Details of Filing

File Number:	A24/2024
File Title:	CD & Anor v. Director of Public Prosecutions (SA) & Anor
Registry:	Adelaide
Document filed:	Form 27D - 1st Respondent's submissions
Filing party:	Respondents
Date filed:	17 Apr 2025

Important Information

IN THE HIGH COURT OF AUSTRALIA
ADELAIDE REGISTRY
BETWEEN:

CD
First appellant
and
TB
Second appellant

and

DIRECTOR OF PUBLIC PROSECUTIONS (SA)
First respondent
and
ATTORNEY-GENERAL OF THE COMMONWEALTH OF AUSTRALIA
Second respondent

FIRST RESPONDENT'S SUBMISSIONS

PART I: CERTIFICATION

1. This submission is in a form suitable for publication on the internet.

PART II: CONCISE STATEMENT OF THE ISSUES

2. Should special leave be rescinded because of the enactment of the *Surveillance Legislation (Confirmation of Application) Act 2024* (**CA**)?

3. Assuming special leave is not rescinded, the First Respondent (**DPP**) agrees with the Appellants' articulation of the primary issue arising for determination, being when is a communication[1] passing over a telecommunications system for the purposes of s 7(1) of the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIAA**).[2]

4. The DPP also agrees that the primary issue raises for consideration the proper construction of s 5F TIAA, which prescribes when a communication is taken to *start* and *cease* passing over a telecommunications system.[3]

PART IIA: SPECIAL LEAVE SHOULD BE RESCINDED

5. The trial Judge ruled that the obtaining of the ANOM communications pursuant to, or purportedly pursuant to, relevant warrants, within the meaning of s 4 CA, did not occur in breach of the prohibition contained in s 7(1) TIAA (i.e. in obtaining the communications utilising the ANOM platform, the Australian Federal Police (**AFP**) did not intercept a communication passing over a telecommunications system).[4] The Court of Appeal (**CoA**) agreed with the trial Judge, answering the first question reserved accordingly.[5] In the result, s 77(1) TIAA was not engaged and the ANOM communications were admissible. The grounds of appeal challenge the CoA's conclusion that utilising the ANOM platform, the AFP did not intercept a communication passing over a telecommunications system contrary to the prohibition contained in s 7(1) TIAA.

6. Sections 5(1), (2) and (3) CA, respectively: deem information or a record obtained under, or purportedly under, a relevant warrant not to have been intercepted while passing over a telecommunications system and not to have been obtained by intercepting a communication passing over a telecommunication system; deem anything done or purported to have been done under a relevant warrant valid and lawful and to always have

[1] Whether consisting of text, photographs, videos, voice memos or note files as the case may be: *Questions of Law Reserved (Nos 1 and 2 of 2023)* [2024] SASCA 82 at [22] & [71] (**CoA Reasons**), Amended Core Appeal Book (**ACAB**) 70 & 79.

[2] Appellants' Written Submissions (**AWS**) [2].

[3] AWS [3].

[4] ACAB 47.

[5] CoA Reasons [240], ACAB 120.

been so; and, deem any evidence obtained under, or purportedly under a relevant warrant not to have been obtained, and always not to have been obtained, improperly or unlawfully.

7. The retroactive status attributed by ss 5(1)-(3) CA to information or a record obtained under, or purportedly under, a relevant warrant, to acts done pursuant to, or purportedly pursuant to such warrants, and to evidence obtained, respectively, has the legal and practical effect of rendering the judgment of the CoA otiose. Accordingly, the grounds of appeal no longer raise questions fit for a grant of special leave to appeal.

PART III: 78B NOTICE

8. The DPP agrees with the Appellants that no notice is required.

PART IV: FACTS

9. The evidence as to the operation of the ANOM platform is accurately summarised by the CoA at pages 11-23, [53]-[118] of the judgment.[6] The core facts are:

i. A mobile phone is a computer end system that connects to a network.[7] The functionality of a mobile phone is generally located on, and controlled through, a motherboard or mainboard. That functionality includes the device's processor, storage, and memory. The operation of these functions is determined through the transmission, from the software installed on the device to the motherboard, of digital signals comprising electrical signals or impulses representing instructions to perform specific tasks.[8]

ii. Operating systems and applications are both forms of software. The operating system manages the hardware of the end system,[9] while allowing additional functionality to be developed.[10]

iii. Applications are software programs that provide specific services to users of an end system or device.[11] They may be built on top of an operating system.[12]

[6] ACAB 76-88.

[7] CoA Reasons [61], ACAB 77.

[8] CoA Reasons [62], ACAB 77.

[9] E.g. it controls the power management of the device, what is written to, and stored in, the memory of the device, and how data is transmitted and received via the device's network interfaces: CoA Reasons [63], ACAB 77.

[10] CoA Reasons [63]-[64] & [100], ACAB 77-78 & 85.

[11] Which include mobile phones, computers and servers, all of which may be described as end systems where data comes to rest for a time before it is processed or retransmitted: ACAB 80.

