Commissioner Initiated Investigation into Singtel Optus Pty Ltd (Privacy) [2026] AICmr 22 (20 March 2026)

Decision and reasons for decision of

Privacy Commissioner, Carly Kind

Respondent	Singtel Optus Pty Ltd
Decision date	20 March 2026
Case reference number	CII20/00001
Catchwords	Privacy — *Privacy Act 1988* (Cth) — Australian Privacy Principles — APP 11.1 — Whether reasonable steps taken to protect personal information — Must not repeat or continue acts and practices found to be an interference with individuals' privacy.

Determination

1. I find that Singtel Optus Pty Ltd (**respondent**) interfered with the privacy of individuals, namely individuals whose personal information was listed in the White Pages contrary to an expressed preference or request for an unlisted number, within the meaning of s 13(1) of the *Privacy Act 1988* (Cth) (**Privacy Act**) by:
   a. failing to take such steps as were reasonable in the circumstances to protect that personal information from unauthorised disclosure, in breach of Australian Privacy Principle (**APP**) 11.1, between 1 October 2015 to 27 September 2019 (**relevant period**).

Declarations

2. I declare, under s 52(1A)(a) of the Privacy Act, that the acts and practices of the respondent as outlined at paragraph 1, constitute an interference with the privacy of individuals and that the respondent must not repeat or continue the acts and practices.

Findings and Reasons

Key issues

3. This matter concerns the publication of personal information in the White Pages, against the explicit request or instruction of the individuals concerned. The Office of the Australian Information Commissioner's (**OAIC**) investigation, and my resulting determination, concerns the respondent's compliance with APP11.1, which requires an entity that is subject to the Privacy Act to take reasonable steps to protect personal information from unauthorised disclosure.
4. Although some of the issues that the determination engages with are now outdated, due to the time that has elapsed since the incident, this determination provides further guidance on the application of APP 11.1 to the conduct of highly sophisticated regulated entities, and in particular with respect to expectations as to steps required to be taken to address and mitigate known and persistent security risks.
5. Given the dated nature of the contravention of APP11.1 and the steps taken by the respondent, I do not propose to make declarations beyond that in paragraph [2]. However, I intend to apply the findings in this determination to the OAIC's investigation into a representative complaint relating to the same conduct, in relation to individuals who were affected by unauthorised disclosure of their personal information in the White Pages, as described at paragraphs [34] to [37]. I intend to consider compensation for this class of individuals in a determination with respect to the representative complaint in due course.

Factual background[1]

6. The respondent is a carriage service provider (**CSP**) within the meaning of s 87 of the *Telecommunications Act 1997* (Cth) (**Telecommunications Act**). This matter concerns the acts and practices of the respondent during the relevant period.

The public number directory

7. Pursuant to cl 9(1) of the Telecommunications (Carrier Licence Conditions – Telstra Corporation Limited) Declaration 2019 (**Telstra Licence Conditions**), Telstra was obliged to produce an "alphabetical public number directory" annually.[2] Under cl 9(1)(d), the alphabetical public number directory should include all customers of CSPs supplied with standard telephone service, regardless of who supplies them with that service.[3]
8. Under cl 9(7), Telstra was obliged to "ensure, to the greatest extent practicable, that the directory does not include details of a customer whose number is an unlisted number" – that is, the directory only includes 'public numbers'.[4] The Telstra Licence Conditions stipulate that a mobile number is unlisted by default, unless the customer and the CSP

[1] Facts described were correct as at 22 December 2023 at the conclusion of the OAIC's investigation.
[2] Telstra Licence Conditions cl 9(1).
[3] Telstra Licence Conditions cl 9(1)(d).
[4] *Telecommunications Act 1997* (Cth) s 285.

agree that it will be listed.[5] Geographic numbers (landlines) are listed by default and can be unlisted where the customer and the CSP agree.[6]

9. At all relevant times, Telstra was under the above obligations, or analogous obligations under earlier iterations of the Telstra Licence Conditions – including the Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997 (Cth) which was in force until March 2019.[7]

10. Since 2014, Telstra has fulfilled its obligations to maintain an alphabetical public number directory through publication of the White Pages via an arrangement with Thryv (previously named Sensis). Under this arrangement, Thryv manages the production and distribution of the White Pages.[8] Throughout this document, the name Thryv is used for the publisher of the White Pages, although at the relevant time Thryv was named Sensis (and many of the contemporary documents refer to Thryv as Sensis).

The integrated public number database

11. Under cl 10 of the Telstra Licence Conditions, Telstra was also obliged to maintain an industry-wide integrated public number database (**IPND**) for purposes including publishing public number directories, including the public number directory discussed above at paragraphs [7] to [10].[9] Under cl 10 of Schedule 2 to the Telecommunications Act, the respondent as a CSP was obliged to provide information to Telstra in connection with Telstra's obligation to maintain the IPND. The IPND Code registered by the Australian Communications and Media Authority (**ACMA**) under s117 of the Telecommunications Act imposed obligation on CSPs such as the respondent with respect to the IPND such as an obligation to provide customers "with the choice of either a Listed Entry or an Unlisted Entry and [to] make arrangements to record the Customer[']s preference" in the Public Number Customer Data (cl 4.1.1).[10]

12. The respondent uses the same back-end systems, including the interface gateway system (**System 1**), containing the same customer information, to transmit data to Telstra for the purposes of both the White Pages and IPND.[11] However, the respondent has submitted that Thryv was not a listed authorised user of the IPND and that the IPND data was not used by Telstra for the purposes of the White Pages during the relevant period.[12] For that reason I have not further considered the submission of customer information to Telstra for the purposes of the IPND as relevant to this investigation.

The Optus Access Agreement

13. Telstra and the respondent are parties to a contractual agreement (the **Optus Access Agreement**), pursuant to which the respondent provides Telstra with information (**Customer Directory Details**) for the purpose of Telstra discharging its obligation to maintain an alphabetical public number database through the publication of the White

[5] Telstra Licence Conditions cl 4.
[6] Telstra Licence Conditions cl 4.
[7] Submission prepared by Optus Counsel dated 28 September 2023 (**Counsel Submission**) at [25].
[8] Counsel Submission at [26].
[9] Telstra Licence Conditions cl 10.
[10] Letter from respondent dated 8 July 2020, Appendix A, paragraph 13.2.
[11] Letter from respondent dated 17 June 2022, Annexure 1.
[12] Counsel Submission at [36] and [75].

Pages.[13] The Optus Access Agreement was entered into on 14 August 1992, and has been varied over 279 times since that date.[14]

14. The Optus Access Agreement is a private contractual relationship (notwithstanding that it facilitates Telstra discharging its statutory functions under the Telstra Licence Conditions). At all relevant times, the respondent did not have any direct contractual arrangements with Thryv. However, the respondent had direct lines of communication with Thryv, including with respect to issues relating to the listing or unlisting of Customer Directory Details in the White Pages.

15. Pursuant to the Optus Access Agreement, the respondent was required to provide "Raw Data for Directories Purposes" (**Raw Data**) to Telstra, namely listing information (name and address) for all customers other than those whose number is unlisted. The provision of Raw Data was subject to terms and conditions including:[15]

    a. clause 12.2.1, which provides that the respondent "shall supply to NDS[16] Raw Data for Directories Purposes relating to each of its customers in accordance with the Telecommunications (General Telecommunications Licences) Declaration (No 1) of 1991".

    b. clause 12.2.2, which provides that the respondent "shall ensure that all Raw Data for Directories Purposes supplied to NDS is accurate, complete and up to date" (see also cl 12.2.5).

    c. clause 12.2.3, which requires the respondent to "… supply the Raw Data for Directories Purposes to NDS within 24 hours of the time [the respondent] provides connection of the Telecommunications Service to the customer".

    d. clause 12.2.5, which requires the respondent to "… notify NDS in an electronic form which is suitable for immediate down loading to the NDS computer database used for Alphabetical Directory purposes… from time to time of any change (including changes caused by the cessation or removal of a Telecommunications Service) in any Raw Data for Directories Purposes relating to a customer previously supplied to Telstra or of any entry in an Alphabetical Director becoming a Dead Entry, within 25 hours of [the respondent] becoming aware of the change or the entry becoming a Dead Entry".

    e. clause 12.6.1, which provides that the respondent "shall notify NDS … of any number in Raw Data for Directories Purposes which has been or is supplied to NDS which is or is to be a Silent Number or Unlisted Number. This notification shall be made by [the respondent] to NDS within 24 hours of the time [the respondent] becomes aware that the number is or is to be a Silent Number or Unlisted Number".

