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 4:19:37 PM AEDT
Date Accepted for Filing:	20/02/2026 4:19:36 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.

No. NSD 1288 of 2025

Federal Court of Australia

District Registry: New South Wales

Division: General

On appeal from the Federal Court

CPC PATENT TECHNOLOGIES PTY LTD (ACN 615 736 028)

Appellant/Cross-Respondent

APPLE PTY LIMITED (ACN 002 510 054) and another

Respondents/Cross-Appellant

Apple's outline of submissions in chief on the cross-appeal

Filed on behalf of (name & role of party) Apple Pty Limited and Apple Inc (Respondents)

Prepared by (name of person/lawyer) Robynne Sanders

Law firm (if applicable) DLA Piper Australia

Tel 03 9274 5539 Ref 00314520-000147

Email Robynne.sanders@dlapiper.com

Address for service (include state and postcode)

DLA Piper Australia
80 Collins Street
Melbourne 3000 VIC

A. INTRODUCTION

1. In this proceeding, Apple[1] defended CPC's patent infringement case by submitting that, on the proper construction of the claims, Apple did not infringe; but if CPC's claim constructions applied, the claims were invalid. Apple succeeded, including because the PJ largely accepted Apple's claim constructions and evidence as to the operation of the Apple Devices, such that Apple did not infringe.

2. As a result, the PJ did not need to determine many of the grounds of invalidity advanced by Apple in its cross-claim, which were premised on CPC's claim constructions, although in some instances, the PJ did so anyway. To the extent that, contrary to Apple's submissions on the appeal, this Court decides that CPC's claim constructions are correct (with the consequence that a claim is infringed and not otherwise invalid), it would be necessary to determine those grounds. That is largely the purpose of this cross-appeal.

3. In summary: (a) where the PJ did not consider the relevant ground, this Court would remit the matter to the PJ for determination (cross-appeal grounds 1, 2, 3 and 4(a)); and (b) in relation to the question whether the Series Feature was disclosed by the prior art on CPC's construction, the PJ should have held that it was (ground 4(b)).

4. Two further matters are raised in the cross-appeal. *First*, the PJ should have held that, properly construed, a "*secure access signal*" is disclosed by Hamid (ground 4(c)).

5. *Secondly*, the PJ correctly held that the terms "*transmitter subsystem*" (**TSS**) and "*receiver subsystem*" (**RSS**) of the claims must be separate and distinct subsystems (Reasons at [167]). That was sufficient for Apple to succeed on non-infringement. However, the PJ could have gone further, and determined that those terms refer, in the context of these Patents, to separate and distinct items of *hardware* (onto which software is loaded). A particular aspect of that context is that the specification, consistently with the nature and purpose of the invention, describes the TSS and RSS in that way.

6. This point is primarily the subject of Apple's notice of contention (ground 1), which will be addressed in separate submissions. The aspect of this point which is relevant to the cross-appeal is that, if this Court holds that the disclosure in the body of the specification is limited to an invention in which the TSS and RSS use separate items of hardware, but the claims are not so limited, they are not fairly based (ground 5).

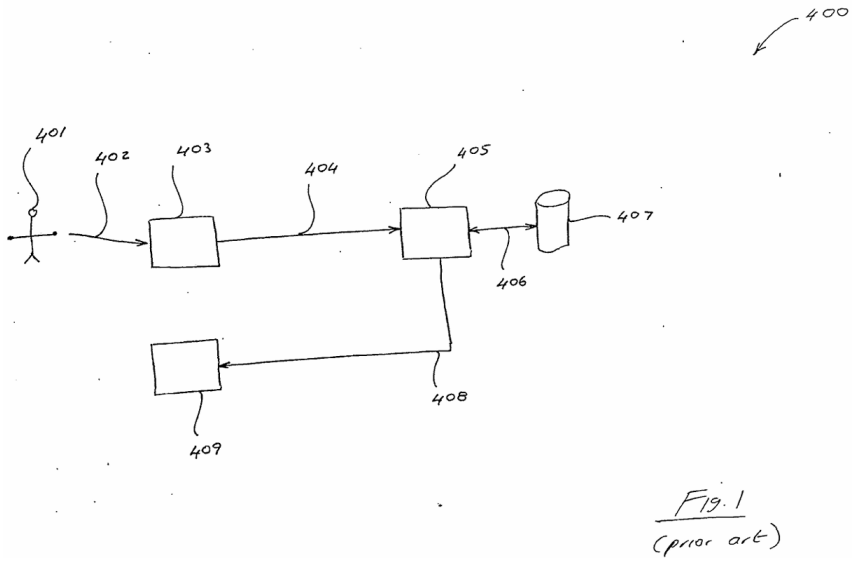
---

[1] Capitalised terms have the meanings given in *CPC Patent Technologies Pty Ltd v Apple Pty Ltd* [2025] FCA 489 (**Reasons**) unless otherwise indicated.