[12] CoA Reasons [64] & [100], ACAB 78 & 85.

iv. The operating system enables application software to read data from the hardware of the device through specialised software, such as an application programming interface (**API**), which allows two software packages to speak to one another.[13]

v. The ANOM application was installed on Android Operating System (**AOS**) programmed devices (**the ANOM device**). The ANOM application had an API which allowed it to access the functionality of the AOS.[14]

vi. ANOM devices were connected to a telecommunications network using either a Wi-Fi or cellular data connection to the internet. In this way, they were connected to a server (an Extensible Messaging and Presence Protocol (**XMPP**) server) which facilitated the instant messaging functionality of the ANOM platform.[15] Messages or communications were able to be sent between users' devices through the transmission of packets of data, in the form of electromagnetic energy or waves, over the telecommunications system.[16]

vii. The ANOM application was disguised on the user's mobile device as a calculator application.[17] Upon launch, the ANOM application automatically connected to the XMPP server,[18] and was authenticated by a username and password. Once authenticated by the XMPP server, the application was available for use.[19]

viii. To send a message, User A would compose their message, address it to User B, and press the "send" button.[20] Upon User A pressing the icon to send the message to User B, an entirely separate copy of the message was made by the application.[21] After being encrypted, both the original message and the second message were then sent as separate packets of data to their different destinations[22] – the original message to User B, and the second message to the address "bot@anom.one" (**the bot user**). The existence of the bot user, and its presence in the contacts list of all ANOM applications, was not known to users of ANOM devices.[23]

[13] CoA Reasons [65], ACAB 78.

[14] CoA Reasons [66] & [101], ACAB 78 & 85.

[15] The XMPP server enabled asynchronous communication between users of the ANOM platform: CoA Reasons [67], ACAB 78.

[16] CoA Reasons [67], ACAB 78.

[17] CoA Reasons [68], ACAB 78.

[18] CoA Reasons [69], ACAB 78.

[19] CoA Reasons [70], ACAB 79.

[20] That is, the icon next to the field in which the message had been entered, also referred to as the "trigger." CoA Reasons [71], ACAB 79.

[21] The functionality of the ANOM application operated differently from the BCC functionality of emails. In the case of the ANOM application, two end-end encrypted messages were sent. Both messages were created and encrypted in the ANOM application on the sending device: CoA Reasons [87], ACAB 82.

[22] CoA Reasons [72], ACAB 79.

[23] CoA Reasons [74], ACAB 79.

10. With respect to the creation of a message using an ANOM device:

    i. The creation of the copy message occurred entirely within the ANOM application. To the extent that additional data was attached to the copy message, it was obtained from outside of the ANOM application via an API, taken back into the application, and then added to the second message – whilst it was within the application and before it left the application.[24]

    ii. In relation to a particular communication, the sequence of operations which followed the pressing of the send button included performance checks to determine whether the XMPP server was online, encryption of the communication, formatting the communication in accordance with the XMPP, and transferring the encrypted message to the AOS for transmission over the network to the XMPP server.[25]

    iii. The encryption of the communication involved steps, including, checks to determine the encryption protocol to be used, calls to the relevant code libraries to encrypt the message in the selected protocol, creation of the end-to-end encryption "envelope" through the exchange of public keys, and encryption of the message based on the public key of the recipient(s).[26]

11. In relation to the sending and transmission of a communication by the sending device:

    i. When the ANOM application sent a message to the XMPP server, it transited layers on the phone defined by an international standard known as the Open Systems Interconnection (**OSI**) model, before being transmitted across the network.[27] This was a function of the AOS. In this way, the AOS provided the "doorway to the telecommunications network."[28] The bottom "physical layer" is where a communication is transmitted from one piece of hardware to another.[29]

    ii. The "physical layer" of the OSI model is a technologically neutral description of the hardware responsible for the transmission and conveyance of data as electromagnetic energy across the network.[30] In the case of the ANOM device, this was by means of a Wi-Fi or cellular connection.[31]

[24] CoA Reasons [73] & [80], ACAB 79-80.
[25] CoA Reasons [75], ACAB 79.
[26] CoA Reasons [76], ACAB 80.
[27] CoA Reasons [82] & [102], ACAB 81 & 85.
[28] CoA Reasons [78], ACAB 80.
[29] CoA Reasons [102], ACAB 85.
[30] CoA Reasons [102] & [109], ACAB 85-86, RBFM 181-187 (Exhibit VDP12 pgs. 12-20).
[31] CoA Reasons [67], ACAB 78.

