NOTICE OF FILING

Details of Filing

Document Lodged:	Outline of Submissions
Court of Filing	FEDERAL COURT OF AUSTRALIA (FCA)
Date of Lodgment:	20/02/2026 3:46:42 PM AEDT
Date Accepted for Filing:	20/02/2026 3:46:44 PM AEDT
File Number:	NSD1288/2025
File Title:	CPC PATENT TECHNOLOGIES PTY LTD (ACN 615 736 028) v APPLE PTY LIMITED & ANOR
Registry:	NEW SOUTH WALES REGISTRY - FEDERAL COURT OF AUSTRALIA

Registrar

Important Information

This Notice has been inserted as the first page of the document which has been accepted for electronic filing. It is now taken to be part of that document for the purposes of the proceeding in the Court and contains important information for all parties to that proceeding. It must be included in the document served on each of those parties.

The date of the filing of the document is determined pursuant to the Court's Rules.

Federal Court of Australia
District Registry: New South Wales
Division: General

No. NSD 1288 of 2025

On appeal from the Federal Court of Australia

CPC Patent Technologies Pty Ltd (ACN 615 736 028)
Appellant

Apple Pty Limited (ACN 002 510 054) and another
Respondents

CPC'S OUTLINE OF SUBMISSIONS IN CHIEF

2 February 2026

Filed on behalf of (name & role of party) CPC Patent Technologies Pty Ltd, the Appellant
Prepared by (name of person/lawyer) Michael Williams
Law firm (if applicable) Gilbert + Tobin
Tel (02) 9263 4000 Fax (02) 9263 4111
Email mwilliams@gtlaw.com.au
Address for service (include state and postcode) Level 35 Tower Two, International Towers Sydney, 200 Barangaroo Avenue Barangaroo NSW 2000

A. INTRODUCTION

1. This is an appeal from *CPC Patent Technologies Pty Ltd v Apple Pty Limited* [2025] FCA 489 (**J**; Pt A Tab 13). The appellant, **CPC**, is the patentee of the patents in suit, referred to as the **168** and **293** Patents (Pt C Tabs 28 and 29), which are directed to systems and methods for providing secure access to a resource or device using biometric data, such as facial or fingerprint recognition. At trial, CPC contended that the respondents/cross-claimants, **Apple**, infringed the Patents by the supply and exploitation of certain **Apple Devices** having Touch ID or Face ID functionality, categorised into agreed **Exemplar Categories** identified at J [7].

2. Apple denied infringement on the bases that: **(a)** on its proposed construction, the Apple Devices do not fall within the scope of the Patents; and **(b)** the claims in suit are invalid. Much of Apple's invalidity case was abandoned by the end of the hearing (including grounds that Apple now seeks impermissibly to re-enliven by way of its cross-appeal, which will be addressed further in answer); and the remainder of the invalidity case was largely unsuccessful. However, his Honour found that the Apple Devices did not infringe the Patents, and that three of the asserted claims of the 168 Patent only are not novel in light of the Wuidart publication.

3. The appeal largely turns upon the proper construction of the Patents, which the Full Court is in as good a position as the primary judge to decide, especially where (as in this case) the claims concern plain English words: *Globaltech Corporation Pty Ltd v Australian Mud Company Pty Ltd* (2019) 145 IPR 39 at [105]-[106]. In general terms, his Honour adopted an overly narrow and strained construction of the asserted claims, which on their face are framed in broad and functional terms consistently with the general description in each specification. An illustration of this is his Honour's finding that the Apple Devices are not "controlled items" to which secure access is provided within the meaning of the Patents. Plainly, the provision of such access is the intended purpose and effect of Apple's Touch ID and Face ID functionality.

B. CONSTRUCTION - GROUNDS 1-6

B.1 Introduction

4. The specifications of the Patents are similar, aside from the consistory clauses and claims. References below are to pages of the specification of the 168 Patent.

