

Author: Anonymous

After a brief read of the Code, and in respect of my own personal experiences, I have the following comments:

General Comments

- The Code does not appear to place enough emphasis on appropriate management of personal data. While I appreciate that other Privacy legislation may often be sufficient, there are limitations, particularly in respect of the management of IPND data, the voluntary provision of data to other parties such as Sensis and ACMA's powers to authorise release of IPND data.
- The Role and Obligations of Communications Compliance in Appendix 1 could be expanded to require details to be published on their website of who can access IPND data and the terms of that access. Excluding access for emergency services, law enforcement or national security purposes this list could include all Carriers and CSP's and ACMA's terms and conditions of approvals for other bodies (for example, for printed and public number directories (PND's) and research purposes) who have access to or can receive IPND data. This list could also include links to websites, email addresses and contact phone numbers of those entities with access to IPND data so that consumers can contact them directly.
 - Ideally, the Code should require Carriers and CSPs also to inform customers (eg by up to date website info) of this information.
 - This obligation on Communications Compliance, Carriers and/or CSP's would place pressure on ACMA and/or the IPND Manager to at least inform those groups where and how the data is distributed.
 - Despite the publicity over recent years, a large number of consumers would not be aware of the role of the IPND, the difference between IPND and Sensis data or how extensively IPND data can be accessed and distributed.
 - Currently, it is unlikely that CSPs have sufficient knowledge as to how IPND data is accessed and distributed and it is possible that frontline staff of CSPs are even not aware of the differences between IPND and Sensis data.
 - Neither the IPND Manager (currently Telstra) or ACMA appear to publish details or terms of ACMA's approvals to access IPND data so there is no ability for consumers to identify recipients of that data so that they can monitor the accuracy or use of that data (for example as per Privacy legislation). One PND provider even only freely provides data it has extracted from the IPND to its own clients and not the general public and it is not possible for consumers to check whether this arrangement is consistent with the terms of ACMA's approval to access IPND data.
- As I understand it, CSP's currently voluntarily provide data to Sensis which is separate to the data that is provided to the IPND. This should be discouraged and, like all other directory and PND providers, Sensis should be persuaded to seek approval from ACMA to extract relevant data from the IPND. To achieve this, the Code could require CSPs to cease providing data directly to Sensis from a future date.
 - This would ensure that customers, who are more likely to be familiar with Sensis than any other directory provider, would have a better chance of knowing what personal data is held in the IPND.
 - This would also remove a potentially growing competitive advantage whereby at least one PND provider has access to (and promotes that they have access to) both IPND and Sensis data. (If the data held in the IPND and by Sensis was the same why would anyone need to spend resources extracting and promoting that they have separate sets of data from two different sources?)

- While I appreciate that it would be outside the original intent of the Code or the role of the TIO, consideration could be given to extending the Code in the future (with a statement of intent in this Code) to permit other related parties to become voluntarily parties to the Code (eg, the IPND Manager, public directories (eg Sensis, Veda, FCS OnLine, Acceleon and Local Directories) and possibly even ACMA). In the future the Code could be expanded in respect of those other parties to meet perceived deficiencies in other legislation.

Specific Comments

- Clause 4.6.3 which relates to the Storage and Security (and access) of data should be expanded to include obligations on the CSP in respect of data reported to and held by the IPND Manager and other entities such as Sensis. It could be argued that the CSP's obligations under 4.6.3 only extend to data held within the organisation and that there is no obligation on the CSP to ensure that correct data is reported to the IPND Manager (and to Sensis) or to audit the accuracy of data once recorded in the IPND.
 - As noted above, currently customers have no means of monitoring IPND data other than by requesting it from the CSP or ACMA. Also Privacy legislation does not appear to apply to CSPs and ACMA in respect of this data as the data is held by the IPND Manager and not the CSPs or ACMA.
 - Also, there is no apparent obligation on CSPs to advise customers when the CSP proposes to take action that will alter data held in the IPND or by Sensis. For example, this requirement would ensure that CSP's are obligated to respond to customer enquiries about IPND data - including historical IPND data - (which consumers also can't access directly from the IPND Manager). It would also ensure, for example, that CSPs advised consumers when IPND data is altered, such as when an UnListed entry or a Suppressed Address entry is changed to a Listed Entry.
- Clause 4.6.3 only appears to apply while a person continues to be a customer of the CSP. Any data held, reported or used by the CSP in respect of a former customer should also be subject to this clause.
- Clause 7.5 should be expanded to ensure that gaining CSP's inform customers of their need to re-establish any Unlisted/Silent Number or Suppressed Address Listing on a change of provider (or the gaining CSP should assume, as a default, that the listing is an Unlisted entry). As I understand it, currently, suppressed details are commonly inadvertently listed when consumers change CSPs (or even change their contracts with an existing CSP) because the consumers are often not aware that they need to reestablish this listing each time.
- Clause 7.7 and 7.8 should be expanded to include data reported to and held in the IPND in respect of the customer.
 - Also, if Clause 4.6.3 does not cover data held or reported in respect of former customers, a less desirable alternative would be to expand Clauses 7.7 and 7.8 to ensure that historic IPND data (ie that was reported by a former CSP) can be retrieved from the new CSP if requested by the customer.