16. The respondent is not required under the Optus Access Agreement to provide any information to Telstra about customers with an unlisted number.[17] Telstra paid the respondent a certain amount per month for the supply of Raw Data for Directories Purposes.[18]

---

[13] Counsel Submission at [27].
[14] Letter from Telstra to the OAIC dated 19 November 2021, paragraph 1.1.
[15] Optus Access Agreement, Sch 12 at paragraphs 12.2.1 – 12.2.5 and 12.6.1.
[16] "References to "NDS" in Schedule 12 are references to the National Directory Services business division of Telstra, which is no longer in existence": Counsel Submission at [27]. For the purposes of this determination, I understand references to NDS to be references to the relevant department in Telstra.
[17] Optus Access Agreement, Sch 12 at paragraph 12.6.1.
[18] Optus Access Agreement, Sch 12 at paragraphs 12.1 (definition of 'Raw Data for Directories Purposes') and 12.6.1.

Listing and unlisting numbers in the White Pages

New Optus customers

17. During the relevant period, the respondent's customers signing up for a new mobile or geographical number could elect whether to have their number listed or unlisted in the White Pages at the time of opening an account.[19]

18. Once a new customer account was opened, the respondent would transmit the customer information of listed numbers only to Telstra via a daily secure file transfer.[20] The provision of new customer information to Telstra occurred every 24 hours via this daily secure file transfer, referred to by the respondent as "daily secure transaction files" or "daily update files" (**Daily Secure Transaction File**).[21] This process was governed by the arrangements between the respondent and Telstra outlined in the Optus Access Agreement.[22] The respondent understood that Telstra would forward the information on to Thryv for updating and maintaining the White Pages.[23]

19. At all relevant times, the respondent did not transmit the customer information of their new customers who had elected to have an unlisted number when 'signing up' for an account.[24]

Existing Optus customers

20. During the relevant period, existing customers of the respondent, who had previously elected to have a listed number, could change their White Pages publication status from 'list' to 'unlist' via several means:

    a. making a verbal request to a customer-facing Customer Service Representative via phone;

    b. submitting a hard-copy form in-store to a Customer Service Representative; or

    c. submitting an online form or, from approximately May 2017 onwards, amending their details via the 'My Account' portal.[25]

21. Following the customer making an election, the respondent's Customer Support Consultants would update its back-end system, System 1, which underpinned the Daily Secure Transaction File.[26] Within 24 hours, the respondent sent Telstra an update known as an 'unlist transaction' to notify of the need to change the customer's publication status to 'unlist'.[27] This transaction was contained in the Daily Secure Transaction File, alongside any other relevant updates to the information of the respondent's customers, including new customers' information and any changes to existing information.[28] Telstra conveyed these requests to Thryv for execution.

---

[19] *Communications Alliance Ltd Industry Code C555:2020 Integrated Public Number Database* cl 4.1.1.
[20] Letter from the respondent dated 8 July 2020, [2.2].
[21] Letter from the respondent dated 27 May 2022, paragraph 30.
[22] Letter from the respondent dated 27 May 2022, paragraph 30.
[23] Letter from the respondent dated 27 May 2022, paragraph 30.
[24] Letter from the respondent dated 8 July 2020, appendix A, paragraph 13.14.
[25] Letter from the respondent dated 8 July 2020, appendix A, paragraph 18.
[26] Letter from the respondent dated 8 July 2020, paragraph 2.3.
[27] Counsel submission at [12].
[28] Letter from the respondent dated 8 July 2020, paragraph 8.2.

22. In addition, the respondent also provided ad hoc requests directly to Thryv via email and Dropbox from time to time, to action individual list and unlist requests received from customers in relation to their White Pages listings.[29]

23. From October 2015 to October 2018, the respondent had a process where, if a customer requested an immediate or expedited directory change to a Customer Service Representative, the Customer Service Representative could use an internal web page to complete an expedited request, which generated a case for a Customer Support Consultant.[30] The respondent would communicate these changes via weekly escalation files via email directly to Thryv at optuschanges@sensis.com.au.[31] This process apparently existed outside of and despite the Optus Access Agreement in place with Telstra.[32]

24. In October 2018, Thryv informed the respondent they were not aware that this nominated email address existed and had not been processing its contents. The respondent did not receive any bounce back email or other indication that the optuschanges@sensis.com.au address was not being monitored during the three-year period it used this email address. [33]

Porting customers

25. During the relevant period, customers who were porting their service from another CSP to the respondent were, in the relevant paperwork provided by the respondent, invited to elect whether to have their number listed or unlisted in the White Pages.[34] The respondent employed the same process as employed with respect to new customers of the respondent to porting customers, that is, it transmitted the customer information of listed numbers only to Telstra via the Daily Secure Transaction File.[35]

26. During the period of 1 October 2015 to 15 March 2019, where a porting customer elected to have an unlisted number, the respondent did not transmit any customer information to Telstra.[36]

27. From around 15 March 2019 to August 2020, the respondent sent a daily email to Thryv containing a list of phone numbers of customers porting to the respondent that had requested an unlisted number.[37] This process apparently occurred outside of the Optus Access Agreement arrangements.[38]

28. From August 2020 onwards, the respondent provided Telstra with an additional audit file via secure file transfer on a daily basis (**Daily Alignment File**).[39] Each Daily Alignment File contains all active unlisted numbers from all of the respondent's Customer Relationship Management systems (between ten and eleven million entries).[40] This information is forwarded by Telstra to Thryv pursuant to an agreement between the respondent and Telstra.[41] The respondent submitted that it implemented this arrangement because Thryv

[29] Letter from the respondent dated 27 May 2022, paragraph 30.
[30] Letter from the respondent dated 6 December 2021, paragraph 7.
[31] Letter from the respondent dated 6 December 2021, paragraph 7(b).
[32] Letter from the respondent dated 6 December 2021, paragraph 7.
[33] Letter from the respondent dated 6 December 2021, paragraph 2.
[34] Letter from the respondent dated 8 July 2020, paragraph 8.1.
[35] Letter from the respondent dated 8 July 2020.
[36] Letter from the respondent dated 8 July 2020, paragraph 7.2.
[37] Letter from the respondent dated 27 May 2022, paragraph 32.
[38] Letter from the respondent dated 27 May 2022, paragraph 32.
[39] Letter from the respondent dated 6 December 2021, paragraph 50.
[40] Letter from the respondent dated 6 December 2021, paragraph 50.
[41] Letter from the respondent dated 6 December 2021, paragraph 52.

indicated in discussions that it only acted on the most recent transaction received, regardless of carrier, as Thryv had no knowledge of which carrier is in possession of the published number. Accordingly, the respondent produces a Daily Alignment File of customers with an "unlist" status to reconfirm on a daily basis that these customers remain on its network and do not wish to appear in the White Pages.[42]

Unauthorised disclosures of certain customers' personal information in the White Pages

2013 and 2014 data breaches

29. Between February 2013 and April 2014, the personal information of over 122,000 customers who had requested an unlisted number was published in the White Pages. On 28 July 2014, the OAIC opened a Commissioner-initiated investigation into this and other acts and practices, resulting in the respondent and the OAIC entering into an enforceable undertaking (**EU**) in 2015.[43]

30. The EU required the respondent to engage an independent third party (**Auditor**) to conduct a number of reviews and certifications.