iii. Above the physical layer in the OSI model is the "data link layer." The functionality of this layer is to facilitate the reliable transmission of the packets of data and to correct for errors that may occur during transmission.[32]

iv. The layer above this is the "network layer." Network layer protocols route packets of data through an interconnected network. The most common protocol for this purpose is the Internet Protocol (**IP**) which was used by ANOM devices. This protocol adds to the packets of data a unique identifier for the intended receiving end system, in the form of an IP address.[33]

v. Above the network layer is the "transport layer." Transport layer protocols ensure reliable delivery and receipt of packets of data sent between end users. The most widely used transport layer protocol is the Transmission Control Protocol (**TCP**). A widely used security extension to TCP is Transport Layer Security (**TLS**).[34]

vi. A communications application (such as the ANOM application) operates within the "application layer" of the OSI model. A communications application may not engage all seven layers of the OSI model, however, it will utilise the application, transport, network, data link and physical layer.[35]

vii. The transmission of a communication involves two phases – a connection establishment phase and a data transfer phase.[36] The connection establishment phase commences at the application layer. This phase involves a "handshake" to establish a secure channel between two end systems (the ANOM device and the XMPP server) and authentication of the transmitter and receiver.[37] The data to establish the connection transits the layers, from the application layer to the physical layer of the device, and then through the network to the recipient.[38] The signal received travels back through the layers to the application layer, to signal that the connection has been made, before the data transfer phase can commence.[39] The type of encryption to be used in the data transfer phase is determined during the connection phase, before the data can be transferred.[40]

[32] CoA Reasons [103], ACAB 85.
[33] CoA Reasons [104], ACAB 85.
[34] CoA Reasons [105], ACAB 85.
[35] CoA Reasons [107], ACAB 86.
[36] CoA Reasons [102], ACAB 85.
[37] CoA Reasons [108], ACAB 86.
[38] CoA Reasons [108], ACAB 86.
[39] CoA Reasons [109], ACAB 86.
[40] CoA Reasons [113], ACAB 87.

viii. The transfer of data (constituting a message) is called the data transfer phase. An application accesses a code library which collates and encrypts the data representing the typed content of the message. The encrypted message then passes through a socket to the AOS. Control information is added to the data packets to route the data to the recipient's device as a function of transport layer protocol (namely, TLS).[41]

ix. TLS is used during both the connection phase and the data transfer phase.[42] Once a TLS connection is established, data, including the typed content of a message, is packaged into packets of data. The network layer protocol routes the data packets to the destination before the packets can reach the physical layer for transmission – by conversion of the packets of data into a signal sent over the telecommunications network to the XMPP server.[43]

x. In the case of the ANOM communications, the XMPP server then forwarded or re-transmitted the message to the intended recipient when they came online.[44] Once received by User B, or the bot user, the encrypted message was decrypted using the encryption key on the application in the receiving end device (the private key).[45]

xi. The messages created in the ANOM application remained in the temporary memory of the ANOM device while being packaged and encrypted, and before it was passed to AOS to then be sent from the device.[46]

xii. While the ANOM application required an internet connection to "work" (in the sense of sending a message to another user), it could nevertheless launch and run on the ANOM device without the device being connected to the internet.[47] If a message was "sent" in this state, it would not go anywhere until a connection was established.[48] When transmission was able to occur the process could be, by human perception, almost instantaneous.[49]

12. As to the receipt of the communication by the bot user:

i. The message to the bot user was sent, via the XMPP server, to a computer server having the bot user IP address (bot@anom.one) and which was operating software (**iBot**

[41] CoA Reasons [110], ACAB 86.
[42] TLS is a transport layer protocol within the AOS: CoA Reasons [105] & [113], ACAB 85-87.
[43] CoA Reasons [113], ACAB 87.
[44] CoA Reasons [77] & [91]-[95], ACAB 80 & 83-84.
[45] CoA Reasons [110]-[111], ACAB 86.
[46] CoA Reasons [84]-[85], ACAB 81.
[47] CoA Reasons [84]-[85], ACAB 81.
[48] CoA Reasons [84]-[85], ACAB 81.
[49] CoA Reasons [83], ACAB 81.

application) that enabled it to connect to the XMPP server as the bot user (**iBot server**).[50] The iBot application can be understood as the equivalent of a cut down version of the ANOM application.[51]

ii. The purpose of the iBot application was to connect to the XMPP server, as the bot user, and retrieve messages sent to the bot user and save them into a database on the iBot server.[52] The application was designed to maintain a connection with the XMPP server and to receive messages addressed to the bot user.[53]

iii. Upon receipt of an encrypted message, the iBot application would decrypt the message, check to see whether it required further content to be downloaded and, if so, download that content and save it to a database on the iBot server.[54] In later builds of the iBot application, a process of re-encrypting the content and saving it to a database was introduced.[55]

iv. The iBot server operated a piece of software called the iBot API. A core functionality of the iBot API was to query the iBot server's database containing the data (representing the messages to the bot user) in response to requests from software operating on an AFP computer server (**AFP retrieval server**), and to then make that data available for download by the AFP retrieval server via a web interface.[56]

PART V: FIRST RESPONDENT'S ARGUMENT

First ground: interception upon creation of the second message?[57]

13. Before communications intercepted while passing over a telecommunications system may be adduced in evidence in a criminal trial, the interception must be authorised by a warrant issued under s 46 TIAA. Absent a warrant, the interception contravenes the prohibition contained in s 7(1) TIAA. Contravention of s 7(1) does not enliven the public policy

[50] The iBot server being a computer server installed with the iBot application software which enabled it to receive messages sent to the bot user. To log in as the bot user a configuration file was required which included the IP address of the XMPP server, details about encryption including the private key, and a username and password. CoA Reasons [88]-[89] & [92], ACAB 82-83.

