Australian Government | acma

Australian Communications and Media Authority
communicating | facilitating | regulating

Investigation Report

File No.	ACMA2018/409-2
Carriage Service Provider	Singtel Optus Pty Ltd ACN 052 833 208
Type of Service	Carriage Service Provider
Relevant Legislation/Code	- *Telecommunications Act 1997* - *Industry Code (C555:2017) Integrated Public Number Database (IPND)*
Date	13 December 2018

Findings

The Australian Communications and Media Authority (the **ACMA**) finds that, on multiple occasions, Singtel Optus Pty Ltd ACN 052 833 208 (**Optus**):

> contravened subsection 101(1) of the *Telecommunications Act 1997* (the **Act**), which requires a carriage service provider (**CSP**) to comply with the service provider rules that apply to it, by failing to give Telstra Corporation Limited (**Telstra**, or the **IPND Manager**) the information it reasonably required to provide and maintain the Integrated Public Number Database (**IPND**), thereby contravening the service provider rule in clause 10 of Schedule 2 to the Act.

> contravened the following clauses of the *Industry Code (C555:2017) Integrated Public Number Database (IPND)* (the **IPND Code**):

- 4.2.1 – because Optus, a CSP that provides carriage services to customers using public numbers[1], failed to provide the relevant public number customer data[2] to the IPND Manager in respect of certain carriage services Optus supplies;
- 4.2.11 – because Optus failed to ensure that the public number customer data it provided to the IPND Manager was accurate, complete and up to date; and
- 4.2.25 – because Optus failed to supply to the IPND Manager public number customer data updates that occurred on one business day, by the end of the next business day.

[1] In this report, *number* and *public number* mean a number under in the *Telecommunications Numbering Plan 2015.*
[2] As defined in the IPND Code, where it is also referred to as 'PNCD'.

Background

1. This report details findings of an investigation conducted by the ACMA under paragraphs 510(1)(a) and (c) of the Act into whether Optus contravened the Act and/or an industry code registered under Part 6 of the Act.

2. The investigation commenced on 16 July 2018. On 18 July 2018, the ACMA issued Optus a notice under section 521 of the Act requiring the production of documents and information (the **Notice**).

3. Optus responded to the Notice on 31 August 2018 and provided further information on 25 September 2018.

4. On 11 October 2018, the ACMA issued preliminary findings to Optus. Optus responded on 2 November 2018, providing information it considers relevant to giving a more complete picture of the findings.

Relevant facts

5. Optus is a CSP within the meaning of the Act[3]. Optus supplies, among other things, fixed-line and mobile telecommunications services to residential, business and government customers. Optus also supplies telecommunications services on a wholesale basis to other retail CSPs.

6. Optus is a 'Data Provider' within the meaning of clause 2.2 of the IPND Code.[4]

The IPND and its legislative framework

7. The IPND is intended to be an industry-wide database of all public telephone numbers. It was established in 1998 and is managed by Telstra as required by section 10 of the *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997* (**Telstra Licence Conditions**). The maintenance of the IPND by the IPND Manager is supported by, among other things:

    a. a service provider rule requiring a CSP that supplies a carriage service to an end user, and where that user has a public number, to give Telstra such information as Telstra reasonably requires in connection with Telstra's fulfilment of its obligation to provide and maintain the IPND[5]; and

    b. the IPND Code, which is an industry code registered by the ACMA under Part 6 of the Act, and which sets out procedures relating to the storage of information in the IPND and the transfer of information to and from the IPND Manager.

8. The IPND Code, and the associated IPND Data Guideline (G619:2017), also refer to the *Integrated Public Number Database (IPND) Data Users and Data Providers Technical Requirements for IPND* (the **Technical Requirements**). The Technical Requirements, which are issued by Telstra and made with the agreement of a majority of relevant Data

[3] See section 87 of the Act.
[4] 'Data Provider' is defined to mean a CSP who has an obligation to provide PNCD to the IPND Manager, or an entity acting on behalf of the CSP, and who is registered with the IPND Manager.
[5] Subsection 101(1) of the Act requires CSPs to comply with the service provider rules, and paragraph 98(1)(a) of the Act provides that the service provider rules include the rules set out in Schedule 2 to the Act. Clause 10 of Schedule 2 to the Act deals with the information that CSPs must give to Telstra in association with its IPND Manager responsibilities.

Users[6] and Data Providers (see clause 7.1.8 of the IPND Code), set out the detailed operational and technical requirements for the submission of information by Data Providers to the IPND Manager.

9. The information in an IPND record includes customer name and address, phone number, the type of service, whether the service is listed or unlisted and details about the service provider. The Technical Requirements (at clause 6.1.2) specify the information that is included, or which can be included, in an IPND entry. An IPND record includes a mandatory field, called the 'Service Status Code', which is used to indicate whether a service is connected or disconnected.