31. PricewaterhouseCoopers (**PwC**), the initial Auditor, and Privasec, the subsequent Auditor, conducted the required reviews and certification, and produced the required assurance reports. The OAIC considered these documents, along with some further documentation requested from the respondent. The OAIC formed the view that although the respondent had failed to comply with some of the procedural elements of the EU (regarding timeliness and the provision of interim reports), it had met the substance of its requirements and satisfied the terms of the EU. On 26 May 2020, the matter was closed with a letter to the respondent advising that the then Information Commissioner was satisfied that Optus had met the key requirements of the EU.[44]

32. In performing its obligations under the EU, from March to May 2015, the respondent conducted a reconciliation between its front-end and back-end systems and identified 26,000 customers who had made an unlist request whose Customer Directory Details had been disclosed to the White Pages, contrary to the expressed preference of the customer.[45] On 30 April 2015, the respondent initially identified '26K services initially identified as potentially having been incorrectly disclosed to White Pages'.[46] The respondent informed the OAIC of this on 4 June 2015 as part of its work in relation to the EU. The OAIC processed this as a separate data breach notification (DBN15/00047).[47] The number of affected individuals was subsequently revised down to approximately 6,000 individuals.

33. On or around 8 May 2015, as part of its performance of obligations under the EU, the respondent engaged Accenture to conduct an independent internal review of its end-to-end solution for providing data to Telstra for publication in the White Pages and the INPD. On 10 July 2015 Accenture delivered a report to the respondent which made a range of

[42] Letter from the respondent dated 27 May 2022, paragraph 32.
[43] Singtel Optus: enforceable undertaking | OAIC.
[44] Letter from the OAIC to the respondent dated 26 May 2020.
[45] Letter from respondent dated 17 June 2022, paragraph 23.
[4646] Document titled 'Overview Optus Findings – End to End White Pages Reconciliation' dated 10 June 2015.
[47] Email chain between the respondent and OAIC dated 10 June 2015.

conclusions and recommendations with respect to its processes for managing data provided to the White Pages and INPD.

2018 data breach notification (DBN18/00153)

34. On 20 December 2018, the respondent notified the OAIC that it had identified a number of incidents where its customers' personal information had been published in the White Pages against their explicit instruction or request for their information to be unlisted during the period of 1 October 2015 to 14 November 2018.

35. The respondent provided the following reasons for the relevant customer information being or remaining erroneously listed, and provided figures for the numbers of individuals affected. Though the numbers subsequently changed slightly once more information came to light, the ultimate numbers were:[48]

    a. omission by Thryv to validate list or unlist transactions sent by the respondent – 425 individuals affected;

    b. errors in updating the respondent's back-end systems with the correct information, or the use of incorrect codes in its systems – 292 individuals affected; and

    c. omission by the respondent to transmit unlist transactions with respect to porting customers or in the case of change of account name ownership – 110 individuals affected.

2019 data breach notification (DBN19/01252)

36. In response to the 2018 data breach notification, the respondent conducted a full reconciliation with Thryv of all 9.6 million fixed and mobile numbers of its customers. On 27 September 2019, the respondent provided the OAIC with an update following the completed reconciliation. The respondent advised that it had identified further incidents where customers' personal information had been published in the White Pages against their explicit instruction or request for their information to be unlisted during the period of 1 October 2015 to 27 September 2019. This increased the affected individuals that had remained published in the White Pages, from 827 to 51,219. This correspondence was taken as a new data breach notification.

37. The respondent also erroneously notified the OAIC that a further 6,405 individuals had been affected by unauthorised disclosure. This information was later corrected by the respondent in correspondence of 8 July 2020.

38. The respondent provided the following reasons for the relevant customer information being or remaining erroneously listed, and provided figures for the numbers of individuals affected, which were subsequently revised to the following:[49]

    a. conflicting information contained in the respondent's back-end systems – 421 individuals affected;

    b. omission by Thryv to honour or implement unlist transactions submitted by the respondent – 3,660 individuals affected; and

    c. omission by the respondent to transmit unlist transactions with respect to porting customers – 40,733 individuals affected.

[48] Letter from the respondent dated 8 July 2020, appendix A, paragraph 1.2.
[49] Letter from the respondent dated 8 July 2020, appendix A, paragraph 1.2.

The investigation

39. Following the notification to the OAIC of the two related data breaches on 20 December 2018 and 27 September 2019, on 21 July 2021 a delegate of the Commissioner notified the respondent that the Commissioner intended to open an investigation into the two related data breaches under sub-s 40(2) of the Privacy Act. On 2 August 2021, the investigation was commenced.[50]

40. In the course of the investigation, the OAIC issued s 44(1) notices to the respondent (2 August 2021, 18 November 2021, 12 May 2022) and also to third parties Thryv (12 August and 4 November 2021), and Telstra (on 4 November 2021) and considered the responses received.

Application of relevant law

41. The APPs in Schedule 1 of the Privacy Act regulate the handling of personal information by Australian government agencies and certain private sector organisations (**APP entities**). It is not in dispute that the respondent is an APP entity under section 6C of the Privacy Act.

42. Section 15 of the Privacy Act prohibits an APP entity from doing an act or engaging in a practice that breaches an APP.[51] An act or practice of an APP entity is an interference with the privacy of an individual if the act or practice breaches an APP in relation to personal information about an individual.[52] For the purposes of this matter, APP 11.1 applies, concerning the respondent's reasonable steps to protect the personal information it held from misuse, interference and loss, and from unauthorised access, modification or disclosure.

43. I have considered the material obtained during the investigation, including information and submissions provided by the respondent. I have also considered the *Australian Privacy Principles Guidelines* (**APP Guidelines**)[53] and the *OAIC Guide to privacy regulatory action*.[54]

44. For the purposes of s 43(4) of the Privacy Act and following my consideration of the submissions and evidence, I am satisfied that:

    a. the acts and practices to which the investigation relates can be adequately determined in the absence of a hearing with the complainant and respondent; and

    b. there are no unusual circumstances that would warrant holding a hearing before making this determination.

    c. at the time of making this determination, there is no application for a hearing made under s 43A.

45. The facts and circumstances of this matter required me to consider the relevant law, and in particular determine the answer to the following questions:

    - What information did the respondent hold?

---

[50] Email from OAIC to the respondent dated 2 August 2021.
[51] Privacy Act s 15.
[52] Privacy Act s 13(1).
[53] December 2022 version – Australian Privacy Principles guidelines — OAIC.
[54] December 2024 version – Guide to privacy regulatory action — OAIC.

- Did the respondent take such steps as were reasonable in the circumstances to protect the personal information it held from unauthorised disclosure, in accordance with its obligations under APP 11.1?

What information did the respondent hold?

46. Subsection 6(1) of the Privacy Act provides that an entity 'holds' personal information if the entity has possession or control of a record that contains personal information.[55]

47. The APP Guidelines provide that 'the term "holds" extends beyond physical possession of a record to include a record that an APP entity has the right or power to deal with.'[56] It was accepted in *Australian Information Commission v Facebook Inc (No 2)* [2020] FCA 1307 at [195] that 'possession or control' included 'control through an agent and that control need not be exclusive'.

48. The respondent accepts that it held the personal information of new and existing customers whose personal information was published in the White Pages to the extent that it held that information on its systems and disclosed it to Telstra for publication in the White Pages.