B. BACKGROUND – THE PROVISIONAL AND THE PATENTS

7. This section summarises key aspects of the Provisional, the 168 Patent and the 293 Patent relevant to this appeal, with references to the Reasons. The Provisional is relevant in particular to the priority date (subject of the notices of appeal and contention), and is addressed here for convenience.

8. **The Provisional** identifies a problem arising from the use of a physical cable carrying a transmission between a code entry module (e.g., in an enclosure on a door jamb) and a controller which controls access to the door, namely that the cable can be the subject of physical interference and replay attacks may be carried out on it to gain unauthorised access. In this context, the prior art is depicted by hand-drawn Fig. 1 (Reasons at [482]):



9. A user (401) provides a fingerprint (402) on a biometric sensor of a code entry module (403) located on the external jamb of a door. The module transmits a scan of the fingerprint via cable (404) to a controller (405) which is contained in a hidden location such as the roof of a building. The controller interrogates (406) a database of fingerprints (407) to authenticate the user. If it determines a match, the controller sends a signal (408) to the door locking mechanism (409) to unlock it.[2] In another example, there may be a number of such mechanisms associated with a number of doors in a building, to which the controller may provide access. In such a case, the user may be presented with means to select which door she or he wishes to unlock, referred to as a "*control option*".[3]

10. The Provisional discloses that there is a risk that the signal sent over the cable (404) can be intercepted by an unauthorised person gaining physical access to the cable,[4] and describes

[2] Provisional 1:6-2:2 (Appeal Book Part C (**Pt C**) Tab 27 AB-985-986); Reasons at [483].
[3] Provisional 8:3-14 (Pt C Tab 27 AB-992).
[4] Provisional 2:4-10 (Pt C Tab 27 AB-986).

the risk that captured information can be "*replayed in order to gain the access which rightfully belongs to the user*".[5] Similarly, that cable is described as providing an "*attack point for the unauthorised person*".[6]

11. The specification then identifies the asserted advance in the art as follows:[7]

> *Disclosed are arrangements which seek to address the above problems by replacing the vulnerable wired path 404 with a strongly encrypted wireless path between the code entry module and the controller, and by incorporating biometric authentication at the code entry module 403.*

12. That passage emphasises two aspects: (a) replacing the cable (404) with a strongly encrypted wireless path; and (b) undertaking the fingerprint matching process on the transmitter side, that is, at the code entry module (403), so that the fingerprint signal itself is not transmitted over the vulnerable wired path (404). Both aspects together (not individually) are used to address the above problems.

