Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

27 August 2010

Ms J. Nagajek
Attorney-General's Department
National Security Resilience Policy Division
Central Office
3-5 National Circuit
BARTON ACT 2600

Dear Ms Nagajek

Re: Emergency Warnings to Mobile Phones

The Australian Privacy Foundation (APF) is the country's leading advocacy organisation in the specific area of privacy. A brief backgrounder is attached.

I refer to the invitation to the APF sent by IIS to one of APF's Board members in late July. I regret that, due to the considerable efforts made by APF Board members in the lead-up to the election on 21 August, we were unable to submit a response by 20 August.

As always, the APF welcomes opportunities to engage with agencies that are developing, or considering the possible development of, projects that may have negative impacts on privacy.

We are concerned, however, about several aspects of the process used in this instance.

The first page of the attachment addresses these important process issues. The remainder identifies a number of areas of concern about the proposal itself.

Yours sincerely

Roger Clarke
Chair, Australian Privacy Foundation
(02) 6288 1472 Chair@privacy.org.au

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that 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 APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF's Board comprises professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by a Patron (Sir Zelman Cowen), and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87)
  http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90)
  http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07)
  http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-)
  http://www.privacy.org.au/Campaigns/Media/

Emergency Warnings to Mobile Phones

Concerns About the Process Undertaken

1. Confidentiality

The covering letter stated that "the information contained in this letter and the enclosed PIA is confidential".

APF's longstanding policy in relation to confidentiality and consultations is here: http://www.privacy.org.au/Papers/ConsConf.html. Briefly:

- APF can only in highly unusual circumstances accept for consideration a document that is entirely subject to confidentiality constraints
- APF is very happy to respect (and to undertake to respect) confidentiality in specific parts (or even aspects) that are drawn to attention as being in-confidence, and that warrant it

After discussion with IIS, we understand that the limitation is only that "at this stage, ... the documents should not be shared beyond the APF or the other organisations to which the document has been sent". This is constraining, and is not generally an appropriate approach to eliciting information from civil society, but the degree of openness is sufficient for us to provide a response.

2. The Process

The function of a PIA process is to surface issues, and engage in a constructive effort to identify alternative approaches that will avoid or mitigate negative impacts on privacy. A PIA Report accordingly needs to reflect the interactions that have taken place among sponsoring organisations and the representative and advocacy groups that have participated in the consultative process. Further, the PIA Report needs to integrate the various perspectives.

We note that:

(a) the covering letter states that "[IIS]) has conducted a Privacy Impact Assessment (PIA)", the document provided to us is not marked 'Draft', and s.5.6 refers to the writing of the final Report in the past tense. We therefore infer that the PIA Report has been completed

(b) there seems to be no scope for change in the document we are being asked to comment on

(c) no opportunity has been provided for interactions between AGD and the representative and consultancy organisations

(d) no opportunity has been provided for interactions among the representative and consultancy organisations that have been invited to comment (which we understand to have included at least APF, ACCAN and EFA, but perhaps also other organisations)

(e) the covering letter indicates that the submissions of these organisations would be provided to COAG separately from the PIA Report.

Each of these represents a serious weakness in the process that has been adopted. They have handicapped the APF in preparing its response, and they will handicap the members of COAG from appreciating the issues and the possible approaches to addressing them.

The APF accordingly submits that:

(1) the PIA process should be re-opened

(2) all submissions of representative and advocacy organisations should be provided to all other such organisations, to enable cross-fertilisation

(3) if appropriate, a further round of submissions should be invited

(4) the PIA Report should be re-worked to reflect and integrate the input from the representative and advocacy organisations

Emergency Warnings to Mobile Phones

Comments on the PIA Report version of 6 August 2010

1. Operational Use of Mobile Phone Identifiers

APF agrees that there is a clear justification for the use of mobile phone location information, by telecommunications carriers, to enable emergency warning delivery.

Further, **the design of the operational system appears to involve no disclosure of identified data beyond the carrier**.

That is a very important feature, and **the APF welcomes and supports that key aspect of the design approach adopted to the delivery of the service**.

2. Retention of the Data

The Report makes various references to retention of mobile phone numbers, in particular:

- "maintaining a secure repository of data for forensic analysis" (1.1 on p. 4); and
- "[telecommunications carriers are to be required to retain] lists of mobile phone numbers that were in a particular area at a certain point in time ... in case it is needed for an inquiry or royal commission relating to the handling of the emergency" (12.6 on p. 32, emphases added).

No explanation is provided of why the need exists.

Dependence on a 'just in case' justification is a source of serious concern.

The APF does not believe that any case has been made for the retention of the lists of numbers.

The APF strongly opposes the retention of the data, and does not agree with the Report's position of merely accepting that data will be retained.

In the event that a sufficient justification were to be demonstrated, and accepted by advocacy organisations as being sufficient, then the APF would strongly support the Report's Recommendation 5 relating to encryption and audit.

Further, no boundary is defined for retention of the data, and the Report notes that "key privacy risks associated with the proposed system ... include ... information will be kept for longer than is strictly necessary".

The APF strongly supports the Report's Recommendation 6 relating to deletion.

3. Scope of Use

The Report does not provide clear information about the circumstances in which it is envisaged that the scheme could be applied.

All that appears to be available is vague references such as:

- "targeted emergency warning messages that will reach more people located in an area experiencing an emergency" (1.3 on p. 5);
- "Emergency Alert ... has been used 37 times [in the 8 months since it came into operation] ... in New South Wales, Victoria, South Australia and Queensland for flood, tsunami, bushfire, chemical incidents and lost child emergencies" (6.1 on p.13);
- "[the trigger for invocation of the process is that] an emergency occurs or is deemed likely to occur by the relevant State/Territory authority" (8 on p. 15, emphases added).

Further, the Report acknowledges that:

- "Given the authorisation processes in place within jurisdictions, and jurisdictional disaster and emergency legislation, [use of the capability for an increasingly wide range of emergencies] ... is something that could emerge in the future" (re IPP2 on p.20);
- "There may be a risk that a telecommunications carrier might seek to use the capability developed for emergency purposes for commercial purposes. However, restrictions imposed by the Privacy Act and Telecommunications Act are likely to address this risk" (re NPP2 on p. 24); and hence
- "key privacy risks associated with the proposed system ... include ... extensions in the uses made of the new location-based mobile phone emergency warning capability without reference to community response or privacy implications" (1.3 on p. 6).

Firstly, the APF is concerned that no assessment has been performed of the extent to which telecommunications carriers are actually constrained by law in relation to use of the data.

The APF accordingly urges that a check of the legal constraints on telecommunications carriers be undertaken as part of this PIA process, and that the conclusions and any necessary Recommendations be integrated into the PIA Report, and communicated to the organisations that have been involved in this consultation process.

Secondly, the APF is seriously concerned that no clear rules concerning invocation of the scheme appear to have been specified, and hence function creep appears to be uncontrolled.

Although the APF supports Recommendations 1 (Transparency), 2 (Public Education), 3 (Accountability) and 7 (Review), they are inadequate by themselves, and must be complemented by a front-end control.

The APF accordingly urges that further Recommendations be inserted (logically, at the beginning of the list), to the following effect:

- **that a definition be included within the scheme of the nature of an emergency that can be used to trigger the scheme's use, such definition to be of sufficient clarity that there is no risk of delays in implementation for the key purposes that the public strongly support, but that function creep is prevented**
- **that the definition be given legal effect, through the authorisation of those, and only those, interpretations of an emergency that can be used to trigger the scheme's use**