49. However, the respondent contended that it does not hold the personal information of customers who had their personal information listed in the White Pages prior to porting their number to the respondent, as that personal information was disclosed to Thryv by their former CSP.[57] Even though, subsequent to the porting of the customer, the respondent clearly holds the Customer Directory Details of the relevant customer, and has the ability to change or unlist those details subject to an instruction from the customer to the respondent, the respondent contends that that information is "information held by an unrelated third party" which is simply "of similar content (or the same as) information held" by the respondent, akin to a particular person's email address and mobile telephone number being held by any number of commercial and governmental entities.[58] For the respondent, whether or not it holds the personal information listed in the White Pages is contingent upon whether it directly disclosed that data to Telstra for publication in the White Pages. The respondent considers the Customer Directory Details disclosed by the former CSP to be a 'Previous CSP record' with which they have no right or power to deal, as the respondent has no agency relationship or contractual entitlement in respect of it.[59]

50. I am not persuaded by this construction. The Optus Access Agreement establishes a framework for the provision of Customer Directory Details, over which the respondent has control, by the respondent to Telstra. At all material times, the respondent had the ability to determine to add, remove or alter the Customer Directory Details held by Thryv and, subsequent to a customer porting to the respondent, was the only entity that could do so upon the request of the customer. As between Thryv and the respondent, only the respondent had the ability to determine what Customer Directory Details would be published, including whether a number would be listed or unlisted. This ability constitutes a form of control over the personal information comprised in the Customer Directory Details. I therefore find the respondent 'holds' the Customer Directory Details of

[55] Privacy Act s 6(1).
[56] APP Guidelines at [B.84].
[57] Submission from the respondent in response to the first preliminary view, 22 February 2024, at [7].
[58] Counsel submission at [89].
[59] Submission from the respondent in response to the first preliminary view, 22 February 2024, at [52].

its customers on its system and on Thryv's system on the basis that the respondent retained control over the Customer Directory Details on both systems.

Did the respondent to take such steps as were reasonable in the circumstances to protect the personal information it held from unauthorised disclosure, in accordance with its obligations under APP 11.1?

51. In determining whether the respondent breached APP 11.1, it is relevant to consider what steps the respondent took to protect the personal information it held and whether those steps were reasonable in the circumstances to protect the information it held from the risk of unauthorised disclosure in the White Pages. The steps an APP entity is required to take to meet its obligations under APP 11.1 will depend on the circumstances.[60]

52. The Privacy Act is not prescriptive concerning what steps will be reasonable in the circumstances. This is an objective test that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances.[61] This is a question to be determined on a case-by-case basis and the obligation is not susceptible to reduction to fixed rules.[62] That is to say, what is reasonable is a question of fact in each individual case and includes, where relevant, taking steps to implement strategies in relation to:

    a. ICT security;

    b. Governance, culture and training; and

    c. Internal policies, procedures and systems.[63]

53. The Federal Court of Australia (**Court**) has provided guidance on the approach to be taken to determine if steps taken were reasonable in the circumstances, albeit within the context of corporations law matters.[64] The Court has observed that identifying steps that could have been taken, but were not taken, can be helpful, and is an obvious way of testing the reasonableness of what was (and was not) done. However, the focus must always be on whether the steps that were taken, in their totality, were reasonable.[65] This requires consideration of whether the steps that were taken to protect personal information from the risk of unauthorised disclosure[66] were commensurate to the risks presented in the relevant circumstances.[67]

54. In the matter of *Australian Information Commissioner v Australian Clinical Labs Limited*, Justice Halley summarised at [51]:[68]

> The breadth of the necessary inquiry into what might constitute 'such steps as are reasonable in the circumstances" is informed by judicial consideration of other legislation that import a "reasonable steps" obligation, in particular, ss 961L, 963F

[60] APP Guidelines at [11.8].
[61] APP Guidelines at [B.108].
[62] *Australian Securities and Investments Commission v R M Capital Pty Ltd* [2024] FCA 151, [86].
[63] APP Guidelines at [11.9].
[64] *Australian Securities and Investments Commission v Firstmac Ltd* [2024] FCA 747; *Australian Securities and Investments Commission v R M Capital Pty Ltd* [2024] FCA 151.
[65] *Australian Securities and Investments Commission v R M Capital Pty Ltd* [2024] FCA 151, [80].
[66] i.e., risk of misuse, interference and loss, and unauthorised access, modification or disclosure.
[67] *Australian Securities and Investments Commission v R M Capital Pty Ltd* [2024] FCA 151, [85].
[68] *Australian Information Commissioner v Australian Clinical Labs Limited (No 2)* FCA 1124, [51].

and 994E(5) of the *Corporations Act 2001* (Cth) (**Corporations Act**). The obligation has been stated:

a. to differ depending on the complexity of the entity's business and the procedures within the entity: *Australian Securities and Investments Commission v Healey* (2011) 196 FCR 291; [2011] FCA 717 at [162] (Middleton J);

b. not to be capable of being discharged simply by delegating it to another entity and doing nothing more: *Clarke (as trustee of the Clarke Family Trust) v Great Southern Finance Pty Ltd (Receivers and Managers Appointed) (in liquidation)* [2014] VSC 516 at [543] (Croft J);

c. to require a wholistic analysis, considering the full framework of the entity's systems, policies and procedures: *Australian Securities and Investments Commission v Diversa Trustees Ltd* [2023] FCA 1267 at [375] (Button J);

d. not to require a person to find and take the optimal steps: *Australian Securities and Investments Commission v RI Advice Group Pty Ltd (No 2)* [2021] FCA 877; (2021) 156 ACSR 371 at [392] (Moshinsky J);

e. not to require a person to take all reasonable steps, nor to identify the universe of possible reasonable steps or the "one true path" to be followed; the focus of the inquiry must always be on whether the steps that were taken in their totality were reasonable: *Australian Securities and Investments Commission v R M Capital Pty Ltd* [2024] FCA 151; (2021) 172 ACSR 1 at [73] and [80] (Jackson J);

f. to be assessed objectively by reference to the standard of behaviour expected of a reasonable person in the regulated person's position: *Australian Securities and Investments Commission v Firstmac Ltd* [2024] FCA 737 at [51] (Downes J).

55. Accordingly, I adopt the following analytical approach to determine whether the steps that the respondent took were reasonable in the circumstances to protect the personal information of its customers from unauthorised disclosure in the White Pages:

- What are the relevant circumstances?
- What steps were taken by the respondent to protect the personal information it held from the risk of unauthorised disclosure in the White Pages?
- Were the steps taken by the respondent, in their totality, commensurate to the risk of unauthorised disclosure in the White Pages in relation to the personal information it held?

56. I observe that it not necessary for me to first be satisfied that unauthorised disclosure has in fact occurred to make a finding that the respondent has contravened APP 11.1. In this matter the respondent does not contest that there has been unauthorised disclosure of personal information in respect of certain customers, as acknowledged in their notification of two data breaches on 18 December 2018 and 27 September 2019. Further, the respondent accepts that where it has received a request from new or existing customers to have their personal information removed from the White Pages, the ongoing publication of that customer's personal information in the White Pages is an unauthorised disclosure for the purposes of the Privacy Act. However, the respondent has submitted at length that the continued listing of porting customers' information, contrary to those customers' expressed request for unlisting, is not an unauthorised disclosure for which it is responsible. The respondent has submitted that, in circumstances where a customer's former CSP – and not the respondent –originally disclosed the customer's details to Telstra, the respondent did not hold that personal information. In my view, this

is both wrong at law (see consideration at paragraphs [41] to [44] above) and, in any event, extraneous to the consideration of compliance with APP 11.1.

57. I also note that the respondent submitted that the obligation in APP 11.1 'does not extend to taking such steps in respect of information held by unrelated third parties, who are not subject to the direction of the entity in question.'[69] I agree. In most circumstances, APP 11.1 will not require an APP entity that holds personal information to take reasonable steps to prevent the unauthorised disclosure of that personal information by some unrelated third party who, due to circumstances unrelated to the APP entity, happens to possess the same personal information.

58. In the circumstances here it is my view that the respondent acquired control over the personal information (the Customer Directory Details) such that the respondent may be considered to hold that personal information. I consider that APP 11.1 is applicable to an APP entity in respect of the disclosure of personal information by a third party where the APP entity holds that information, and it can take such steps as are reasonable in the circumstances to protect the information from unauthorised disclosure.

59. I disagree with the respondent's submission that APP 11.1 is incapable of applying in any circumstance to the obligations of an APP entity with respect to personal information that is held by third parties, where the information is not provided to the third party by the APP entity. In my view, in circumstances in which the respondent acquires a customer who has ported from another CSP, the respondent acquires control over the personal information it collects from the customer and acquires control over the Customer Directory Details as they may be published in the White Pages by Thryv.