[51] CoA Reasons [91], ACAB 83.

[52] CoA Reasons [89], ACAB 82.

[53] CoA Reasons [92], ACAB 83.

[54] CoA Reasons [93], ACAB 83.

[55] CoA Reasons [93], ACAB 83.

[56] CoA Reasons [90], ACAB 83; the iBot servers were the servers in Sydney with fixed IP addresses 35.189.36.241 and 35.201.29.116 over which relevant warrants issued to the AFP pursuant to ss 16 and 27C of the SDA were in force.

[57] AWS [15]-[33]; ACAB 165, Ground 2 (2.1 and 2.2).

discretion,[58] rather, s 77(1) TIAA provides that the intercepted communications are inadmissible.

14. The DPP contends that the CoA and Kimber J were right to conclude that the ANOM application did not intercept communications passing over a telecommunications system within the meaning of s 7(1) TIAA. Accordingly, Part 2-6 of the TIAA is not engaged and the communications are admissible.

When is a communication passing over a telecommunications system?

15. Section 7(1) TIAA prohibits the interception of a communication passing over a telecommunications system. The prohibition is confined to that period during which a communication is passing over a telecommunication system. Interception of a communication that has not yet commenced its passage over a telecommunications system, or has ceased in its passage,[59] is not prohibited by s 7(1). Section 6(1) TIAA provides that the interception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication "in its passage over that telecommunications system" without the knowledge of the person making the communication, but it does not assist in determining when a communication commences and ceases such passage. That task is performed by s 5F TIAA, which on its face establishes bookends between which the relevant passage occurs. Section 5F provides:

> For the purposes of this Act, a communication:
>
> (a) is taken to start passing over a telecommunications system when it is sent or transmitted by the person sending the communication; and
>
> (b) is taken to continue to pass over the system until it becomes accessible to the intended recipient of the communication.

16. Resolution of the first ground of appeal centres upon the meaning of the words "sent or transmitted" as contained in s 5F(a) TIAA. The DPP contends that the CoA correctly held that a communication is "sent or transmitted" by the person sending the communication when it is dispatched in the form of electromagnetic energy from the sending (transmitting) device.[60] The ordinary meaning of "send" and "transmit" supports the CoA's focus on the *movement* of electromagnetic energy over a system for carrying such signals.[61]

[58] *Bunning v Cross* (1978) 141 CLR 54; s 138 *Evidence Act 1995* (Cth).

[59] E.g. *Voxson Pty Ltd v Telstra Corporation Limited (No 10)* [2018] FCA 376. This decision involved similar technology to the present case, where encrypted communications received by one or more proxy servers were held to have been received by the intended recipient; see also *R v Giaccio* (1997) 68 SASR 484 at 491; *Edelsten v Investigating Committee of New South Wales* (1986) 7 NSWLR 222 at 228-9 (Lee J).

[60] CoA Reasons [200], ACAB 109.

[61] CoA Reasons [182]-[183], ACAB 105.

17. That construction is consistent with, and supported by, the textual indicators within s 5F and the concept of an "intercept" of a communication "passing over a telecommunications system" to which the prohibition applies. These indicators are, in turn, further supported by the definitions of "telecommunications system," "telecommunications network" and "telecommunications device" – each directing attention to the conveyance, in real-time, of signals over telecommunications infrastructure in the form of electromagnetic energy.[62]

18. That construction accords, and gives effect to, the purpose of s 5F, which emphasises the distinction between communications "passing over" a telecommunications system and "stored" communications.[63] In so doing, s 5F accords with the broader purpose of protecting national telecommunications infrastructure from unlawful interference, and in turn, the integrity of the telecommunications system established by the *Telecommunications Act 1997* (Cth) (**TA**).[64]

19. The evidence of the functionality of the ANOM application, and the mobile phone devices on which it was installed, established that the second message sent (by User A) to the bot user was created in the ANOM application on User A's mobile phone. Several sequential and functionally distinct processes occurred in order to effect transmission as electromagnetic energy.[65] The evidence was that the ANOM communications existed as digital information within the memory of the User A's mobile phone device *before* being converted into electromagnetic energy at the physical layer of that device.[66]

20. Therefore, the message sent by User A to the bot user did not involve an interception of the message sent by User A to User B in contravention of s 7(1) of the TIAA – because the information constituting the message had not, at the time of the creation of the message to the bot user, taken the form of electromagnetic energy (that is, it remained in the application layer). It follows that it had not been "sent or transmitted" for the purposes of s 5F(a) TIAA and was not recorded in its passage over the telecommunications system.