5. CPC makes the following observations relevant to construction at the outset. ***First***, none of the integers in dispute are terms of art. They comprise ordinary English words, which should be given their ordinary meaning: see, eg *Minnesota Mining and Manufacturing Co v Beiersdorf (Australia) Ltd* (1980) 144 CLR 253 at 270, 272 and 279. ***Secondly***, whilst the specification provides non-limiting examples of particular embodiments of the invention, these are examples only and should not be used to confine the scope of the claims in a manner not supported by the

plain language used: see, eg *Welch Perrin & Co Pty Ltd v Worrel* (1961) 106 CLR 588 at 610. ***Thirdly***, the invention is framed in terms of functionality, and the claims are directed to differing functionalities to ensure that they encompass a wide range of different systems. As the specifications state, the invention is not limited to any particular device, and the concept of "secure access" extends beyond access to physical areas: p 28 lines 19-20 (Pt C Tab 28, AB-1032). The different combinations and arrangements of the functional elements claimed emphasise the flexibility that the specification ascribes to the invention, and supports a broad construction.

B.2 Controlled item (ground 1)

6. The primary judge ought to have found that the "controlled item" is the physical or logical item that the user seeks to access. The field of the invention relates to secure access systems, and the claims are directed to providing secure access to a controlled item: J [89]; [103]-[104]. They uniformly refer to access (i.e. entry) being provided "to" a controlled item.

7. Contrary to the primary judge's findings, the controlled item of the claims is not a "single locking mechanism": cf J [108]. Access is not granted to a locking mechanism, this serves no purpose. Rather, a locking mechanism is unlocked to grant access to the item it controls, being the physical and/or logical item which the user can seek to access. In reaching a contrary view, and despite acknowledging that it was not determinative, the primary judge relied upon a single sentence in the specification at page 10 lines 18 to 20: J [107]-[108]. In doing so, his Honour departed from well-established principle that it is not legitimate to confine the scope of the claims by reference to limitations which may be found in the body of the specification but which are not expressly or by proper inference reproduced in the claims themselves: ***Decor Corp****oration Pty Ltd v Dart Industries Inc* (1988) 13 IPR 385 at 391 per Lockhart J and at 400 per Shepphard J.

8. Further, his Honour ignored entirely or erroneously disregarded other clear disclosures in the specification that support the alternative construction. In particular: **(a)** p 15 lines 3-7 discusses control options that would enable the user to "**access one of a number of secure doors** after his or her identity has been authenticated…". His Honour was wrong to dismiss this disclosure on the basis that there was no reference to a "controlled item" in that passage: J [110]. The passage discusses an example of an accessibility attribute, which "establishes whether and under which conditions access **to the controlled item** should be granted to the user": see p 14 lines 18ff (Pt C Tab 28, AB-1018). Page 14 lines 5-6 also make clear that Figure 3, which is being discussed in that passage, is the method of operation of the transmitter subsystem in Figure 2, which relates to providing access **to a controlled item**; **(b)** p 12 lines 18-21 refers to providing "secure access **to a PC**", which expressly envisages the controlled item being the PC (ie the device to be accessed), rather than a locking mechanism; and **(c)** p 28 lines 14ff, which in particular states

"The system 100 can also be used to provide authorised access to lighting systems, building control devices, exterior or remote devices such as air compressors and so on. The concept of "secure access" is thus extendable beyond near access to restricted physical areas". The experts also agreed that "the controlled item in claim 1 captures or includes, amongst other things, a secured PC to which access of a logical kind is provided: T486.41-487.34 (Pt C Tab 88, AB-3100-3101); JER [18] (Pt C Tab 72, AB-2045); Dunstone 2 [196] (Pt C Tab 43, AB-1384).

9. The primary judge also wrongly concluded that the access granted to the "controlled item" must be unlimited, such that the claims do not encompass a situation where additional authentication may be required to access different parts of the controlled item, such as, for example, a facility with a number of areas secured by doors that require additional authentication before access is granted, or a computer that requires additional authentication in order to gain access to particular files: J [111], [366]. There is nothing in the language of the claims that precludes this, and the specification expressly acknowledges that it may occur: see paragraph 8 above.