What are the relevant circumstances?

60. The APP Guidelines set out the circumstances that should be considered in determining whether an APP entity took reasonable steps to ensure the security of personal information.[70]

61. I consider the following matters to be relevant to determining what steps taken by the respondent were reasonable to ensure the security of personal information:[71]

    a. **Amount and sensitivity of personal information held:** The respondent held the Customer Directory Details for all of its customers, which numbered over 10 million in 2018.[72] This information, although not "sensitive information" within the meaning of the Privacy Act, may be information that if disclosed could in certain circumstances result in serious harm to the individuals to whom the information relates. The nature of the personal information publicly disclosed, including customers' names, phone numbers and physical addresses is capable of exposing individuals' locations, presenting a real risk of physical and/or emotional harm, particularly for individuals in vulnerable circumstances.

    b. **Potential harm to individuals of unauthorised disclosure:** I consider that the possible adverse consequences of an individual having their Customer Directory Details disclosed publicly contrary to their preferences may be significant. For example, such disclosures may have significant consequences in situations of domestic violence and family law disputes, and for professions which may invite

[69] Counsel Submission at [94].
[70] APP Guidelines at [11.7].
[71] *With reference to Australian Information Commissioner v Australian Clinical Labs Limited (No 2)* [2025] FCA 1224 at [50].
[72] Singtel Pty Ltd, Singtel Annual Report 2017: Connecting Your World (Report, 29 June 2017).

retribution where addresses are known (such as law enforcement etc). In addition, even for customers who did not have a special vulnerability, many people would be distressed to learn that their customer information was published online when they had understood (based on an instruction given to the respondent) that those details would be unlisted.

c. **Size and sophistication of APP entity:** The respondent is a highly sophisticated entity, being a telecommunications service provider, with over 10 million customers in 2018,[73] and was (and still is) Australia's second-largest CSP. In 2018, it had approximately 8,400 employees.

d. **Cybersecurity environment and history:** The respondent is a provider of critical national infrastructure and operates in a highly regulated sector. There is no evidence before me that, at the time of the relevant acts and practices, the respondent had been the subject of any significant cybersecurity incident. However, the respondent had repeatedly failed to protect the personal information it held from unauthorised disclosure in the White Pages. On at least two previous occasions that pre-date the acts and practices the subject of this investigation, the OAIC had been made aware of unauthorised disclosures of the respondents' customers' personal information in the White Pages (see paragraphs [29] to [33] above).

What steps were taken by the respondent to protect the personal information it held from unauthorised disclosure in the White Pages?

62. During the relevant period, the respondent had in place a number of processes, both organisational and technical, to ensure that customer information listed in the White Pages was up-to-date and accurate, reflected changes submitted by customers and, importantly, was not listed in circumstances in which the customer had expressed a preference for an unlisted number. At a fundamental level, as described at paragraphs [17] to [28] above, the respondent took steps to put in place:

    a. Policies and processes to ensure customers were offered a choice between a listed and unlisted account at the time of signing up for a new account, porting their number to the respondent, and at any time after that point.

    b. Organisational processes to ensure that requests from new and existing customers to change a listed number to unlisted were routinely submitted to Telstra every 24 hours.

    c. Technical processes to automatically submit list and unlist transactions, and changes to Customer Directory Details, directly to Telstra every 24 hours in the form of the Daily Secure Transaction File.

    d. Organisational processes to ensure that expedited requests for unlisting were submitted directly to Thryv at least weekly by email.

63. However, the simple existence of policies and processes is unlikely to be effective without robust technical systems to give effect to them, and appropriate data governance mechanisms to underpin them. For example, the data breach reports of 20 December 2018 and 27 September 2019 indicate that a range of human errors contributed to data deficiencies that led to the unauthorised disclosure of personal information to the White Pages, including:

[73] Singtel Pty Ltd, Singtel Annual Report 2017: Connecting Your World (Report, 29 June 2017).

a. Customer Service Representatives and Customer Support Consultants using an incorrect code when recording an unlist preference in the front-end system.[74]

b. Customer Support Consultants failing to update the front end system to record an unlist preference when sending a listing escalation form, meaning System 1 was also not updated.[75]

c. Customer Support Consultants updating the back-end System 1 when actioning directory listing escalation forms, without updating the front-end system as well. This meant that the change in System 1 would eventually be overridden by the incorrect information in the front-end system.[76]

64. The 2018 and 2019 data breaches also revealed that the respondent's migration to a new Customer Relationship Management System, System 2, had caused 'stuck-order errors' arising from conflicting information between the Customer Relationship Management system and the back-end System 1, and that those errors had not been appropriately addressed by IT staff.[77]

65. The risk of unauthorised disclosure of Customer Directory Details in the White Pages was well-known to the respondent. The OAIC had previously taken regulatory action against the respondent with respect to this very issue which, among other issues, gave rise to an Enforceable Undertaking between the respondent and the OAIC in 2015.[78] As such at the beginning of the relevant period, namely 1 October 2015, the respondent was already aware of the deficiencies in its technical systems and data governance relating to its transmission of information to the White Pages, over a prolonged period.

66. On or around 8 May 2015, the respondent engaged Accenture to conduct an independent internal review of its end-to-end solution for publishing data to the White Pages and the INPD. On 10 July 2015 Accenture delivered a report to the respondent which made a range of conclusions and recommendations with respect to its processes for managing data provided to the White Pages and INPD. Optus also engaged Price Waterhouse Coopers to conduct a Privacy Incident Review and evaluate Accenture's findings.

67. The key finding of the report was that gaps existed in three areas resulting in data integrity and alignment issues within the respondent's systems, as well as between the respondent and Thryv.[79] Accenture summarised those three areas as 'people, processes and technology'.[80] The respondent characterised them as 'insufficient data governance, gaps in processes resulting in errors not being actioned, and lack of data reconciliation between systems'.[81]

68. In greater detail, Accenture identified the following issues:

People

a. a lack of appropriate staffing assigned to the management of data integrity and alignment of White Pages data;

b. greater clarity required in the roles and responsibilities of the respondent's resources devoted to maintaining White Pages data;

---

[74] Letter from the respondent dated 8 July 2020, appendix A, paragraph 5.3.
[75] Letter from the respondent dated 8 July 2020, appendix A, paragraph 4.3(a).
[76] Letter from the respondent dated 8 July 2020, appendix A, paragraph 4.3(a).
[77] Letter from the respondent dated 8 July 2020, appendix A, paragraph 4.3(b).
[78] Singtel Optus: enforceable undertaking | OAIC.
[79] Accenture report.
[80] Accenture report pages 3 and 4.
[81] Letter from respondent dated 27 May 2022, paragraph 17.

c. a lack of institutional knowledge due to organisational changes;

Processes

d. failures in processes that lead to some errors not being actioned prior to data being sent to the White Pages;

e. the absence of end-end transactional or system reconciliation of listing data, both within the respondent's systems and between the respondent and Telstra;

f. failure to allocate process owners to all processes involved in sending data to the White Pages;

g. failure to always undertake regression testing as part of system changes;

Technology

h. poor data integrity due to historical IT system changes;

i. data inconsistences and lack of integrity in System 1 and source systems, including incomplete records requiring manual intervention;

j. problems with data fields in key source systems; and

k. System 1 is an end-of-life platform impacting ability to make changes.

