Australian
Privacy
Foundation
post: GPO Box 1196
Sydney NSW 2001
email: mail@privacy.org.au
web: www.privacy.org.au

Use of IPND information to provide Location Dependent Carriage Services (LDCS)

Discussion Paper

Australian Privacy Foundation submission to the Department of Communications Information Technology and the Arts

August 2007

The Australian Privacy Foundation

The Australian Privacy Foundation (APF) is the leading non-governmental organisation dedicated to protecting the privacy rights of Australians. We aim to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians.

Since 1987 the Australian Privacy Foundation has led the defence of the rights of individuals to control their personal information and to be free of excessive intrusions. We use the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed.

For further information about the organisation, see www.privacy.org.au

1. Introduction

The relevant legislation and legislative instruments for this issue include:

- Telecommunications Act 1997 (the Act), particularly Part 13
- Privacy Act 1988, Schedule 3 (National Privacy Principles)
- ACIF C555:2007 Integrated Public Number Database Industry Code (IPND Code)

The IPND Scheme, mentioned in Discussion Paper, only applies to the use of IPND data for research and for public number directories and directory assistance services; it does not deal with the use of IPND data for the provision of location dependent carriage services (LDCS) – although we think it should – see comments below on limited scope of the review.

2. Protection of telecommunications customer information – General Position

The overlapping effect Part 13 of the Act and the Privacy Act NPPs is broadly to ensure that personal particulars/information[1] is only collected, used and disclosed when reasonably necessary and are kept secure, and in the case of the NPPs that

(a) individuals are informed about the collection, use and disclosure of that information, and
(b) certain other obligations and rights attach to the information.

In the telecommunications environment, personal particulars/information includes a customer's name, address and telephone number(s). Even a number or an address alone would be 'personal particulars' and

[1] Part 13 of the TA protects 'affairs or personal particulars' - undefined and implicitly not synonymous with 'personal information' under the Privacy Act.

'personal' information' if it is reasonably easy to identify an individual associated with them. .

APF was a member of the ACIF Working Committees that developed all of the versions of the IPND Code (the 2000 and 2002 versions as well as the current 2007 version). While the AFP is reasonably comfortable with the Code, it has significant reservations about the overall privacy protection offered by the confusing interaction of the TA, the PA, and in particular, in this context, the IPND Scheme. Those reservations are detailed in our submissions to the current ALRC Privacy Review and to DCITA and ACMA in relation to the IPND amendments to the TA and the IPND Scheme (see www.privacy.org.au).

Limited scope of the review

We note that the definition of LDCS in the Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997 (CLC) (and carried over into the IPND Code), limits LDCS in effect to 'inbound' call services, and excludes services that make outbound calls (or messages) to those users based on their geographic location.

While the current review has an immediate agenda, we find it disappointing that the Department has yet again missed an opportunity to review policy in a wider 'technology neutral' context and has also again failed to look at the bigger picture in terms of the regulation of the use of telecommunications data whether it falls under the jurisdiction of the Telecommunications Act (when handled by sections of the industry) or the Privacy Act (most users) or both (sections of the industry).

Whatever action is taken to resolve the immediate issue of LDCS access to IPND data, we urge the Department, together with the Attorney-General's Department and the Office of the Privacy Commissioner, to urgently conduct a second stage review looking at these wider issues.

3. LDCS access to IPND data

Both the IPND Code and the CLC provide for CSPs to access IPND data for the provision of LDCS. The starting point of the Discussion Paper is that the Telecommunications Act conflicts with this.

We are not persuaded that s.291 of the TA prevents the provision of information for all non-customers of the requesting LDCS provider. The Discussion Paper assumes that s.291 applies to the IPND Manager (Telstra) in its capacity as a CSP (p.10). In that capacity, since most of the numbers in the IPND are those of Telstra customers, the IPND Manager is allowed to disclose these for LDCS purposes under s.291(1)(c)(i).

The only constraint would therefore seem to be on disclosure of those numbers in the IPND that are those of persons who are neither customers of Telstra nor customers of the requesting LDCS provider. We nevertheless accept that this could be a sizeable population and still prevents LDCS providers from accessing required information about the complete set of public numbers. The issue raised in the Discussion Paper therefore still needs to be addressed.

However, as you will see below, we are not persuaded that 'personal particulars' are necessary for LDCS. If LDCS needs can be met, as we suggest, with partial information from the IPND, then the issue of s.291 compliance may not arise in the first place.

To the extent that it is confirmed:

(a) that LDCS requires 'personal particulars' from the IPND

(b) that the TA prevents access to Public Number Customer Data (PNCD) about all assigned numbers

then we have no objection in principle to an amendment that would allow this access.

However, we believe that CSP access to IPND data for the purpose of providing LDCS should be strictly limited to that which is necessary, and subject to strict safeguards.

Do LDCS require 'personal particulars' covered by s.291?

All versions of the IPND Code contain the following definition of Location Dependent Carriage Service Data, being the data agreed by industry members on the ACIF Working Committee as necessary for LDCS:

> **Location Dependent Carriage Service Data**
> means the data relevant to a Customer excluding the Customer's name but including:
> a) the Public Number;
> b) the address of the Customer which is:
> (i) for a Local Service, the service address as installed, unless not technically feasible; or
> (ii) for a PMTS, the physical address, where practicable, as provided by the Customer;
> c) a code that can be used to identify the CSP that provides:
> (i) service for the originating or terminating Carriage Services to the Customer; or
> (ii) PMTS to the Customer; and
> d) an indication of whether the service is to be a Listed Entry, an Unlisted Entry or a Suppressed Address

This definition was not reviewed in the last revision by ACIF but we think in the context of the Discussion Paper it needs to be.