The text of s 5F – "sent or transmitted"

21. The text and context in which "sent" and "transmitted" appear in the TIAA are indicative of meaning more than the action of a person pressing a button on a mobile device. The

[62] CoA Reasons [180]-[184], [189], ACAB 104-107.

[63] CoA Reasons [151] & [215], ACAB 96 & 114.

[64] *R v Metcalfe* (2018) 338 FLR 357 at [11]-[14] (Blokland J); *R v Migliorini* (1981) 38 ALR 356 at 360 (Cosgrove J); *In the Marriage of Parker and Williams* (1993) 117 FLR 1 at 10 (Butler J).

[65] RBFM 242-249, 303-305 (T902-909, T963-965 (Khatri)), 342-344 (Exhibit VDP16 at [92]-[103]), 392-394 & 418-419 (T1081-1083, T1107-1108 (Jenkins)).

[66] CoA Reasons [67], [196]-[197], ACAB 78, 108-109.

language of “is taken” in s 5F is used to define, confirm, or clarify, how the legislature intended that the phrase “passing over”[67] should be understood, by describing the point at which the passage commences and ceases in ss 5F(a) and (b). [68]

22. When a communication *is taken* to commence its passage over a telecommunications system depends upon what is meant by the composite expression, “when it is sent or transmitted by the person sending the communication.” More particularly, when does the person sending the communication send or transmit the communication?

23. While “sent” and “transmitted” are not synonymous, they carry similar connotations. Neither “sent” or “transmitted” is defined in the TIAA, however, their appearance together connected through a conjunctive “or” suggests that their respective meanings inform each other, impute substantial overlap and, further, are two means of describing the same concept.[69] The Macquarie Dictionary defines “send” to mean “to cause to go; direct or order to go; to cause to be conveyed or transmitted to a destination” and defines “transmit” to include “to send over or along, as to a recipient or destination; forward, dispatch, or convey,” in the context of physics “to cause (light, heat, sound, etc.) to pass through a medium,” and in the context of radio “to emit (electromagnetic waves).”[70] Each word, in the context of s 5F(a) and the section as a whole suggests a focus upon the movement or transport of the communication over the telecommunications system.

24. It is significant that both “sent” and “transmitted” appear as past participles. They identify a point in a process – the point at which a communication is to be taken to have commenced its passage across the underlying telecommunications system. Both the words themselves, and their tense, contemplate that preparatory or preceding actions, such as the sequential execution of computer code prior to transmission, are not captured by the prohibition but rather it contemplates a completed process – actual dispatch of the communication from the sending device and actual conveyance over a telecommunications system. In this way, the protection is linked to the definition of a “telecommunications system” and, in turn, the definition of a “telecommunications network.” Such an interpretation sits comfortably with the ordinary meaning of “transmitted” and with the concept of a communication passing, or being carried, over a telecommunications system in the form of electromagnetic energy.

[67] The concept of “passing over” is defined in s 5(1) TIAA as “includes being carried” – “carry” is defined as “includes transmit, switch and receive”.

[68] CoA Reasons [186]-[187], ACAB 105-106.

[69] CoA Reasons [189], ACAB 106.

[70] *Macquarie Dictionary* (7th ed; online as at 14 April 2025).

25. The phrase "sent or transmitted" appears as part of a composite phrase – "sent or transmitted by the person sending the communication." Much is made by the Appellants of the reference to "by the person sending"[71] – the Appellants submit the inclusion of that phrase is intended to draw attention to the act of a human being in authorising the sending of a message. Those words do not serve that purpose. The composite phrase must be understood in the light of the fact that the provision is attempting to identify, with some specificity, when a communication is taken to start passing over a telecommunications system – as distinct from emphasising an action authorising the sending or transmission by a human being.

26. So understood, the composite phrase necessarily contemplates the use by the person of a telecommunications device to access and engage a telecommunications system (and network). That is, the communication is taken to be sent or transmitted, by the person, when it is sent or transmitted by the "telecommunications device" (as defined in s 5(1)[72]) over a network comprised of a system or series of systems for carrying communications by means of guided or unguided electromagnetic energy (or both). In this sense, the utility of the words "by the person sending" is only to identify the sender in the context of the sentence as a whole – which identifies the commencement of the telecommunications passage by reference to the moment a communication is "sent or transmitted by the person sending the communication."

Contextual considerations

27. Section 5F(a) is directed to when a communication commences "passing over" a telecommunications system. As mentioned, the terms "passing over," "being carried" and "carry" are consistent with the transport or movement of a communication over the telecommunications system in the form of electromagnetic energy. It is significant that a telecommunications system is defined in s 5(1) TIAA by reference to a telecommunications network, which is, in turn, described as a system for carrying communications in the form of guided or unguided electromagnetic energy.

28. These definitions focus upon the movement or actual conveyance of communications over the telecommunications system in the form of electromagnetic energy – as distinct from any processing which might occur within the mobile phone devices (being terminal devices), and while the communication is in a form other than electromagnetic energy –

[71] AWS [30].