69. Accenture made a number of recommendations to the respondent to resolve the issues it identified.[82] PwC, as the initial Auditor under the EU, assessed Optus' Privacy Incident Review process, and validated the Accenture report. the respondent provided a recommendation plan which sets out and addresses the key recommendations stemming from both PwC and Accenture's assessments.[83] The plan indicated that the respondent would complete the implementation of a number of the recommendations by December 2015.[84]

70. With respect to the steps taken by the respondent during the relevant period, it submitted on 17 June 2022 that a range of measures had been taken by that date (which covers the entire relevant period of the investigation) to address the Accenture recommendations.[85]

71. Below is a summary of the relevant recommendations and steps taken to implement, with recommendations not implemented (or only partially implemented) in bold. The table retains the terminology used in the Accenture report, although other terminology has been adopted in this determination.[86]

Recommendation made 10 July 2015	Steps taken by the respondent and when
Establish a Master Data Management strategy for the Directory Listing and Address entities which specifically addresses data governance, quality, processes, standards, architecture and security.	**Implemented partially with respect to the IPND only in 2020.** **Not implemented with respect to the White Pages as at 17 June 2022.**

[82] Accenture report, page 4, paragraph 1.4; and pages 13 to 15.
[83] Letter from respondent dated 17 June 2022, Annexure 1.
[84] Letter from respondent dated 17 June 2022, Annexure 1.
[85] Letter from respondent dated 17 June 2022, Annexure 1.
[86] Letter from respondent dated 17 June 2022, Annexure 1.

Recommendation made 10 July 2015	Steps taken by the respondent and when
Appoint a senior resource as the data steward for the White Pages Listing and Address master data who has defined responsibility for the ongoing data integrity of these entities.	Data Steward role established in 2020 but does not have responsibility for data integrity of the White Pages Listing and Address master data. Business owner with responsibility for overall governance of the White Pages Listing data including processes, controls and procedures appointed in October 2021.
Implement daily transactional reconciliation between data producers (the Customer Relationship Management systems), data masters (System 1) and consumers (Telstra/Thryv) for the Directory Listing and IPND Address updates.	**Partially implemented. By 23 May 2016 the respondent implemented an automatic daily internal reconciliation process for its various systems, in particular the front-end systems and the back-end System 1.**
Implement a regular (Monthly or Quarterly) reconciliation of Listing Values across the respondent's systems which are Masters, Producers or Consumers of Directory Listing values, and action all discrepancies to ensure alignment of data across systems.	**Not implemented. The respondent considers the daily reconciliations referred to immediately above as sufficient to respond to this recommendation.**
Perform a standard set of end-end regression tests to verify White Pages Listing and IPND Address data as part of system/configuration change to systems.	The respondent implemented an IT project described as the 'Test Automation' project, involving the implementation in March 2016 of 'golden regression suite' tests. The process was run by the respondent's Test Management Office and included White Pages specific testing in the regression suite.
Ensure that all notifications and errors are actioned each day and that the relevant teams and resources involved have defined responsibilities which include actioning these notifications and errors.	The respondent implemented an IT project described as the 'Move jobs to a centralised workflow' project in around June 2016, using a new System 3[87] monitoring framework.[88] The System 1 functions performed by the System 3 tool were transitioned to another system called System 4 from July 2017 onwards.
Implement and maintain a comprehensive repository of errors,	By 9 August 2016, the respondent commenced documenting different types

[88] The System 3 tool is a centralised 24/7 system that continuously monitors jobs and informs relevant Optus IT personnel if any job within the back-end System 1 fails so that steps can be taken to rectify the issue: Letter from the respondent dated 17 June 2022, paragraph 23.

Recommendation made 10 July 2015	Steps taken by the respondent and when
including error codes, messages, workarounds, resolutions and root causes.	of errors that can arise in System 1 in an operations manual used by the respondent's IT staff.
The Data Steward for the Directory Listing and Address entities should document the systems which are masters, producers and consumers of these entities. This should be documented in an overall Data Management Strategy Plan for these entities.	**While the Data Steward role was established in 2020, as at 17 June 2022, there was no Data Management Strategy Plan in place.**
Perform a user audit for roles and responsibilities of users which can make updates to data directly via the System 1 graphical user interface. Remove update access to those users who do not require access for endorsed processes.	By 9 August 2016, the respondent undertook a user audit of System 1 and took appropriate actions arising from that audit. In addition, in May 2016 the respondent implemented a project to adopt audit logging in the System 1 system to enable it to identify what data is changed at any given time and by whom.
Changes to White Pages Listing and INPD data should only be made to data master or producer systems. Any updates to non-masters should only be by exception by approved resources.	**The respondent continues to provide direct data updates to Thryv/Telstra outside of the data master systems in certain circumstances requiring overrides of the Daily Secure Transaction File, including when urgent changes need to be made. However, the respondent updated the directory listing escalation form used by Customer Support Consultants to require them to update the relevant provisioning system.**
Review all address validation errors in System 1 and work with the respondent's solution architect to define a resolution to prevent address validation errors in System 1 and downstream.	Implemented via the introduction of the respondent's new Customer Relationship Management system, System 2, which was rolled out in a phased approach, commencing in November 2016.
Create online dashboards with real-time monitoring of critical metrics for all batch jobs.	Implemented through System 4 adopted in July 2017.
Develop an interim solution to no provision for a Service Address in System 5,[89] and in the long term look to decommission System 5.	System 5 was in the process of being phased at, to be completed by April 2023.

[89] A legacy system used for rating and billing of usage: Letter from respondent dated 6 December 2021, paragraph 26(a).

Recommendation made 10 July 2015	Steps taken by the respondent and when
Commence an activity to assess the long-term roadmap for System 1.	The respondent intended to replace the back-end System 1 with System 6[90] by mid-2023.
Remediate inconsistent data in System 1 to ensure there is a single accurate record for each of the respondent's telephone services.	The respondent conducted a 2019 data reconciliation with Thryv which enabled the remediation of inconsistent data prior to 2019. The respondent addresses ongoing data inconsistencies through the daily internal reconciliations implemented in May 2016.
Ensure every process has an agreed process owner who has responsibility for the process flow.	**Not implemented with respect to White Pages Listing data but expected to be implemented by around September 2022.**
Identify and assign a business owner for the System 1 application.	Implemented as at 17 June 2022.
Perform data reconciling for listing values between DSS, ESS with respect to Business Directory Listings.	**Not implemented with respect to the White Pages as the respondent does not manage Business Directory Listings in the White Pages.**
The respondent to validate requirements and solution for Local Access Resale services (that is, reselling Telstra local services) prior to implementing RDSL project into production.	The respondent ultimately decided not to proceed with the RDSL project.
The respondent to validate if Thryv or IPND provide newer interfaces which may provide enhanced functionality for interacting with these systems.	**The respondent is not aware of specific steps have been undertaken in respect of this.**
Implement a fix to stop System 7[91] from sending Remove transactions on cancellation of a Pending Install.	Addressed by implementing a fix to System 7 which had occurred by August 2016.
Add audit trail information to System 1.	Implemented by August 2016.

72. Some of the recommendations made by Accenture relied upon Thryv and/or Telstra taking specific actions, notably the provision of a daily return file by Thryv to enable the respondent to test the effectiveness of processes across multiple systems used to deliver listings data to Thryv.[92] In correspondence to the OAIC on 13 February 2019, following the first data breach of 20 December 2018, the respondent indicated that it was working with

[90] A simplified version of System 1 with better functionality in dealing with issues such as the rejection of transactions: Letter from respondent dated 17 June 2022, paragraph 4.

[91] An internal legacy system used for Optus' fixed cable network services: Letter from respondent dated 6 December 2021, at paragraph 26(c), 30.

[92] Accenture report, page 13, GAP07.

Thryv to develop a regular daily error file based on the respondent's daily transaction file to identify individual transactions that have not been actioned successfully by Thryv. At that point Thryv informed the respondent that it would be delivered "when testing is completed and agreements are in place between Sensis (Thryv) and [the respondent]".[93] In correspondence to the OAIC dated 17 June 2022, the respondent noted it had not at that point been able to obtain a daily return file from Thryv.[94] In the absence of a daily return file being provided by Thryv, since October 2020, the respondent has implemented an internal Daily Checker Report as a manual sample check of 100 customer records against White Pages listings. Since August 2020 a monthly meeting has been implemented between the Optus and Thryv technical teams to ensure that any changes to specifications and guidelines are actioned, involving Telstra as necessary. [95]

Were the steps taken by the respondent, in their totality, commensurate to the risk of unauthorised disclosure in the White Pages, in relation to the personal information it held?