It is not immediately obvious why, for the purposes of LDCS, providers need a full street address, or even the full telephone number.

The principle underlying any new provisions should be to permit only as much information to be disclosed as is necessary for the purpose – this would complement the Privacy Act obligation on the LDCS providers to only collect necessary personal information (NPP1.1) and to wherever lawful and practicable allow anonymous transactions (NPP8)

For **fixed line services**. we believe that the release of Location Dependent Carriage Service Data to CSPs should be restricted to the geographic part of the number (the area code and next four digits?) and/or the suburb and/or postcode part of the service address. This should suffice to allow the LDCS provider to route the call to the nearest relevant location. The customer's name should not in any circumstances be necessary, and nor should the full number or full address.

For **mobile services**, we are not aware that there is any information in the IPND that would be relevant and useful for LDCS. Mobile numbers are not geographic, and the subscriber's billing address cannot reliably be used for LDCS. Mobile origin Location Information (MOLI) that can geographically locate the cell from which the call is made may well be of use but this is not available through the IPND and should if required be pursued separately, as should access to any GPS information which is increasingly becoming integrated with mobile phones.

If for reasons that have yet to be explained it is considered necessary for detailed addresses to derive location for LDCS, then we suggest consideration of another alternative, which we are disappointed is not even mentioned in the Discussion Paper. This is establishment of a central 'location' directory – either as part of the IPND or separately. One of the main issues that the Discussion Paper addresses is the risk of distributing public number customer data more widely, with all of the issues about controlling secondary uses which this necessarily invokes. A central location directory and automated 'look up' service could provide LDCS providers with location information without them needing to acquire any address information at all.

4. Response to Specific Options/Questions

Our overall response to the three options has already been given above. Here we address specific issues that come up under one or more of the options.

4.1 Option 1 – No change

Given the obvious uncertainty as to the current position, and also our doubts about whether LDCS data as defined in the IPND Code is all required for LDCS, we do not favour this option. It is desirable to clarify the position and at the same time establish a more rigorous regime allowing access only as required and subject to strong safeguards.

4.2 Option 2

As outlined above, APF supports in principle those CSPs wishing to provide LDCS having access to the minimum information that is actually required for the purposes of providing the LDCS. This would be consistent with the IPND Code.

In response to the other questions asked under this heading:

- **Liability for unauthorised secondary use**: If CSPs are to be given access to any personal particulars/information, they will already be liable under the TA for any use and disclosure of information. Further, CSPs who are Data Users under the IPND Code can only use IPND data for an approved purpose, and can be directed by ACMA to comply with those Code provisions.
- **CSP liability under the IPND Scheme**: – this is not relevant as the IPND Scheme does not currently deal with the provision of IPND date for the provision of LDCS. However, as already noted above, we favour a comprehensive review of the IPND Scheme to ensure that it applies to all providers of directories and directory services, and such a review could also consider extending the scheme to cover CSPs accessing IPND data for all purposes including LDCS .

4.3 Option 3

APF opposes non-CSPs being given direct access to IPND data for the purpose of providing LDCS. While CSPs may contract with other non-CSPs in the provision of LDCS, the responsibility for receipt, use and disclosure of any IPND data should remain directly with the CSPs.

While the Discussion Paper proposes that entities that are not CSPs may be declared as 'sections of the industry under section 110 of the Act so they could be directly provided with access to IPND data, it is likely that such entities are not directly tied to telecommunications in any way, and so would not likely be declared. In that case, ACMA jurisdiction would not extend to those entities for the purpose of ACMA enforcement of rules surrounding that access.

Further, the jurisdiction of the TIO is limited to carriers and CSPs that supply an eligible service (standard telephone service, public mobile service, or internet access service). Therefore, public access to an effective complaint mechanism for breach of rules regarding access to IPND data would also not be possible when the entity involved is not a carrier or CSP. Non-CSP entities may be subject to the Privacy Act and its complaint mechanism, but the Privacy Commissioner would only be able to address general compliance with the NPPs, and would not be able to deal with breaches of the specific TA rules governing access to the IPND data.

4.4 Response to Other Issues

- **Use of silent numbers in the provision of LDCS**: If as we suggest LDCS only requires information that is not personal particulars/information, then there would be no privacy objection to disclosing location information about numbers which are not unlisted in the IPND for the provision of LDCS .
- **Disclosure of unlisted numbers to non-CSPs**: As stated above, AFB opposes the release of IPND data to non-CSPs.

4.5 Response to the proposed disclosure of personal information, including unlisted number information, to the called business

APF opposes the disclosure of personal information, particularly any unlisted number information, to the called business, without the informed consent of the individual concerned. Under the ACIF C522: 2007 Calling Number Display Industry Code, carriers and CSPs must ensure that, if a customer has chosen to block the sending of the CND information, that information (the CLI) does not leave the network where it could then be accessed by the called party if that party has subscribed to a CND service. Silent lines have CLI information blocked by default. Ultimately, the customer has a choice as to whether their CLI information is blocked, and that choice must be respected and upheld.

CLI information is exchanged between CSPs, even where the customer has chosen to block it, for the purposes of completing the required network transaction, and this is allowed under the 'business needs' exceptions in Part 13. APF has previously complained about what we regard as abuses of these exceptions, with our complaint being upheld by the then ACA, but without any action being taken against the CSPs involved. We urge DCITA to ensure that any amendments relating to access to IPND data for LDCS specifically address the issue of how the 'business needs' exception applies to the disclosure of CLI where a line or call block is in place.

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.