[72] Being a terminal device that is capable of being used for transmitting or receiving a communication over a telecommunications system.

such as digital (binary) data represented in one of two electrical states within a computer's memory.[73]

29. Further, the proper construction of s 5F(b) informs the construction of s 5F(a). Section 5F(b) must be read in the light of s 5H. Section 5H provides that a communication is accessible to the intended recipient if has been "received by the intended recipient," is "under the control of the intended recipient", or has been "delivered to" the "telecommunications service" provided to the intended recipient. That is, access is satisfied by a technical event.[74] To construe "sent or transmitted" in s 5F(a), as the DPP contends, by reference to a technical event gives ss 5F(a) and (b) a coherent operation. This view accords with ss 5F-5G of the TIAA, and coheres with both the Act as a whole – including the concept of "stored communications"[75] and the evidence adduced about modern communications systems[76] – because it necessarily contemplates that the communication has been received by an "end system,"[77] and is therefore "at rest."[78]

30. The construction of s 5F(a) TIAA advanced by the Appellants urges an asynchronous construction of ss 5F(a) and (b). It does so by seeking to tie s 5F(a) to a non-technical event (pressing send) whilst s 5F(b) is tied, by virtue of s 5G, to a technical event (receipt by an end system). It is most unlikely that this was intended by the legislature, given the intended purpose of s 5F of confirming and clarifying the concept of "passing over a telecommunications system" as evinced from the Explanatory Memorandum (**EM**) and Supplementary Explanatory Memorandum (**SEM**) to the *Telecommunications (Interception) Amendment Bill 2006* (**the Amending Act**).[79]

31. The construction preferred by the CoA sees those two provisions operating harmoniously by reference to technical events, and having a reciprocal operation at the respective ends of the telecommunications passage in a manner consistent with their plain and apparent meaning.[80] As the CoA held, it is plain that s 5F(b) may be satisfied by a technical event rather than any human action and that "peculiar asymmetry" results if a non-technical event were to satisfy s 5F(a).[81] When a different meaning is assigned to s 5F(a) than s 5F(b), an

[73] RBFM 185-186 (VDP12 at [67]-[68]).
[74] CoA Reasons [209], ACAB 112.
[75] As defined in TIAA s 5(1), CoA Reasons [122]-[123], ACAB 89.
[76] CoA Reasons [96]-[118], ACAB 84-88, RBFM 171-187 (VDP12 at [16]-[70]).
[77] RBFM 16 & 175-177 (T703 (Prof. Seneviratne),VDP12 at [27]-[38]).
[78] Appellant's book of further materials (**ABFM**) 59 (Blunn Report at 1.5.5(c)).
[79] EM (p 6), SEM (p 3); enacted as the *Telecommunications (Interception) Amendment Act 2006* (Cth).
[80] *Project Blue Sky Inc v Australian Broadcasting Authority* (1998) 194 CLR 355 at [70]-[71] (McHugh, Gummow, Kirby and Hayne JJ).
[81] CoA Reasons [209], ACAB 112.

incongruent outcome results that does not contemplate simultaneous receipt and transmission of information over a telecommunications system.[82]

32. Further, nothing in the secondary material to the Amending Act (which introduced ss 5F-5G) is consistent with the Parliament intending to expand the prohibition on the interception of communications beyond the *conveyance* of the communication over telecommunications infrastructure. Nor is the extrinsic material consistent with Parliament intending to regulate processes occurring within the transmitting device *prior* to the communication being dispatched or transmitted in the form of electromagnetic energy.

33. The secondary material is consistent with the contrary proposition – that the legislature intended to dispel ambiguity by "giv[ing] express recognition to the fact that a communication is not in its passage over the telecommunications system (and therefore subject to the telecommunications interception regime) until it is sent or transmitted."[83] The Parliament therefore intended to clarify that the communication was not in its passage "until it has been sent or transmitted by the sender"[84] – thus identifying the moment the communication commenced being carried in the form of electromagnetic energy over a system for carrying such energy.

34. The Appellants' construction conflicts with the secondary material and evident purpose of the TIAA.[85] Section 5F was introduced to bring certainty to the concept of "passing over" and sought to do so by tying the commencement to a technical event of actual dispatch and conveyance of a communication, not a non-technical event which may not result in sending or transmission. This was contemplated by Parliament in addressing "concerns raised about draft emails and sent items."[86] This is the same apparent scenario grappled with by the CoA arising from situations where pressing send in relation to text-based communications does not in fact result in a communication being sent or transmitted[87] – that is, does not result in the communication departing the sending device.