B.3 Accessibility attribute (ground 2)

10. It was common ground that the definition of "accessibility attribute" at p 14 lines 18 to 19 of the specification is to be adopted, and the dispute related to how this definition should be understood in the context of the claims: J [112]-[113]. The primary judge correctly found that the claims do not restrict the particular form of the "accessibility attribute" or how it is interpreted or decoded, and correctly characterised the distinctions between the claims: J [118]-[120], [126], [144]. However, in construing "accessibility attribute", his Honour erred in two respects.

11. ***First***, the primary judge incorrectly found that the accessibility attribute must "convey" whether and under which conditions access to the controlled item should be granted and, therefore, itself contain the conditions of access: J [122], [136]-[137]. However, the definition of accessibility attribute at p 14 lines 18 to 19 (set out at J [123]) requires it to "establish", not "convey", whether and under which conditions access to the controlled item should be granted. This is an important distinction. "Establish" means "to set up or bring about", whereas "convey" means "to communicate; impart; make known": see, eg See, Macquarie Dictionary online ed. Thus, an accessibility attribute can establish (ie set up or bring about) whether and under what conditions access should be granted, without necessarily needing to "convey" it directly.

12. This in turn led the primary judge to make a ***second*** error, namely finding that the provision or output of the accessibility attribute must always be separate to the "communication of a biometric match": J [126], [137]. His Honour ought to have found that it is sufficient for there to be a means for "providing" or "outputting" something which, in the context in which this occurs, establishes whether and under which conditions access should be granted; and that where the user seeking access identifies the specific condition of access sought, the authentication may

constitute the provision or output of the accessibility attribute, because it nevertheless establishes whether and under what conditions access should be granted in response to the request.

13. Nothing in the claim language suggests that a "match" must be communicated before and separately from the provision or output of an accessibility attribute, or that a "precondition" kind of secure access is excluded, only that an accessibility attribute is to be "provided" or "output" if a legitimate biometric signal is received. Such a constrained construction is not supported by the language of the claims. Indeed, as the primary judge correctly observed, claim 3 of the 168 Patent is silent as to the conditions for the provision of the accessibility attribute, save that it be received from the transmitter sub-system (**TSS**): J [137]. The claims are silent as to whether a match must occur separately from or as part of the output / provision of an accessibility attribute. Contrary to J [125], claims 1, 2 and 3 of the 168 Patent do not expressly require a biometric signal to be "compared (matched)" against signatures stored in the database at all, and claims 5 and 6 of the 168 Patent and claims 1, 37, 39 and 41 of the 293 Patent only require a "means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute" (emphasis added). This does not suggest that a separate "match" must be communicated prior to the output / provision of the accessibility attribute: cf J [125]-[126]. The requirement that the accessibility attribute only be output / provided if a "legitimate biometric signal is received" does not mean that a match must be communicated prior to the output / provision of an accessibility attribute.

14. This is consistent with the disclosures in the specification. In particular, at p 14 lines 16 to 18 it is stated that the "authentication of the biometric signature matching produces an accessibility attribute for the biometric signal 102 in question" - there is no stipulation that the match and production of the accessibility attribute must be entirely separate. Further, p 14 line 20 to p 15 line 13 confirms that the user can select the specific condition of access sought using the controller (for example one of a number of secure doors), and will obtain access **after** his or her identity has been authenticated. In that instance, the accessibility attribute need not itself contain the conditions of access of the user, because the user has already identified the control option (ie the condition of access) sought, which will be granted after the identity has been authenticated and an appropriate access signal has been sent. The finding at J [136] that this passage is "a different concept to an accessibility attribute" is incorrect - as the chapeau of that passage acknowledges, it is directly concerned with the accessibility attribute.

B.4 Transmitter subsystem / receiver subsystem (ground 3)

15. The primary judge erred in finding that each of the TSS and receiver subsystem (**RSS**) referred to in the claims must be discernible as identifiably separate components: J [163].