73. The respondent was aware, throughout the entire period, of the risk that the personal information of customers who had requested an unlisted number may still be published in the White Pages in error. The respondent was also aware that those errors affected a not insignificant number of its customers.

74. Following the Accenture report in July 2015 and during the relevant period, the respondent took the steps articulated in paragraphs [62] to [72] to reduce or mitigate the ongoing risk of unauthorised disclosure on the White Pages in relation to its customers' personal information. It is my view that, through the program of work that was catalysed by the Accenture report delivered to the respondent on 10 July 2015, the respondent took steps to address many of the risks identified by Accenture which may have contributed to the unauthorised disclosure of customer information in the White Pages.

75. However, given the circumstances outlined at paragraph [61] and the size, resources and sophistication of the business conducted by the respondent in the context of the high volume of personal information held by the respondent, and the historical context of the particular risk, it is my view that those steps were not, in their totality, commensurate to the ongoing risk of unauthorised disclosure of personal information in the White Pages against the express requests of the respondent's customers. This is particularly the case given that the respondent was well aware of the deficiencies in its system of provision of Customer Directory Details to Telstra.

76. In my view, despite the steps taken by the respondent, the following risks remained real during the relevant period:

    a. the risk of human errors made by Customer Service Representatives and Customer Support Consultants resulting in inaccurate listing information being recorded or transmitted;

    b. the risk that transactions transmitted by the respondent were not correctly received, recorded or reflected by the White Pages; and

    c. the risk that the personal information of porting customers would be subject to unauthorised disclosure where a porting customer had made an unlist request.

[93] Letter from respondent dated 13 February 2019.
[94] Letter from respondent dated 17 June 2022.
[95] Letter from respondent dated 17 June 2022, paragraph 41.

77. I find that there were corresponding steps the respondent could have taken to mitigate or eliminate the risks, but did not, as follows:

    a. Promoting a culture of privacy awareness and stewardship with respect to the White Pages, including through the appointment of senior staff with the responsibility of ensuring that Customer Directory Details are managed appropriately, and through the provision of appropriate training to Customer Service Representatives and Customer Support Consultants on the use of front and back-end systems (**people and culture**).

    b. Performing periodic reconciliations between the Customer Directory Details held by the respondent on its own systems with the information published in the White Pages, coupled with a process to remediate any errors or discrepancies (**system reconciliations and alignments**).

    c. Putting in place processes and systems to ensure that the personal information of customers who are porting to or from the respondent is being handled appropriately and, in particular, that the Customer Directory Details are accurate, current and complete and that any unlist request has been promptly implemented (**processes for porting customers**).

People and culture

78. The respondent was aware at least as early as 10 July 2015 (the date of the Accenture report) of the range of organisational and technical issues pervading it systems, policies and processes with respect to the provision of Customer Directory Details to Telstra. The data breaches reported to the OAIC on 20 December 2018 and 27 September 2019 suggest that those issues continued to persist for the respondent for many years.

79. The Accenture report taken as a whole, makes it clear that there was an overarching absence of governance and strategy in the respondent's handling of Customer Directory Details for the purpose of provision to the White Pages, which was a significant, high-volume and contractual obligation and corporate function performed by the respondent during the relevant period. Implicit in Accenture's report is also a conclusion that the contribution made by the respondent in ensuring the White Pages was accurate, up-to-date and did not include customers who had expressed a request not to be listed was not culturally valued and reflected in governance and management arrangements.

80. The respondent's response to the Accenture recommendations further reflects a reluctance to properly invest in the management of its White Pages functions in a wholistic way. For example, in response to Accenture's recommendation to establish a Master Data Management strategy for both the White Pages and IPND functions, the respondent proceeded to establish a IPND Council some five years later, but has not provided evidence of any concrete work done by the IPND Council to address the gaps identified in the report, and had not implemented a Master Data Management strategy with respect to the White Pages as at 17 June 2022. With respect to Accenture's recommendation that the respondent appoint a senior resource to act as a data steward for the White Pages Listing and Address master data, this was not implemented with respect to the White Pages until October 2021. This is despite the respondent having indicated to the OAIC that it would implement the Accenture recommendations by 31 December 2015.

81. I acknowledge the complex reality of implementing Accenture's many technical recommendations in the context of legacy systems. In these circumstances, however,

prompt implementation of recommendations pertaining to governance and processes, such as those articulated in the preceding paragraph, should have been prioritised.

82. It does not appear that the respondent's stewardship and privacy responsibilities as they pertained to the White Pages were well valued by leadership or communicated to employees. On the materials available to me I cannot be confident that the respondent provided frequent training to staff on the importance of faithfully recording unlist requests or on the risks of not adhering to processes to change records from list to unlist. For example, the respondent has asserted that, following the 2018 data breach incident, it provided Customer Service Representatives with refresher awareness training emphasising the importance of directory listing flags. However, the evidence provided to support that assertion appears to be a short update on an internal messaging group, rather than any form of training.[96] I also note that as at August 2016 the respondent provided only one module of Privacy Training to its customer service staff. [97]

83. It appears to me that the lack of emphasis of faithful adherence to list and unlist requests in the respondent's management and culture reflected limited recognition by the respondent of the potentially harmful impacts for its customers of having their personal information disclosed in the White Pages against their wishes. This is reflected by the respondent's submission which highlights that the number of errors arising relating to a failure to honour unlist requests was comparatively small compared to the approximately 912,500 change requests transmitted by the respondent in 2018 alone. This approach fails to recognise the potential serious impacts for each individual affected by an error. Furthermore, in my view, the fact that the respondent invited customers to express an 'unlist' preference when porting their accounts from another CSP to the respondent, but did not consider it had a responsibility to proactively transmit those preferences to Thryv, is further evidence of the absence of recognition of the important role it had to play in protecting the personal information it held from unauthorised disclosure.

84. Taking into consideration its important role and responsibility with respect to the management of a high volume of personal information and the potential risk for unauthorised disclosure, it would have been reasonable for the respondent to have made more significant investments in building a governance environment and framework that valued its important stewardship role and communicated that to its staff. At a minimum, I consider the respondent could have heeded the Accenture recommendations to:

    a. establish a data management strategy or plan with respect to its management of customer information for the White Pages; and

    b. appoint a member of senior staff with the responsibility of ensuring that Customer Directory Details are managed appropriately throughout the different stages in which that information is used and disclosed by the respondent.

System reconciliations and alignments

85. A key recommendation of the Accenture report was for the respondent to implement daily transactional reconciliations as between its own back-end and front-end systems (the Customer Relationship Management systems and System 1) and between its system and Thryv's system.[98] The respondent indicated that by May 2016 it had implemented an automatic daily internal reconciliation process with respect to its own system with a focus on eliminating data discrepancies between its own systems.

---

[96] Letter from the respondent dated 8 July 2020, appendix A, paragraph 5.5.
[97] Optus, Privacy Training – Reporting and Escalation Process, 3 August 2016, page 4.
[98] Accenture report page 4, paragraph 1.3, 2(ii), page 13, GAP07 and page 14, GAP13.

86. However, the respondent was also aware of data discrepancies as between its own systems and Thryv's system. These discrepancies may have arisen because of historical data inaccuracies provided by the respondent to Thryv, or because of acts or omissions by Thryv itself.

87. From June 2016 to August 2020, the respondent deployed an ad hoc process of reconciliation that involved the monthly transmission to Thryv of a file containing all numbers with an 'unlist' preference for Thryv to check against its data.[99] However, when in April 2019, following the first notifiable data breach, the respondent and Thryv undertook a data reconciliation process at the respondent's request, and Thryv provided the respondent with the listing status of telephone numbers provided by the respondent, the respondent identified approximately 123,000 numbers currently published by Thryv on the White Pages should not be listed.[100] The respondent has indicated that the number of customers affected was revised down to approximately 40,000 by the end of the reconciliation exercise.

