to protect themselves from unsolicited marketing approaches.

28. The Determination should not be used as a 'back door' way of mandating this information for a sub-set of telecommunications customers.

Step 3. – Validation

29. It is proposed that CSPs will check that the customer's name and address are 'valid'. This begs the question as to what constitutes a 'valid' name. Individuals in Australia are free to use whatever name they like when entering most commercial transactions, and to give any 'real' address (although the current Determination requires it to be a residential address). There is no central database of valid names and corresponding addresses – only a number of available sources against which they can be matched.

30. There is a central file of known postal geographic addresses (the GAF) but use of this again begs the question as to why a customer for a pre-paid mobile phone should not be able to give any address, including a PO Box (not just residential), that will allow him/her to be contacted if required (assuming the requirement for identification is accepted in the first place). There would be no privacy objection to CSPs using automated address validation software to reduce spelling mistakes and other inadvertent errors, but the absence of a 'match' cannot be a legitimate reason for declining to activate a service.

Step 4 – Verification

31. The current Determination requires CSPs or their agents to either confirm a new customer's name and address as matching those on an existing customer record, or to sight some evidence of identity (EoI) from a prescribed list, sufficient to meet a required threshold (types of document for purchasers, a points test for end-users). The EoI requirements appear somewhat arbitrary and do not, for example, equate with EoI requirements required for bank account opening under the Financial Transaction Reports Act 1988.

32. Current exemptions from the requirement for EoI that would remain are:

- Payment by credit or debit card, on the grounds that the EoI requirements for obtaining these cards are even stronger.
- Existing customer record for fixed line service. We support the extension of this exemption to an existing customer record for other services such as post paid mobile or Internet.
- A match against other existing records of other financial accounts such as a cheque account. We support the suggestion of extending this to accounts such as B-pay.
- Identity already verified for a previous pre-paid service

33. For customers not fitting into the exemptions, evidence of identity would (as now) be required. The main proposed change in verification requirements is a revised list of acceptable EoI documents, and the removal of this option from 'distributed sales outlets' not connected to the CSPs systems.

34. It is proposed to provide an alternative whereby the identity of a third party associated with the customer can be validated and verified. This would supposedly cater for anyone who could not, for whatever reason, meet the standard for themselves.

35. The net effect of the proposed changes would appear to be to allow more individuals to be exempt from the requirement to produce any EoI, but to make others (or their associates) attend a CSPs' premises to show EoI before their service can be activated, rather than being able to do this at the point of sale at an agent's premises.

Benefits

36. We note that a claimed benefit of the new requirements is 'Improved personal privacy, with identification documents produced only once and only to the staff of the CSP (rather than to sales staff in distributed sales networks)' (DP 7.1.2). We accept that removing collection and record-keeping requirements from agents would be a privacy benefit, albeit at the expense of some convenience, although it should be noted that many customers will still give personal information to agents if they choose to pay by means other than cash.

37. As already noted, we dispute the claimed benefits to individuals and emergency service organizations in relation to emergency calls.

Costs

38. We suggest that the first potential consumer detriment in 7.2.2 is actually a more significant privacy issue in that the proposed new requirements will mean more intrusion for some people, who would currently be able to satisfy the EoI requirements with simpler documents such as a tertiary ID card, or government benefit card/document.

Future options (as set out in section 8)

Document Verification Service (DVS) (DP 8.1)

39. We commend the cautionary approach taken to possible future access to the DVS. Extension of this service to private sector users raises very significant privacy issues which have yet to be resolved, and legislative amendments would almost certainly be required. It is not a realistic short term option.

Telecommunications Industry Account Verification System (AVS) (DP 8.2)

40. The DP correctly identifies that there would be significant privacy issues with any such system of shared account information, as well as obvious competition issues.

Direct contact with issuers of EoI (DP 8.3)

41. This may be possible, subject to existing or future privacy laws, and may be preferable from a privacy perspective to a centralised system.

42. We have a number of queries/difficulties with the illustrative case studies at Attachment B.

Case Study 1 – Milo & Ellis

43. This does not seem to correspond with the proposed EoI criteria – the case study says Ellis is required to provide photo ID to the CSP, whereas the list of acceptable Type A documents includes at least two – birth certificate and citizenship certificate, which do not include photos.

44. The case study also seems to assume that the CSP has access to Milo's credit card details, but it is not clear why this would be the case – surely an agent would typically take and process the payment and merely pass on an aggregate sum for a period of business to the CSP.

Case Study 2 – Sadie

45. This case study has Sadie providing her credit card number over the phone. We assume that the top-up authority qualifies her for the exemption from production of EoI for credit/debit card payment. It should be made clear that a credit card is no longer listed as acceptable Type B EoI – the case study misleadingly implies that she provides the credit card number a response to the request for EoI.

46. We would have serious reservations about the recording of credit card numbers as a form of EoI where there is no financial transaction involved, and suggest that the card issuers may share these reservations. This appears to be an option under the existing Category B documents, but we note that it has been removed from the proposed list. We suggest any guidance material makes it clear that recording credit or debit card numbers is only appropriate where there is a relevant financial transaction involving the card.