13. Consistently with that description, the invention is depicted in Figure 2 as follows:

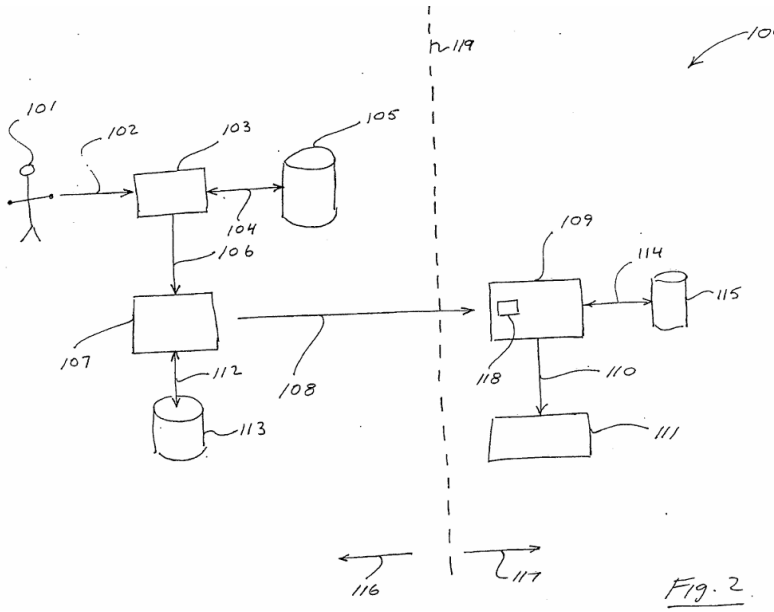


Fig. 2

14. The specification explains that the components and functions on the left-hand side of the dotted line (119) can be implemented in a number of different forms, and provides two alternatives: a portable fob carried by a user; or a protected enclosure on the outside jamb of a secure door, each used to gain access to a door of a building.[8] Thus, a user (101) provides a fingerprint (102) to the sensor of an item of hardware referred to as the code entry module (103) of the fob (116). The code entry module interrogates (104) a database of fingerprints (105) and, if a match is found, sends a signal (106) to a controller/transmitter

[5] Provisional 2:9-10 (Pt C Tab 27 AB-986).
[6] Provisional 2:21-22 (Pt C Tab 27 AB-986) and see Reasons at [484].
[7] Provisional 3:3-6 (Pt C Tab 27 AB-987); Reasons [485].
[8] Provisional 5:22-26 (Pt C Tab 27 AB-989).

(107). The current 'rolling code' is obtained (112) from the code database (113) and then transmitted wirelessly (108) from the fob to a separate piece of hardware referred to as a hidden controller (109) containing a receiver (118). The controller checks the legitimacy of the transmission by consulting (114) its rolling code database (115) and then sends an unlocking command (110) to the door locking mechanism (111).[9]

15. An alternative application is also disclosed in which the user desires access to a PC:[10]

> *In the event that 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 can be integrated into the sub-system 117 of Fig. 1.*

16. Importantly, the computer does not embody both subsystem (116) and subsystem (117). Rather, it is disclosed that the PC may be integrated into subsystem (117). Since that subsystem receives a wireless signal from subsystem (116), the two subsystems are therefore distinct items of hardware separated by a wireless communication channel. In other words, what is described is that the user is seeking access to a PC using a separate computing device, for example, a fob, or a remote computer.

17. The description sums up by stating:[11]

> *Accordingly, existing systems as are described in Fig. 1 can be upgraded by replacing the code entry module 403 and the transmission path 404, leaving the other components of the system 400 (ie., the controller 405, the code database 407, and the controlled item 409, together with existing wiring 408 and 406), largely intact. Minor modifications might however be necessary. When upgrading systems in this manner, the sub-system 116 can either be used in a remote fob configuration, or can be placed in a secure housing on an external door jamb.*

18. However, as the evidence before the PJ demonstrated (and the prior art exemplified), the advance touted – using an encrypted wireless pathway and performing the biometric authentication on the transmitter side – was in truth a commonly known way of implementing access through a secure door. Perhaps for that reason, the drafter of the later filed Patents sought to introduce different features, as addressed in the following sections.

19. **The 168 Patent** contains a similar description of the prior art by reference to Figure 1 (though no longer hand-drawn). But then it takes a different tack in a number of respects.

20. First, it no longer confines itself to using a wireless path from the transmitter to the receiver; this is now only "*typical*" and there are instances where a "*wired medium*" may be used, particularly where the TSS (116) is mounted in a door jamb enclosure rather than a key fob.[12]

---

[9] Provisional 4:9-26 (Pt C Tab 27 AB-988); Reasons [488].
[10] Provisional 6:6-13 (Pt C Tab 27 AB-990).
[11] Provisional 10:16-22 (Pt C Tab 27 AB-994); Reasons [490].
[12] 168 Patent 12:9-12 (Pt C Tab 28 AB-1016); Reasons [65].

Consistently with this, the relevant claims of the 168 Patent are not limited to the use of a wireless path between the two subsystems.

21. Importantly, though, the description continues to identify the TSS and RSS as separate and distinct items of hardware (onto which software is loaded). Thus, the disclosure concerning access to a PC continues to refer to the PC as being integrated into the RSS, and separate from the TSS.[13] That RSS receives a communication from the TSS, which may be transmitted over a wired or wireless medium. Again, since the two subsystems are separated by a wired or wireless medium, they remain distinct pieces of hardware.