88. Subsequently, in response to that reconciliation, the respondent took a number of steps, including that, from August 2020 onwards, it provided Telstra with a Daily Alignment File to ensure that Thryv's status for the respondent's customers aligned with the respondent's own data. This additional file contains a full list of all of the respondent's customers with an unlist status, including for porting customers, and therefore ensures alignment between the respondent's and Thryv's systems. On average, this file contained between 10 and 11 million entries.[101]

89. In my view, transmitting a Daily Alignment File confirming the unlist status of all of the respondent's customers is an entirely prudent and reasonable approach to ensuring that customers' personal information is not disclosed in the White Pages against their instructions. I consider that, in the circumstances, it would have been a reasonable step for the respondent to have taken during the relevant period.

90. I recognise that the respondent attempted to take an additional step to address the data deficiencies as between its system and Thryv's, in that it initiated negotiations in October 2018 with Thryv on a direct commercial agreement to require Thryv to produce a daily return file to the respondent. The return file would have enabled the respondent to audit which transactions were implemented by Thryv and in what timeframe.[102] As at June 2022 those negotiations were ongoing.

91. However, I also consider that, in the absence of daily return files from Thryv, the respondent could have done more to ensure system reconciliation and alignment from its end. In addition to the provision of a Daily Alignment File, the respondent could have undertaken manual checks of a sample of customer records against White Pages listings. Indeed, the respondent indicated that as at 17 June 2022, it had implemented an internal Daily Checker Report as a manual sample check of 100 customer records against White Pages listings.[103] I consider this also could have been a reasonable step for the respondent to have taken during the relevant period.

---

[99] Letter from the respondent dated 17 June 2022, paragraph 28
[100] Letter from Thryv dated 26 August 2021, question 11.
[101] Letter from the respondent dated 17 June 2022, paragraph 28.
[102] Letter from the respondent dated 17 June 2022, paragraphs 29 and 30.
[103] Letter from respondent dated 17 June 2022, Annexure 1, paragraph 41(c).

Processes for porting customers

92. The respondent submitted that it was not reasonable in the circumstances to require it to take positive steps to notify Telstra or Thryv of unlist requests from porting customers.[104]

93. The thrust of the respondent's submission is that there was a 'statutory and contractual regime'[105] that was intended[106] to operate in accordance with 'processes put in place by Telstra (as public directory listing manager)'.[107] In summary, the process which the respondent submits was put in place by Telstra, and which it evidently followed (regardless of who put it in place) was that:[108]

    a. where a customer ports from another CSP to the respondent, it was the responsibility of the former CSP to notify Telstra and/or Thryv that the customer was no longer receiving that CSP's services;

    b. upon receiving that notification, Telstra would notify Thryv of that matter, and upon that notification occurring, Thryv would delist the customer from the White Pages to the extent that customer was previously a "listed customer" (and if they were already an unlisted customer, they would remain so); and

    c. when a customer ported to the respondent and elected to be an "unlisted" customer, the express terms of the Optus Access Agreement were such that the respondent was not under any obligation to notify Telstra of that customer's details or even of the customer's status as an "unlisted" customer.

94. In effect, the respondent assumed that when customers ported to the respondent, their previous CSP and Telstra would have caused the customer to be unlisted from the White Pages. The respondent adopted such a process itself; that is, it had a practice of notifying Thryv (via Telstra) each time that a customer who was listed on the White Pages ported away from the respondent and requested that the customer be delisted from the White Pages.[109] I accept the respondent's submission that such a process was 'logical'[110] and note that it followed this practice itself. However, there is no evidence that the respondent tested its assumption that other CSPs deployed similar processes by consulting with other CSPs or Telstra, or by checking the White Pages to verify that customers had in fact been delisted.

95. Importantly, porting customers were specifically asked by the respondent during the porting process whether they wanted a listed or unlisted number. Customers had no direct contractual relationship with Telstra or Thryv and no longer had any relationship with their former CSP. The respondent has not identified that any disclaimer or notice was given to porting customers that notified them that, if they selected an unlisted number, the respondent would not take any steps to action that request and that the customer should confirm with their previous CSP that they had been unlisted (or contact Thryv and confirm the same). Accordingly, it appears customers were led to believe, based on representations made by the respondent, that it would take steps to implement the customer's request to have either a listed or unlisted number.

---

[104] Counsel Submission at [125].
[105] Counsel Submission at [122]
[106] The respondent does not specify by whom this intention was held.
[107] Counsel Submission at [125].
[108] Counsel Submission at [123].
[109] See paragraphs 7.2 and 8.1 of the 8 July 2022 letter where the respondent explains its process for sending "remove" or "port-out" transactions to Thryv (then Sensis) for customers terminating due to port away.
[110] Counsel Submission at [125(b)].

96. The assumption made by the respondent regarding the obligations and practises of other CSPs was evidently incorrect. When the respondent conducted the 2019 reconciliation, it identified 41,278 porting customers which had indicated an unlist preference when porting to the respondent but whose Customer Directory Details remained published on the White Pages.[111] This indicates that the former CSPs in respect of these customers were not in the practice of notifying Telstra/Thryv that customers were porting away, or that they were notifying Telstra which then did not delist those customers.

97. The respondent also submits that it would not be reasonable to expect it to disclose information (being the personal details of porting customers who had requested an unlisted number) to Telstra/Thryv that the respondent did not need to disclose (and this creating the risk of wider disclosure) in order to prevent the consequence of other CSPs not carrying out their responsibilities.[112] The respondent submitted such an approach would incur 'attendant expense and inconvenience and risk for its customers'.[113]

98. However, the respondent has now adopted the practice it says it was not reasonable for it to be required to adopt. That is, since October 2020 the respondent has transmitted Daily Alignment File containing the phone number of porting customers who requested an unlisted number.[114] This suggests that the practical burden of taking this step was not excessive.

99. Accordingly, I consider that the reasonable steps that the respondent was required to take to manage the risk of unauthorised disclosure of customers' personal information in the White Pages could have included taking positive steps to notify Telstra or Thryv of porting customers' request to have an unlisted number.

100. For completeness, I accept that former CSPs also had the ability, and may have also had an obligation, to take steps to limit the risk of unauthorised disclosure of exiting customers' personal information by taking steps to request the customer's details be delisted from the White Pages. Two or more entities may have obligations under the Privacy Act with respect to the same record or personal information at the same time. However, this investigation was into the respondent's compliance with the APPs alone.

Finding

101. I find that, during the relevant period, the totality of steps taken by the respondent were not reasonable in the circumstances to protect the personal information it held from unauthorised disclosure; and that the respondent has consequently breached APP11.1.

Carly Kind
Privacy Commissioner
20 March 2026

Review rights

Section 96 of the *Privacy Act 1988* (Cth) states that a party may apply to have a decision under s 52(1) or (1A) to make a determination reviewed by the Administrative Review Tribunal (**ART**). The ART provides independent merits review of administrative decisions and has power to set aside, vary, or affirm a privacy determination. An application to the ART must be made within 28 days after the day on which the person is given the privacy determination (s 18(1) of the *Administrative Review Tribunal Act 2024*

[111] Letter from the respondent dated 17 June 2022, paragraph 26.
[112] Counsel Submission at [127](e)-(d).
[113] Counsel Submission at [127](e).
[114] Letter from the respondent dated 17 June 2022, paragraph 41.

(Cth); r 5(3) *Administrative Review Tribunal Rules 2024* (Cth)). An application fee may be payable when lodging an application for review to the ART. Further information is available on the ART's website (www.art.gov.au) or by telephoning 1800 228 333.

A party may also apply under s 5 of the *Administrative Decisions (Judicial Review) Act 1977* (Cth) to have the determination reviewed by the Federal Circuit and Family Court of Australia or the Federal Court of Australia. The Court may refer the matter back to the OAIC for further consideration if it finds the Information Commissioner's decision was wrong in law or the Information Commissioner's powers were not exercised properly. An application to the Court must be lodged within 28 days of the date of the determination. An application fee may be payable when lodging an application to the Court. Further information is available at https://www.fcfcoa.gov.au/gfl and www.federalcourt.gov.au/.