10. Under Part 13 of the Act and the Telstra Licence Conditions, the information in the IPND can only be used for specific purposes. Critical users of the IPND include the emergency call service, the emergency warning system, and national security and law enforcement agencies. These bodies use IPND information to protect life and property and to investigate serious crime. Failure to provide accurate, timely and current information to critical users can have serious consequences. For example, failure to provide location information associated with a call to the Triple Zero emergency call service could place a caller's life at risk. Non-critical users of IPND data include publishers of public number directories and researchers conducting permitted research.

11. There are several ways in which a Data Provider can identify potential errors occurring when uploading data to the IPND, and any discrepancies between its own customer data and that stored in the IPND, including:

    - by reference to clause 4.2.28 of the IPND Code, which allows a Data Provider to obtain an extract of its public number customer data as a full set of records or a subset of records based on criteria agreed between the Data Provider and the IPND Manager for reconciliation purposes.
    - by reference to clauses 6.1.6 and 6.1.7 of the IPND Code, which require a Data Provider to download the information the IPND Manager produces about hard and soft errors[7], and take reasonable steps to resolve the matter and supply the corrected public number customer data to the IPND Manager within one business day for hard errors and two business for soft errors.
    - additionally, the IPND Manager sends reminders via email (at least twice a year) to the approved contact(s) of all Data Providers about the importance of checking the corresponding error file after each IPND upload to ensure the file has been processed successfully.
    - by reference to clause 6.1.10 of the IPND Code, which encourages Data Providers to check a monthly Changed Data Provider report produced by the IPND Manager, which informs the Data Provider of all numbers gained and lost in the last month.

[6] As defined in clause 2.2 of the IPND Code.

[7] 'Hard' and 'soft' errors are identified during the IPND's validation process when a Data Provider attempts to upload a file of IPND records (a file may contain one or more records). A hard error, such as mandatory field in the IPND record being blank, prevents the upload of the file and/or the record containing the hard error to the IPND. A soft error is a possible error in an individual field of a record. In this case, the file is still uploaded to the IPND but is tagged as having a 'soft' error. A soft error can signify potential name and/or address inaccuracies, or missing information within an IPND record. The IPND Manager makes reports about hard and soft errors available to Data Providers.

Optus' response to the Notice

12. Upon carrying out a comparison of its customer database against its records in the IPND (as compelled to do so by the ACMA in relation to the Notice), Optus submitted:

    a. **852,871** public numbers associated with an Optus 'active' service do not have a corresponding record in the IPND;

    b. **3,585,233** public numbers associated with an Optus service are affected by incorrect data, made up of:

        i. 307,048 public numbers associated with Optus 'active' services which have a 'disconnected' status in the corresponding IPND record;

        ii. 911,978 records associated with Optus with a 'connected' status in the IPND which are shown as 'disconnected' in Optus' customer database;

        iii. 2,366,207 records associated with Optus with a 'connected' status in the IPND which are not present in Optus' customer database.

13. Optus also stated that:

    a. The figures referred to at paragraph 12 above would change as Optus conducts further analysis.

    b. It was concerned about the findings and was working to urgently confirm the root cause/s of the discrepancy and address the gap.

    c. It takes its IPND obligations seriously and appreciates the critical role that complete and accurate IPND records play. Optus' initial priority was to ensure missing IPND records were uploaded to minimise the risk of public harm, and that resources were secured to undertake complex root cause analysis to explain why records are missing and develop a detailed mitigation strategy and plan.

    d. Its senior management had been made aware of the investigation and would retain oversight of mitigation activity. Optus was taking urgent corrective action to ensure all outstanding record discrepancies were explained and addressed. It would provide updates to the ACMA on the following mitigation plan:

        i. It would provide the ACMA with a monthly update on the progress of addressing all outstanding record discrepancies, until they are resolved.

        ii. It would develop an IPND compliance plan that would include the following key tasks:

            - add missing or amend incorrectly classified Optus records in the IPND;
            - identify root cause and find solutions to address potential recurrence of errors;
            - review IPND policies, processes, and systems as required; and
            - once it is firmly established that all records are present in the IPND, focus on increasing the quality of those records.

        iii. It also proposes to support change at an industry level through review of the IPND Code.

14. Optus subsequently provided information to the ACMA stating that, in its view, the total number of missing records should be reduced because:

    a. active services initially reported as Optus services (by Optus) should be attributed to its wholesale customers; and

    b. certain records required further consideration of whether they were in fact missing from the IPND.

15. The ACMA accepted that the services referred to at paragraph 14a were not services in respect of which Optus was obligated to provide public number customer data to the IPND. This was because Optus was not the entity providing a carriage service to an end user in connection with the relevant public numbers. The ACMA therefore excluded them from further consideration.