16. It is well-established that the claims must be construed in light of the common general knowledge (**CGK**) at the priority date: *Decor Corp* at 391. As to the CGK, both experts agreed that: **(a)** a subsystem **typically performs a specific function** within the context of the larger system; **(b)** subsystems could be defined at many levels of abstraction and, for instance, **a subsystem could contain other subsystems**; and **(c)** subsystems could consist of both hardware and software components and **could interact with other subsystems within the system to carry out complex operations**: J [152], JER [7]. Further, "as a matter of the underlying technology, it is possible to design a computer system, utilising hardware and software, where for efficiency it is useful to have hardware and software components that overlap in function": J [164].

17. The primary judge also correctly found that the TSS and RSS are defined by functionality, and varying degrees of functionality are required by the claims: J [155], [158]-[161], [167]. None of the claims define the TSS and RSS by reference to hardware and software components, save for claim 39 of the 293 Patent, which requires a single apparatus within the RSS to be responsible for enrolling relevant signatures into a database of biometric systems. This tends against any limitation of the subsystems to discernible apparatus that are identifiably separate. Further, the claims contain no language that indicates there be a requisite distance between the TSS and RSS: J [169]. The ordinary meaning of "transmitter" and "receiver" is something that sends, and something that receives, with a path between the two (J [151]; see also T458.14-35), and "transmit" includes transmitting data along a cable in a PC or other logical system, such that there be no physical separation at all: T483.4-9 (Pt C Tab 88, AB-3097), T494.8-31 (Pt C Tab 88, AB-3108), T504.5-505.6 (Pt C Tab 88, AB-3118-3119).

18. Critically, nowhere in the specification is it stated that the TSS and the RSS must be comprised of discrete components. CPC's construction is supported by disclosures in the specification: **(a)** the specification acknowledges at p 14 lines 1-4 that the TSS is "preferably" fabricated in the form of a single integrated circuit; **(b)** at p 12 line 22 to p 13 line 8, the specification recognises that the TSS need not be entirely remote from the remainder of the system, including the second subsystem, being the RSS; **(c)** the specification recognises that the biometric signature database can be part of either the first or second subsystem (thereby recognising that the two subsystems may have overlapping components and functionalities); **(d)** the specification acknowledges that the entire secure access system can exist within a computer system: p 1 lines 21-23, p 10 lines 18-20, p 26 line 3 to p 28 line 10; and **(e)** the specification recognises that, if the secure access system is being applied to providing secure access to a PC, then the secured PC can store the biometric signature of the authorised user in internal memory, and the PC (ie as a whole) can be "integrated into the receiver subsystem": p 12 lines 13-21 (Pt C Tab 28, AB-1016). Where the first subsystem is not remote from the PC, this will necessarily mean that both subsystems are integrated with one another and that requiring that hardware or software functionality not be

deployed in other operations would only promote illogical inefficiency. It also recognises (contrary to J [165]) shared components, in this case a wire: see also T461.11-462.22 (Pt C Tab 88, AB-3075-3076).

19. Further or in the alternative, the primary judge ought to have found that the TSS and RSS need not be defined by every single component that is ancillary or incidental to achieving the required functions of the subsystems. Rather, they should be defined by the quintessential components responsible for achieving their functionalities. Indeed, if - contrary to the submissions above - the TSS and RSS are defined by their components and must be entirely distinct without overlap, then defining the TSS and RSS by reference to every single component involved in achieving the functions of the TSS and RSS would markedly constrain the scope of the claims in a manner not supported by their plain language, the teachings of the specification, and the CGK. As observed above, the claims are defined by function, and (other than claim 39 of the 293 Patent) make no reference to components at all. Further, the specification acknowledges that the TSS and RSS can be <u>within</u> a computer (see, in particular J [662]). There is no logical reason why the TSS and RSS must include every single component, however minor their involvement, in those circumstances - it would necessitate an excessive number of individual components in an electronic system in circumstances where (as the primary judge correctly found at J [164]), it is useful to have hardware and software components that overlap in function.