22. Consistently with this, the new disclosure in Figure 10 and its associated description[14] identifies the TSS and RSS as separate items of hardware (onto which software is loaded) separated by a communications network, which may be wired or wireless.[15] Thus, each of the TSS (116) and RSS (117) are computing devices: they incorporate their own "*controller module*" or "*processor module*", which includes a "*processor unit*" and a "*memory unit*", each being hardware. The software, which provides the method steps of the secure access system, is described as being: (a) "*loaded into*" the TSS and the RSS, that is, loaded onto the memory unit; and (b) "*executed under direction of*" the processor unit. The TSS and RSS so described are connected by a communications network, which may be wired or wireless.

23. Secondly, the specification contains new disclosure concerning an "accessibility attribute" (**AA**). In particular, the specification states:[16]

> *The authentication of the biometric signature matching produces an accessibility attribute for the biometric signal 102 in question. The accessibility attribute establishes whether and under which conditions access to the controlled item 111 should be granted to a user. Thus, for example, the accessibility attribute may comprise one or more of an access attribute (granting unconditional access), a duress attribute (granting access but with activation of an alert tone to advise authorities of the duress situation), an alert attribute (sounding a chime indicating that an unauthorised, but not necessarily hostile, person is seeking access, and a telemetry attribute, which represents a communication channel for communicating state information for the transmitter sub-system to the receiver sub-system such as a "low battery" condition.*

24. Thus, as the PJ held,[17] an AA is an item of information that specifies not just whether access is granted (i.e., whether the biometric preconditions to access have been met), but also the

---

[13] 168 Patent 12:18-21 (Pt C Tab 28 AB-1016).
[14] 168 Patent 26:3-28:10 (Pt C Tab 28 AB-1030-1032); see Reasons [83]-[85].
[15] See: Boztas at T451.44-T452.5 (Pt C Tab 88 AB-3065-3066); T456.7-11 (Pt C Tab 88 AB-3070); T467.19-24 (Pt C Tab 88 AB-3081); T468.25-28 (Pt C Tab 88 AB-3082); Dunstone at T468.9-16 (Pt C Tab 88 AB-3082).
[16] 168 Patent 14:14-15:7 (Pt C Tab 28 AB-1018-1019); Reasons [72].
[17] Reasons at [126]; see also: Apple's Closing Submissions on Infringement (**ACS Inf**) at [52]-[65] (Pt C Tab 80 AB-2455-2458); First Affidavit of Serdar Boztas dated 2 March 2023 (**Boztas 1**) at [111] (Pt C Tab 35 AB-1214); Second Affidavit of Edward Simon Dunstone dated 24 March 2023 at [203]-[204], in particular at [204(a)] (Pt C Tab 43 AB-1385-1388).

conditions under which access is granted, such as the granting of access subject to the provision of an alert tone in the case of duress (i.e. conditions providing different kinds of access). All of the claims of the 168 Patent require an AA.

25. And as the PJ also correctly held,[18] the AA is a different concept from the "control option" (first referred to in the Provisional). The control option allows a user to select which of a number of controlled items s/he wishes to access (a controlled item being the item or items to which the RSS can give access, for example, doors in a building). By contrast, the AA requires the controller to establish, in relation to any such door, not only whether access is to be granted, but under which conditions, such as the grant of access with an alert tone.

26. Thirdly, the specification describes aspects of enrolling users. The first aspect of enrolment disclosed in the 168 Patent is that *enrolment is performed at the TSS*, i.e., using the biometric sensor (121) in Figure 2.[19] (An effect of performing enrolment at the TSS rather than, say, at a computer connected to a central server, is that biometric processing may be confined to the TSS, so that biometric information need not be transmitted between different components of the system.) This is a requirement of all claims of the 168 Patent.

27. The second aspect of enrolment disclosed is the role of an administrator in enrolling users at the code entry module. Administrators have the ability to amend data stored in the database (including permitting the enrolment of ordinary users), whereas ordinary users do not.[20] Notably, it is a particular fingerprint, not a person, which is designated by the system as an administrator fingerprint (i.e., an "*administrator signature*").[21] In practical terms, this means that the code entry module will require that fingerprint to be presented to the sensor in order to permit administrative functions to be performed, such as enrolling ordinary users. The administrator signature is a feature of, for example, claims 3 and 6 of the 168 Patent.