16. The records at subparagraph 14b were included in the preliminary findings pending further analysis, but excluded from the final findings for the reasons at paragraph 18 below.

Optus' response to the Preliminary Findings

17. The ACMA's preliminary findings set out that Optus had contravened the service provider rule and the IPND Code in relation to:

    a. **732,757** active services with no record in the IPND. This figure comprised 852,871 services identified by Optus in response to the Notice, less 120,505 services subsequently identified as wholesale services (see subparagraph 14a above), plus 391 services confirmed by Optus as missing prior to the start of the investigation.

    b. **3,585,233** IPND records with an inaccurate Service Status Code being the total of the figures provided by Optus in response to the Notice.

18. Analysis by the ACMA in relation to records referred to at subparagraph 14b indicates these records are likely to be in the IPND. On this basis, the total of Optus' missing records has been reduced from 732,757 to **493,886**.

19. In response to the preliminary findings, Optus submitted a remediation update and a further revision upwards of the figures relating to inaccurate records (from **3,585,233** to **3,799,386**).

20. Optus also submitted the following:

    > It reiterated that its priority remains updating missing records to the IPND given they represent the greatest potential risk of harm to an individual.

    > It acknowledged that the evidence available suggests a large number of active Optus services do not have a corresponding IPND record.

    > It was not able, at the time, to provide an explanation or root cause analysis which comprehensively explains the reason(s) for the missing IPND records.

    > It considers a number of facts and issues are relevant to providing a more complete picture and placing the number of missing records in context, including:

a. the scale of its' business operations. Optus provides services to over 11 million customers every day, including fixed, mobile, broadband, satellite and content services;

b. that since the inception of the IPND, it has been an entity which has invested in IT systems and business processes with the objective of fully complying with its IPND obligations. Optus noted that it devoted resources to ensure new systems were designed to service the IPND data feed, including system testing;

c. that it has engaged constructively with the ACMA on matters relating to the on-going improvement in data quality of records in the IPND over the last twenty years.

- It is reasonable to conclude that Optus' IT ecosystem in aggregate is not performing as expected. As such, it now has a substantial diagnostic task to undertake root cause analysis to identify the components of its IT systems which are not contributing correctly to maintaining a full set of IPND records. Based on inquiries to date, it is likely that there is more than one contributing factor as there appear to be mis-matches affecting different service types which are supported from different upstream IT systems.
- That neither the primary legislation, the IPND Code nor operational practice with the IPND Manager provides CSPs with a recommended practice or guidance, or a specific obligation, about when and how to undertake a full-scale reconciliation of the provider's services in operation compared to the stock of records in the IPND.
- It considers that if the legislative or regulatory framework had been more instructive, or if industry processes or the IPND Manager had guidance on best practice for reconciling the sum of IPND records and services in operation across the industry, then there may be greater inbuilt capability in the IPND ecosystem to explain missing records.
- On the information available, there may be several factors which contribute to the missing records including overwriting of records by other providers and shortcomings in Optus' internal systems and processes (including failure to check Changed Data Provider reports) across its various business units and service types.

21. Optus subsequently provided information indicating that its systems may treat connected and ready to be connected numbers in a similar way. This could impact upon the accuracy of the data it has provided and, therefore, the numbers of contraventions. Optus has not provided any substantive or further information on this point.

22. Optus also advised it is building an IPND Compliance Assessment Tool as part of its IPND risk mitigation activity. The intention of the tool is to provide a simple compliance dashboard to increase visibility and IPND governance, including senior management oversight. The dashboard is intended to:

- provide visibility of any backlog of missing records or errors that need to be fixed;
- report on the volume and status of internal errors and daily IPND hard and soft errors;
- highlight errors for repair; and

- provide output on comparison between the monthly IPND Changed Data Provider reports and validated churn – to identify records that may have been erroneously overwritten for investigation.

Optus anticipates having a working prototype by the end of January 2019.

Findings and reasons

Compliance with the Act

23. Subsection 101(1) of the Act requires that service providers, including CSPs, comply with the service provider rules that apply to them. Subsection 98(1) of the Act provides that the service provider rules include those set out in Schedule 2 to the Act.

24. Clause 1 of Schedule 2 to the Act provides that service providers must comply with the Act. Clause 10 of Schedule 2 requires that where a CSP supplies a carriage service to an end-user, and the end-user has a public number, the CSP must give Telstra (as the IPND Manager) such information as Telstra reasonably requires to fulfil its obligation to provide and maintain an IPND.

Clause 10 of Schedule 2

25. In determining what information, the IPND Manager reasonably requires in order to fulfil its obligation to provide and maintain an IPND, the ACMA has regard to the Act, the Telstra Licence Conditions, the IPND Code and the Technical Requirements.