20. CPC's construction is also supported by the evidence concerning the definition of sub-systems given by the experts, Apple's engineers, and how Apple itself defines its sub-systems: see, for example, T283.4-5, T284.21-22, T282.21-286.23 (Pt C Tab 86, AB-2896-2900), T759.27-760.27 (Pt C Tab 90, AB-3373-3374). Whilst that evidence was given in the context of the Apple Devices, there is no reason to conclude that this is not consistent with the CGK position at the priority date, and is nevertheless supportive of what is, in any event, a plain and common sense construction of TSS and RSS. The primary judge was wrong to exclude it in those circumstances.

21. Finally, to the extent that the primary judge (at J [168]) rejected CPC's construction on the basis that it was raised in closing submissions, and was not directly addressed in the written evidence by the experts, the primary judge also erred. TSS and RSS are not terms of art (J [151]) and construction is a matter for the Court not any expert witness.

B.5 Administrator signature (ground 4)

22. Whilst the primary judge correctly found that an administrator is someone with access privileges needed to perform administrative functions such as enrolling new users, his Honour incorrectly held that an "administrator signature" (which appears in claims 3 and 6 of the 168 Patent; and claims 29 and 41 of the 293 Patent) was a mathematical representation of information obtained

from a biometric signal that matches a stored biometric signal in the database signifying that the person whose signature is used has administrator privileges: J [190], [192].

23. The claims do not limit the way in which the system stores and recognises a signature as an administrator signature, and the definitions of "signature" and "matching" referred to by the primary judge at J [190]-[191] also do not prescribe the more limited construction that the primary judge adopted. Further, the passage of the specification relied upon at J [193] does not support a narrower construction - that passage does not suggest that the administrative privileges associated with each signature are necessarily embedded within the signature itself (ie in the mathematical representation). Provided the system has a means for identifying a particular signature (in that case a finger) with a person who has access privileges needed to perform administrative functions, that is sufficient to constitute an administrative signature. In any event, this is one non-limiting example.

B.6 Series Feature (ground 5)

24. The primary judge ought to have found that the series feature is directed to obtaining a quality biometric signature and requires there to be a sufficient number of entries and duration of each entry to obtain a sufficient scan that can be mapped into an instruction: cf J [210]-[211].

25. As the primary judge correctly observed at J [198] - it is plain from the language of the series feature that it concerns the process of enrolment, and users who were new to a secure access system needed to enrol their relevant biometric attributes, which usually involved presenting the biometric attribute to a sensor several times to ensure a sufficient quality scan. The evidence also established that, during enrolment, it was common to get more than one impression or sample (typically three or more) and those samples could then be dealt with in a number of ways, including but not limited to (most commonly) taking individual biometric samples and saving them as individual templates: T565.6-566.1 (Pt C Tab 89, AB-3179-3180), T594.27-596.42 (Pt C Tab 89, AB-3208-3210), T603.25-47 (Pt C Tab 89, AB-3217); Dunstone 2 [229(a)] (Pt C Tab 43, AB-1396-1397).

26. Contrary to J [201], that is precisely what the language of the series feature envisages. The integer requires: **(a)** a means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry - ie a means for receiving the presentation of the biometric attribute to the sensor at least once and for a sufficient duration to ensure sufficient quality scan(s); **(b)** a means for mapping said series into an instruction - ie a means for taking the series (the one or more scans) and mapping it into an instruction (such as an instruction to save the samples as individual templates as the signature of a particular user in the database); and **(c)** a means for enrolling relevant signatures into the database according to the instruction. This is essential to ensure that

an adequately high quality signature can be enrolled in the database according to the instruction. Otherwise, secure access may not be able to be granted. Contrary to J [201], this feature is not required to be expressly stated for matching - a match will necessarily only occur when a sufficient quality scan occurs, whereas secure access to the system may not be achieved if a poor quality scan is saved as the biometric signature.