35. The focus upon the conveyance of communications over the telecommunications system as electromagnetic energy is also consistent with the legislative distinction drawn in the TIAA between the interception of communications passing over the telecommunications

[82] Such as the making of a phone call.
[83] SEM (p 3).
[84] SEM (p 3).
[85] E.g. AWS [27].
[86] EM (p 6), SEM (p 3).
[87] CoA Reasons [86], [152], [204], ACAB 43, 81, 96 and 111.

system ("real-time"[88] communications), and access to communications which are stored on the equipment of a carrier (stored or "at rest"[89] communications). The intention to regulate stored communications separately makes it plain that copying or recording these communications does not involve the interception of communications passing over the telecommunications system – despite the communications being located on equipment that would, by virtue of the definition of telecommunications device and equipment, come within the definition of a "telecommunications system."

36. The dichotomy between real-time access to communications data and access to stored communications data underlies the Amending Act, as borne out by the *Report of the Review of the Regulation of Access to Communications* (**Blunn Report**).[90] It is apparent that the drafters had in mind this distinction, as opposed to any distinction said to exist between the terms "sent" and "transmitted" in s 5F(a) TIAA – both of which connote carriage across telecommunications infrastructure and are directed towards real-time access to communications data.

37. The Appellants emphasise the Blunn Report in advancing the submission that the TIAA is intended to be "technologically neutral."[91] It is argued that the DPP seeks to negate Parliament's intention by recourse to technical evidence focussing on the means of effecting actual sending or transmission of a communication. However, the construction urged by the DPP – which advances the proposition that electromagnetic energy is the thing "passing over" to which the prohibition applies – is consistent with the technologically neutral framing of the TIAA. If it is accepted that the communication in the form of electromagnetic energy is the thing "passing over" a telecommunications system with which the TIAA is concerned, then the policy of technological neutrality is achieved – the conveyance of electromagnetic energy will be the common denominator across all electronic communications technology. It is thus unsurprising that the TIAA has proved to be resilient in the face of changing technology when its provisions concentrate on the conveyance of electromagnetic energy.

38. Further, determining what is "passing over" is also informed by the manner in which an interception is authorised by Chapter 2 TIAA. The TIAA provides for two kinds of warrants for intercepting communications passing over a telecommunications system –

[88] ABFM 56 (Blunn Report at 1.4).

[89] ABFM 56 (Blunn Report at 1.5.5(c)).

[90] E.g. ABFM 56 (Blunn Report at 1.4.1), *Telecommunications (Interception) Amendment Bill 2006* Second Reading Speech, House of Representatives, 16 February 2006, (p 7) (Philip Ruddock MP).

[91] AWS [21].

"telecommunications service warrants" (ss 9, 11A, 46 and 48) and "named person warrants" (ss 9A, 11B and 46A) – together defined in s 5(1) as "interception warrants." A "telecommunications service" is defined in turn to mean "a service for carrying communications by means of guided or unguided electromagnetic energy or both, being a service the use of which enables communications to be carried over a telecommunications system operated by a carrier […]."

39. The interception warrant regime provisions provide further contextual support for the DPP's construction of "sent or transmitted," insofar as the provisions are premised on the notion that an intercept involves the access of communications being conveyed, as electromagnetic energy by a telecommunications service, over a carrier-operated telecommunications system.[92]

The legislative purpose

40. That the TIAA does not protect the privacy of communications once they have been delivered and received is clear. The TIAA only regulates communications that are passing over a telecommunications system when in the form of guided or unguided electromagnetic energy[93] – all other communications are left to other lawful modes of access.[94]

41. The purpose of ss 5F-5G, 6(1) and 7(1) TIAA is not to establish a blanket protection of the privacy of communications between users of the telecommunications system. The purpose is narrower. It is to protect the integrity of the telecommunications system, and hence the privacy of communications in their passage over this system, rather than the integrity of users' devices, or the privacy of their communications, more broadly.[95] This is also to recognise that the TIAA is part of a suite of State and Federal legislation governing access to digital information and the use of surveillance devices.[96]

[92] E.g. by stipulating that an application for an interception warrant must identify the telecommunications service (or, in the case of a named person warrant, information to assist carriers to identify devices or services used by the person) (s 42 TIAA); by stipulating that upon a warrant being issued police are to notify the carrier and provide the carrier with a copy of the warrant (s 60 TIAA); and by deeming that interception warrants do not authorise the interception of communications passing over a telecommunications system that a carrier operates unless notice is given and interception takes place as a result of action taken by an employee of the carrier (s 47 TIAA).

[93] Or that do not meet the definition of a "stored communication": CoA Reasons [123], ACAB 89.

[94] *Telecommunications (Interception) Amendment Bill 2006* Second Reading Speech, House of Representatives, 16 February 2006, (p 7) (Philip Ruddock MP).

[95] *Edelsten v Investigating Committee of New South Wales* (1986) 7 NSWLR 222 at 228-9 (Lee J); See also *Telephonic Communications (Interception) Bill 1960* Second Reading Speech, House of Representatives, 5 May 1960, (p 1422) (Sir Garfield Barwick MP).