28. The third aspect of enrolment disclosed is the interaction with the code entry module to enter enrolment mode. If the same sensor is used for both access and enrolment, the system needs to know when a finger press is to be treated as (i) a request for access or (ii) an instruction to enter enrolment mode, so that a new fingerprint can be enrolled. The specification discloses that "*entering enrolment mode can occur by the administrator providing a series of finger presses of appropriate number and duration*". Thus, page 19, lines 12-21 states:

> *In one arrangement, the control information is encoded by either or both (a) the number of finger presses and (b) the relative duration of the finger presses. If the successive*

[18] Reasons at [134]-[136]; see also: ACS Inf at [66]-[76] (Pt C Tab 80 AB-2458-2460); Boztas and Dunstone at T671.37-T672.9 (Pt C Tab 90 AB-3285-3286).
[19] 168 Patent 9:24-10:3 (Pt C Tab 28 AB-1013-1014).
[20] 168 Patent 18:18-21 ff (Pt C Tab 28 AB-1022); Reasons at [78].
[21] 168 Patent 19:1-6 (Pt C Tab 28 AB-1023); Reasons at [79]; see also: ACS Inf at [83] (Pt C Tab 80 AB-2461); Boztas at T579.42-T580.10 (Pt C Tab 89 AB-3193-3194).

finger presses are provided within this predetermined time, then the controller accepts the presses as potential control information and checks the input information against a stored set of legal control signals.

One example of a legal control signal can be expressed as follows:

"Enrol an ordinary user" -> dit, dit, dit, dah

Where "dit" is a finger press of one second's duration … and "dah" is a finger press of two second's duration.

29. This is the subject of the claims of **the 293 Patent**. The specification of the 293 Patent is the same, except for the consistory clauses and claims. The claims focus in particular on a feature which involves providing a series of entries of a biometric signal characterised by the number and/or duration of entries, and mapping that series into an instruction for enrolling relevant signatures into the database: see Reasons at [199] (the **Series Feature**). This reflects the description of a series of presses to enter enrolment mode, quoted above.

C. GROUNDS 1 to 4(a): matters for remitter if CPC's constructions preferred

30. The grounds of invalidity which the PJ did not decide are inventive step, manner of manufacture, the s 40 grounds identified in his Reasons at [663], [665] and [670], and lack of novelty based on iPAQ. Each involve, or potentially involve, consideration of the expert evidence on those topics, which is not before this Court and in respect of which the PJ did not make findings. To the extent that this Court finds that CPC's claim constructions were correct, such that the Apple Devices infringe, and the claims are not otherwise invalid, the proceeding should be remitted for determination of those grounds.

D. GROUND 4(b) – Novelty: Series Feature

31. As the PJ identified in his Reasons at [196], CPC contended that the Series Feature required: (a) capturing multiple scans of a finger, where the finger has to be held on the sensor long enough to obtain a scan; and (b) mapping those scans into a single mathematical representation, the mathematical representation then being saved in the database as a biometric signature.[22] The PJ correctly rejected that construction because it failed to reflect the claim language (and bore no relation to anything disclosed in the specification). Rather, the claim language describes something quite different: a series of signals characterised by the number and/or duration of them (e.g., "*dit, dit, dit, dah*"), and the mapping of that series to an instruction for enrolling relevant signatures (Reasons at [210]-[212]).[23]

32. Nevertheless, on the cross-claim, the PJ proceeded to consider whether the Series Feature as

[22] See Boztas 1 [125] (Pt C Tab 35 AB-1216), T588.21-T591.10 (Pt C Tab 89 AB-3202-3025) and T880.24-36 (Pt C Tab 91 AB-3494); ACS Inf at [91]-[98] (Pt C Tab 80 AB-2463-2464).
[23] See also: ACS Inf at [90] (Pt C Tab 80 AB-2462-2463); Dunstone at T582.9-18, 34-40 (Pt C Tab 89 AB-3196).

construed by CPC was disclosed in Mathiassen, Scott, Hamid and Wuidart, and held that it was not. Mathiassen is addressed first, because it is a case of express disclosure.