27. In contrast, the primary judge's construction does not give effect to the whole of the claim language. In particular, it fails to grapple with the fact that integer (7) requires "**mapping** said series into an instruction" (emphasis added). No explanation is provided for how the primary judge's construction gives effect to this requirement. Nor is it apparent how the signatures are enrolled "**according** to the instruction" on the primary judge's construction.

C. INFRINGEMENT - GROUNDS 6 AND 7

28. In light of the erroneous constructions adopted by the primary judge, the primary judge also erred in finding that the Apple Devices did not possess each of the above-mentioned integers: J [375], [376], [384], [431]-[433], [440], [444], [446]-[447], [453], [460]-[461], [462].

29. Further or in the alternative, having incorrectly found (at J [151], [168], [399], [419]-[421]) that the TSS and RSS were not able to be defined by the quintessential components responsible for achieving their functionalities, the primary judge approached the question of whether the Apple Devices possessed a TSS and an RSS through the wrong lens. The primary judge ought to have found that the components identified in J [383] and [384] are the key or quintessential components responsible for the functionalities required of the TSS and the RSS respectively. This was supported by the evidence: T283.4-9 (Pt C Tab 86, AB-2897), T284.21-22 (Pt C Tab 86, AB-2898), T314-329 (Pt C Tab 86, AB-2928-2943), T434.19-35 (Pt C Tab 88, AB-3048), T439.26-39 (Pt C Tab 88, AB-3053), T472.15-30 (Pt C Tab 88, AB-3086), T759.27-760.27 (Pt C Tab 90, AB-3373-3374); T772-780 (Pt C Tab 91, AB-3386-3394); Benson 1 [60] (Pt C Tab 50, AB-1651).

30. Similarly, having incorrectly found (at J [439]-[440]) that the Apple Devices could not be a controlled item by reason of the erroneous construction adopted; and made the erroneous findings regarding the construction of accessibility attribute discussed in paragraphs 10 to 14 above, the primary judge erred in finding that the steps referred to in J [431], or alternatively J [432], did not involve the output or provision of an accessibility attribute.

31. Finally, the primary judge incorrectly implied that CPC advanced a construction with an eye to infringement: J [410]. The construction advanced by CPC is correct and accords with well-established principles for the reasons outlined above.

D. DEFERRED PRIORITY DATE - GROUND 8

32. The primary judge correctly outlined the principles concerning external fair basis at J [473]-[481], but misapplied those principles in finding that there was no real and reasonably clear disclosure in the **Provisional** specification of the following integers (Pt C Tab 27).

33. **Accessibility attribute** - it is convenient to focus on CPC's construction. If, as CPC contends, it is sufficient for there to be a means for "providing" or "outputting" something which, in the context in which this occurs, establishes whether and under which conditions access should be granted, then the passage of the Provisional set out at J [489] plainly discloses an accessibility attribute. It discloses access privileges being contained in a database and "comprehensive access privilege screening". Further, in the (non-limiting) example in the Provisional of Tom Smith, after authentication has occurred and a check is done to determine whether Tom Smith can use the door, there is a communication that will either allow Tom Smith to access the door, or not, which thereby determines whether and under what conditions access can be granted. Such disclosure is sufficient, particularly when (as the primary judge acknowledged at J [478]) the invention need only be disclosed in a fairly provisional or rough state.

34. **Administrator signature and series feature -** In the event that the disclosures in Mathiassen, Scott and Hamid are sufficient to disclose an administrator signature on CPC's construction, and (as Apple contends by way of its cross-appeal) Mathiassen, Scott, Hamid and Wuidart disclose the series feature on CPC's construction, it necessarily follows that there is a real and reasonably clear disclosure (which has a lower bar for disclosure) of those integers in the Provisional.