26. Subclause 10(4) of the Telstra Licence Conditions requires that the IPND must include, among other things, the public number, and the name and address of the customer. It is reasonable for Telstra to require that information which the Telstra Licence Conditions require it to obtain, and which are essential to the maintenance of the IPND.

27. Further, the IPND Manager may reasonably require other information that will assist in delivering the objectives of the IPND. Having regard to the critical functions described in paragraph 10 above, the ACMA considers that the service status of a number (that is, 'connected' or 'disconnected') is important to the proper functioning of the IPND, given that an incorrect status could adversely impact Data Users' services (noting that researchers and public number directory publishers only receive connected records). It could also cause severe detriment in some cases (if, for example, a service did not receive an emergency warning because it was listed as 'disconnected').

28. The IPND Manager has explicitly sought the service status information from Data Providers in respect of each IPND entry, via the Technical Requirements. As noted above, the Service Status Code is a mandatory IPND field (others are optional), and the Technical Requirements have been made in consultation with, and with the agreement of, Data Providers. Further, clause 4.2.10 of the IPND Code provides that Data Providers must ensure that all public number customer data transferred to the IPND Manager is in the format specified in the Technical Requirements; and clause 4.2.11 provides that the Data Provider must ensure that the information provided to the IPND Manager is accurate, complete, and up to date.

29. Considering the above, the ACMA is satisfied that the IPND Manager reasonably requires CSPs to provide correct information about whether a telephone number is

connected or disconnected to fulfil its obligations as IPND Manager. By uploading information that incorrectly identified connected telephone numbers as 'disconnected', and disconnected telephone numbers as 'connected', Optus did not give the IPND Manager the information it reasonably required to fulfil its obligation to maintain the IPND.

30. Based on information provided by Optus it did not upload public number customer data to the IPND for 493,886 public numbers and Optus customer data for 3,799,386 public numbers has, at a minimum, an incorrect connection status[8].

31. The ACMA therefore finds that Optus contravened clause 10 of Schedule 2 to the Act.

32. Accordingly, the ACMA finds Optus contravened subsection 101(1) of the Act as it failed to comply with the service provider rule in clause 10 of Schedule 2 to the Act.

Compliance with the IPND Code

33. The IPND Code is an industry code registered under Part 6 of the Act[9] which applies to CSPs (among others).[10]

Clause 4.2.1

34. Section 4.2 of the IPND Code sets out rules in relation to the provision of data to the IPND Manager. As noted above, clause 4.2.1 of the IPND Code obliges a CSP to supply relevant public number customer data (also referred to as PNCD) to the IPND Manager for each public number it uses to supply a carriage service. Optus is a CSP within the meaning of the IPND Code.

35. Public number customer data includes, among other things, the public number, and the name and address of the customer, as referenced in the Telstra Licence Conditions and the definition in clause 2.2 of the IPND Code.

36. Based on information provided by Optus, it did not upload public number customer data to the IPND for 493,886 public numbers used in connection with an active, or previously active Optus service.

37. The ACMA therefore finds that Optus contravened clause 4.2.1 of the IPND Code.

Clause 4.2.11

38. Clause 4.2.11 of the IPND Code requires a CSP to ensure that the public number customer data provided to the IPND Manager is accurate, complete and up to date.

39. Based on information provided by Optus it did not upload to the IPND public number customer data for 493,886 public numbers to the IPND, and 3,799,386 public numbers had an incorrect Service Status Code in the corresponding IPND record.

40. The ACMA therefore finds that Optus contravened clause 4.2.11 of the IPND Code as it failed to ensure that the information it provided to the IPND Manager in those instances was accurate, complete and up-to-date.

[8] This investigation has not considered whether other fields in the relevant IPND records contain inaccuracies.
[9] The IPND Code is registered under section 117 of the Act.
[10] See cl. 1.3.1(b) of the IPND Code.

Clause 4.2.25

41. Clause 4.2.25 of the IPND Code requires a CSP to supply to the IPND Manager all public number customer data updates that occur on one business day, by the end of the next business day.

42. Public number customer data updates can include a change to the customer data for an existing number, or any new or ported numbers for which customer data has not previously been provided by the CSP.

43. Based on information provided by Optus, it did not upload to the IPND public number customer data for 493,886 public numbers to the IPND, and there were 3,799,386 public numbers with an incorrect Service Status Code in the corresponding IPND record. Optus made no claim that these numbers were for services that were newly connected, ported or disconnected and that the time limit for uploading or updating IPND customer data had not expired. Consequently, updates for these services were not supplied to the IPND within the requisite timeframe.

44. The ACMA therefore finds that Optus contravened clause 4.2.25 of the IPND Code by failing to supply public number customer data updates that occurred on one business day, by the end of the next business day.