33. At J [616], the PJ said:

> *Mathiassen discloses at [0164] that enrolment involves "successful capturing of a minimum of images (say three) reduced to master minutiae tables", there is no disclosure that the user's finger be placed on the sensor a sufficient number of times, and for a sufficient number duration, to obtain a quality series of entries that could be mapped onto a mathematical representation.*

34. In so holding, the PJ appears to have overlooked Mathiassen at [130] (emphasis added):

> *The administrative software will be set up to require a minimum of say 3 minutiae fingerprint representations <u>of acceptable quality</u>. If any of these fingerprint <u>captures are of inferior quality, the administrative software will reject the attempt</u>. <u>When sufficient (say three) minutiae tables of the system administrator has been captured with accepted quality, these will be stored in non-volatile memory (7, 7A or 7C) as the system administrator's master minutiae table</u>.*

35. That appears in the context of the medicine cabinet embodiment, but Mathiassen at [164] proceeds to describe the same process in relation to the vehicle embodiment. Thus, the PJ should have found that the Series Feature was disclosed on CPC's construction.[24]

36. As to Scott, Hamid and Wuidart, each of those citations disclosed that the relevant systems included enrolment of biometric signatures.[25] As the PJ recorded, Apple submitted that, on CPC's construction, the Series Feature is inherently present in any system for enrolling biometric signatures, and accordingly is implicitly disclosed.[26] The PJ set out the principles applicable to implicit disclosure at Reasons [526]-[527], the essence of which is that, if the skilled addressee understands that the system disclosed necessarily includes the feature, even if it is not expressly referred to, it is implicitly disclosed.

37. The expert evidence established the case of implicit disclosure. Boztas confirmed in oral evidence the content of the CGK Summary[27] in which it was agreed that, for enrolment, multiple presentations of a fingerprint were necessary; he further accepted that (i) multiple presentations were necessary in order to capture different parts of the fingerprint; (ii) from those scans a template or mathematical representation is produced; (iii) that was the case in a biometric access system in 2003; and agreed that (i) he did not need to be told about the

---

[24] See Apple's Closing Submissions on Invalidity (**ACSI**) [106]-[107], [116] (Pt C Tab 79 AB-2357, 2359); Boztas at T927.3-T928.21 (Pt C Tab 91 AB-3541-3542), T943.20-944.32 (Pt C Tab 92 AB-3557-3558); T1313.4-T1316.23 (Pt C Tab 96 AB-3927-3930).

[25] See Reasons [538] (Scott); J [570] (Hamid); J [630] and see Wuidart Col 4:37-48 (Wuidart) (Pt C Tab 33 AB-1180).

[26] Reasons [545], [588], [645]; ACSI [76], [102], [123], [146] (Pt C Tab 79 AB-2347, 2356, 2361, 2367); Boztas at T900.22-T903.17 (Pt C Tab 91 AB-3514-3517).

[27] Combined Primer and CGK Summary dated 1 September 2023 (**CGK Summary**) at [115] (Pt C Tab 70 AB-1974).

multiple presentations of the fingerprint in order to know that that was how the enrolling process of Hamid worked (Hamid being the first piece of prior art cross-examined upon); and (ii) it was inherent in the function of every fingerprint scanner that you needed to present your finger for sufficient time for the sensor to capture a biometric signal.[28]

38. However, having correctly identified that Apple's case was one of implicit disclosure, the PJ did not in substance address that case, including the above evidence, but rather appeared to only consider whether the feature was expressly disclosed. About Scott, the PJ said:[29]

> *CPC observes that enrolment is addressed in the passage cited in column 9 lines 54 to column 10 line 13 (of which the key portion is extracted above), which, whilst providing that a finger must be placed on the sensor at least once, for some unknown period of time, there is no indication that this involved placing the finger on the sensor a sufficient number of times, and for a sufficient duration, to obtain a quality series of entries that could be mapped onto a mathematical representation. I accept CPC's submission that this is not sufficient disclosure.*

39. But once regard is had to the above evidence, the correct conclusion is that the Series Feature, on CPC's construction, is implicitly disclosed by Scott, Hamid and Wuidart.

E. GROUND 4(c) – Novelty: Hamid/secure access signal

40. Apple's submission in relation to the construction of the term "*secure access signal*" was this: "*secure*" may encompass a range of measures; none is absolute, but each may provide some level of security to a signal; encryption of the signal is one such measure; and requiring that the signal be transmitted from an authenticated source is another.[30] Boztas accepted those propositions.[31] Thus, a signal which requires biometric authentication in order to transmit it is a secure access signal. The PJ referred to parts of that submission at J [173], though without using the term "*authentication*", even though ACSI [64]-[68] did so.