E. NOVELTY - GROUNDS 9 AND 10

E.1 Wuidart (ground 9, and ground 10 insofar as it concerns Wuidart)

35. The primary judge erred in finding that claims 1, 2 and 5 of the 168 Patent are not novel light of Wuidart (both on CPC and Apple's construction). The primary judge incorrectly held that the instigation of "convenience functions" in a vehicle, such as adjusting the position of the seats, constituted conditional access within the meaning of accessibility attribute: J [641]-[644]. As the primary judge correctly held, an accessibility attribute determines whether and under what conditions access to the controlled item is granted: J [112]. A change in a "convenience function" inside a vehicle has no bearing on any condition of access to the vehicle. Contrary to J [642]-[643], there is a key distinction between the "convenience functions" disclosed in Wuidart and the duress, alert and telemetry attributes discussed in the specification at p 14 line 20 to page 15 line 1. In the case of the latter, two of the attributes mentioned (the alert and telemetry attributes) do not permit access at all, and, in the case of the "duress attribute", access is granted but only on the condition that there is an alert to advise authorities of access under

duress. Thus, the duress attribute is directly related to the conditional access granted. Notably, neither expert suggested that the "convenience functions" in Wuidart were access conditions: CB Tab 40.13, integer 1.4 (Pt C Tab 46, AB-1548-1549); CB Tab 33.9 integer 1.4 (Pt C Tab 38, AB-1292).

36. Further, the primary judge erred in relying upon the disclosure in Wuidart concerning the "unlock signal" to: **(a)** find that Wuidart discloses a system in which the TSS alone determines whether and under which conditions access should be granted; and **(b)** refute CPC's contention that Wuidart did not anticipate an accessibility attribute because it required two signals to be produced before the unlock signal is generated, instead of just biometric authentication: J [638]-[640]. The unlock signal is a purely binary lock/unlock signal and (in accordance with the primary judge's own findings) cannot be an accessibility attribute.

E.2 Other prior art (ground 10)

37. Ground 10 addresses the primary judge's findings that Scott, Hamid, Mathiassen and Wuidart disclose an accessibility attribute and an administrator signature (other than in the case of Wuidart) on CPC's construction. The primary judge correctly found that other integers (the series feature and, in the case of Hamid, the secure access signal), as construed by CPC, were not disclosed, which are the subject of Apple's cross-appeal.

38. As to **accessibility attribute** - CPC contends that the primary judge incorrectly held that each of Scott, Hamid and Mathiassen (and Wuidart, which is addressed above) discloses an accessibility attribute on CPC's construction. The disclosures in those prior art documents are vague and do not provide the accuracy of a sniper as required by the authorities. In particular, the primary judge erred in finding that there was a clear and unmistakeable direction in Scott, Hamid and Mathiassen of a system where the determination of whether and under what conditions access should be granted occurred in the TSS, rather than the RSS. Relatedly, the primary judge erred in not considering and failing to find at J [614] that Mathiassen disclosed an accessibility attribute. Mathiassen discloses multiple signals being broadcast to separate receivers, rather than over a single connection. Therefore, it does not disclose a secure access signal that contains material as to whether and under which conditions access should be granted.

39. As to **administrator signature** – the primary judge erred in finding that each of Scott, Hamid and Mathiassen disclosed an administrator signature on CPC's construction of that integer. The nature of the error is the same for each piece of prior art. Whilst the claims do not limit the way in which the system stores and recognises a signature as an administrator signature (as discussed in paragraphs 22 and 23 above), they nevertheless require the system to store and have the capacity to recognise a signature as an administrator signature in some way. In each of Scott,

Hamid and Mathiassen, whilst reference is made to administrator like functionalities, those functionalities are not disclosed to be tied to the administrator's signature in any requisite sense.

F. CONCLUSION

40. For the reasons outlined in these submissions, which will be expanded upon at the hearing, CPC's appeal ought to be allowed; resulting in a finding that Apple Devices have infringed the asserted claims in each of the Patents in suit.

AJL Bannon, C Dimitriadis, M Evetts
Counsel for CPC

Gilbert + Tobin
Solicitors for CPC

20 February 2026