Case Study 3 – Ewen/Elaine

47. This case study misleadingly implies that some sort of credit assessment is involved, by referring to the regular payment of Elaine’s landline bills. Any such assessment may well be unlawful under the provisions of Part IIIA of the Privacy Act.

Compliance with Privacy law

48. The DP acknowledges that CSPs will have to comply with other laws including the Privacy Act 1988. One obligation, under NPP 1.3/1.5, is to ensure that individuals are made aware of certain matters when collecting personal information.

49. Given that the *only* good reason for why CSPs collect personal information about pre-paid mobile customers is to comply with the Determination, they should be making that clear to new customers¹. They should also explain that the information will be disclosed to the IPND.² If CSPs separately decide that they would also like to use the same information for commercial purposes, such as customer service, or marketing, then they will need to make this clear, and if marketing is intended, give individuals the opportunity to opt-out.³ But it would be misleading to imply that the information was *required* for business purposes.

50. As it is the government that is requiring the collection of personal information by CSPs, we suggest that there is an obligation on ACMA to advise CSPs of the specific obligations under NPPs 1.3/1.5, and 2.1(c), and not just assume that CSPs will be aware of these. ACMA should expressly accept this obligation.

Overseas comparisons

¹ NPP 1.3(e) expressly requires notification of ‘any law that requires the particular information to be collected’

² Pursuant to NPP 1.3(d)

³ Pursuant to NPP 2.1(c)

51. The draft report of a major Canadian study finds that only eight of the 30 OECD member countries had mandatory identification requirements for pre-paid mobile accounts as at early 2006, and concludes that:

“The study has found there is no substantial source of empirical evidence identified any country of the OECD that might support or oppose the introduction of prepaid regulations on the grounds that such measure will improve law enforcement or public safety activities.”⁴

52. In relation to Canada itself, the discussion paper for this study states:

“ In Canada, prepaid mobile phone users do not have to be registered in a subscriber database, do not require a credit check and have the benefit of using a product that is simple, easy to purchase and provides a degree of anonymity for customers.

This element of anonymity has been identified as a potential threat to emergency services and national security, particularly in their ongoing efforts to ensure public safety and to maintain public order. In response to this challenge, a number of countries including Australia and Switzerland have banned the sale of anonymous prepaid mobile phone service.

However, at this point in time there is little hard evidence to suggest that eliminating anonymous prepaid services reduces crime or provides definitive benefits to law enforcement or national security. Some say that the collection of customer information is a costly and ineffective strategy that violates Canada’s existing privacy legislation.

...

In 2003, the CRTC (The Canadian Telecommunications Regulator) overturned an interim ruling that had required wireless service providers to collect and verify customer information at the point of purchase”⁵

53. We note that the New Zealand government has recently announced that it has no intention of changing the law to require identification – registering a pre-paid mobile phone in is currently optional in New Zealand.

⁴ Gow, Gordon A. (2006, March 31). ‘Privacy Rights and Prepaid Communications Services: A Survey of Prepaid Mobile Phone Regulation and Registration Policies among OECD Member States.’ Research report for the Office of the Privacy Commissioner of Canada. Prepared by the Centre for Policy Research on Science and Technology, Simon Fraser University at Harbour Centre. Vancouver, Canada.

⁵ *Privacy and Prepaid Communication Services*, Centre for Policy Research on Science and Technology (CPROST) at Simon Fraser University, 2006. <http://www.sfu.ca/cprost/prepaid/index.htm>

“A Ministry of Economic Development document, written in response to a request for a law change by a member of the public, sets out the case against tighter controls.

The ministry said "normal investigative techniques of law enforcement agencies can often establish the identity of unregistered mobile phone users, and a prosecution would typically require additional evidence".

Also a law change could be difficult to enforce because of the use within New Zealand of unregistered mobile phones obtained overseas, and registration could be made with a false or stolen identity.”⁶

54. The draft report of the Canadian study already cited states that:

“Respondents in several [other] countries reported that prepaid registration was considered and rejected following formal public consultation or industry lobbying. These countries include Czech Republic, Ireland, Netherlands, and Poland [although] the respondents were in most cases unable to provide detailed reports about the deliberations and public statements concerning hearings in these countries.”⁷

Conclusion

55. In light of the overseas comparisons, our analysis above, and the failure of the government to provide adequate justification for the identification requirement to balance the loss of anonymity and privacy, we submit that the current Determination be withdrawn and no identification required for pre-paid mobile accounts.

56. If, notwithstanding our submission, a revised Determination is to be issued, then considerable further work and consultation is needed to deal with the range of issues and practical difficulties highlighted in this submission.

*Australian Privacy Foundation
April 2006*

Website: www.privacy.org.au
Email: mail@privacy.org.au

⁶ The Press, Mar 11th 2006

⁷ Gow, 2006, op cit (footnote 4)