41. CPC's position did not materially differ. It too accepted that "*secure access signal*" did not require the signal itself be encrypted. Indeed, the communications CPC relied upon in the Apple devices were not encrypted, but rather *authenticated*, in that they were transmitted by a trusted source; and CPC submitted[32] that the secure access signal must be "*'secure' in some way, whether by encryption, <u>authentication</u> or otherwise*" (emphasis added).

42. Consistently with the submissions of both parties, the PJ found in his Reasons at [176] that "*It must properly be said that the access signal within the system is secure, whether by*

---

[28] And Dr Dunstone agreed with those propositions. See T900.22-901.41, T902:19-24, T903:11-17 (Pt C Tab 91 AB-3514-3517).
[29] Reasons at [559]. See also Reasons at [588] (Hamid), [645] (Wuidart).
[30] ACSI [64]-[68]; see also [100] (Pt C Tab 79 AB-2344-2346, 2355); 168 Patent 13:20-25 (Pt C Tab 28 AB-1017); CGK Summary at [98]-[99] (Pt C Tab 70 AB-1971).
[31] See ACSI [67] (Pt C Tab 79 AB-2345-2346); Boztas at T897:26-898:34 (Pt C Tab 91 AB-3511-3512).
[32] CPC's Closing Submissions on Infringement (**CPC CSI**) at [86], [164]-[169] (Pt C Tab 78 AB-2288, 2306-2308).

encryption, <u>authentication</u> or some other means" (emphasis added). That being so, the PJ ought to have found that Hamid disclosed a secure access signal, since, as the PJ found at Reasons [581]-[582], the signal required authentication in order to be transmitted.

F. GROUND 5 – Fair basis: TSS and RSS

43. As submitted above, and as will be further addressed in relation to the notice of contention, the body of the specifications disclose the TSS and RSS to comprise separate items of hardware (onto which software is loaded), separated by a wired or wireless communication channel. That is unsurprising: a fundamental purpose of the invention is to ameliorate a weak point in a system of that kind, being the communication channel between the two devices, including by confining biometric signals to the transmitter side of that channel. Consistently with this, Boztas accepted that the specification only described the TSS and RSS as being separate items of hardware.[33] He also emphasised that "*A big part of the invention is about transmitting – transmission of something from a transmitter to a receiver. So while it's possible to implement some of – some of these innovations in a standard computer, it's the access part of it – the providing secure access part of it is – is irrelevant unless there are two different computers and a transmission mechanism*".[34]

44. There is no disclosure of how one might embody a TSS and a RSS of the invention on a single item of hardware, much less what the purpose would be in doing so. That is to say, there is no real and reasonably clear disclosure of an invention in which the TSS and RSS are embodied on a single item of hardware; that would be a system different in kind from what is disclosed. It follows that if (contrary to Apple's submission) the claims are construed such that the TSS and RSS are not separate and distinct items of hardware, they lack fair basis on the principles set out by the PJ at Reasons [653]-[655].

45. In concluding to the contrary, the PJ's error was to hold that the specification did disclose the embodiment of a TSS and a RSS on a single piece of hardware. The PJ said at [662]:

> *Several passages in the specification identify that the invention may be implemented not only using a physical mechanism, but also by the provision of logical access such as in the case of a personal computer. On page 26 from lines 3 to 13 (set out in section 3 above) the specification identifies that the secure access methods are preferably practiced using a computer system arrangement and may be implemented as software. Having regard to these disclosures, I am not persuaded that the claims lack fair basis for the reason advanced by Apple.*

46. In so saying, the PJ failed to recognise that, when the specification describes the provision of logical access to a PC, it is describing access *from another item of hardware*, such as a

[33] T459.34-T460.1 (Pt C Tab 88 AB-3073-3074).
[34] T441.45-T442 (Pt C Tab 88 AB-3055-3056).

fob or a remote computer (as Boztas acknowledged). The passage on page 26 to which the PJ referred, unambiguously discloses the same thing. It forms part of the description of Figure 10 (see Reasons at [83]-[85]) which, as submitted above, depicts and describes the TSS and RSS as separate computing devices (on which software is loaded) with a wired or wireless communication channel between them.

2 February 2026

Tom Cordiner, Angus Lang, Peter Creighton-Selvay