[96] E.g. the scheme for the cross-border recognition of warrants relating to surveillance devices: *Surveillance Devices Act 2016* (SA) s 3, *Crimes (Surveillance Devices) Act 2010* (ACT) s 31, *Surveillance Devices Act 2007*

42. The protection provided by the TIAA represents a balancing of users' interests in privacy of their communications, as they transit regulated national infrastructure, against the public interest in access to communications and data for national security and law enforcement purposes. Therefore, the protection of individual privacy is an aspect of the legislature's broader statutory objective of the regulation of carriers, carriage service providers, and the unlawful interference with the telecommunications system.[97]

43. Further, the Appellants' third contention that one of the "core features" of the TIAA is its "avowed" purpose of applying *to applications* on all telecommunications devices, irrespective of the functionality,[98] is contrary to the context and purpose, and the history, of the prohibition – it being first enacted as the *Telephonic Communications (Interception) Act 1960* (Cth) before the development of modern smartphones and software applications.

44. The Appellants' fourth contention similarly overstates the protection of privacy at the point of pressing "send" as the predominant purpose of the TIAA. Had that been Parliament's intention, it might be expected that the draftsperson express that intention clearly. Moreover, if that were the intention, it would be unnecessary to confine the protection to the passage of a communication over a system. Rather, the manner in which Parliament has expressed the protection is consistent with a higher statutory intention, of which privacy is an aspect, of the maintenance of the integrity of national infrastructure.[99]

Application of the legislation in the present case

45. Applying the evidence about the operation of the ANOM platform to the legislative text, activating the send icon on the ANOM application triggered a series of sequential steps, namely:[100]

   a. Before encryption occurred:

      i. a copy of the original communication was made by the ANOM application;

      ii. the data representing the original message and second message remained within

(NSW) s 37, *Surveillance Devices Act 2007* (NT) s 49, *Police Powers and Responsibilities Act 2000* (Qld) s 265, *Police Powers (Surveillance Devices) Act 2006* (Tas) s 30, *Surveillance Devices Act 1999* (Vic) s 30B; see also *Crimes Act*, Part IAA, Division 2 relating to access to electronic equipment.

[97] *R v Metcalfe* (2018) 338 FLR 357 at [12] (Blokland J). This decision involved similar technology to the present case, where the "real-time" recording of a telephone call by a software application within the mobile phone device of one party to the call was not an interception because, in order for the software to engage with the communication, it had necessarily passed over a telecommunications system.

[98] AWS [25].

[99] *R v Metcalfe* (2018) 338 FLR 357 at [11]-[14] (Blokland J); *R v Giaccio* (1997) 68 SASR 484 at 491 (Cox J, Millhouse and Perry JJ agreeing).

[100] RBFM 241-248 (T901-908 (Khatri)), 342-344 (Exhibit VDP16 at [92]-[103]), 392-394 (T1081-1083 (Jenkins)), 38 (T725 (Prof. Seneviratne)).

temporary memory on the device, whilst the data representing the original message was being processed by the ANOM application;[101]

b. After encryption occurred:

   i. the message was passed to the AOS in order to effect transmission,[102] engaging the processes undertaken by the AOS as a function of the protocols referrable to the layers of the OSI model;[103] and

   ii. only at the physical layer did the data, constituting the encrypted message, undergo conversion into electromagnetic energy before being despatched from the device through a Wi-Fi or cellular data connection to the internet and to its ultimate destination.[104]

46. Accordingly, the creation of the message to the bot user occurred prior to transmission of the first message – because of the execution of conceptually and functionally distinct and sequential steps – before being despatched at the physical layer of the sending device as electromagnetic energy.

47. The CoA's judgment did not "disaggregate," in a physical sense, the telecommunications device into layers. Rather, the evidence of the OSI model was used, properly with respect, in considering when, in the process of sending a communication, the communication took the form of electromagnetic energy and commenced passing over a telecommunications system.

48. The importance of the distinction between the ANOM application and AOS – including the phone hardware – is not a physical distinction. Rather, it is a *functional* distinction. A physical distinction *does* exist between the sending mobile phone (the ANOM device) and the equipment operated by "carriers" (as defined in s 5(1) TIAA),[105] requiring transmission across a physical medium as electromagnetic energy. A boundary, necessitated by the concept of being "sent or transmitted," exists at the physical layer of the transmitting device where digital data is converted to electromagnetic energy for transmission across that

[101] RBFM 449 (T1148 (Jenkins)), 242-243 (T902-903 (Khatri)), 342-344 (Exhibit VDP16 at [92]-[103]).

[102] RBFM 449 (T1148 (Jenkins)).

[103] RBFM 22-23 & 166-167 (T709-710, T1030-1031 (Prof. Seneviratne)).

[104] RBFM 156 (T1020 (Prof. Seneviratne)).

[105] Defined for the purposes of Part 1-2 TIAA as a "carrier" or a "carriage service provider" within the meaning of the TA. Section 7(1) TA provides "carrier means the holder of a carrier licence." A "carrier licence" means a licence granted under s 56 TA. A "carriage service provider" is defined by s 87 TA as informed by cascading definitions found in Part 2 TA, RBFM 79-83 & 157-158 (T768-772, T1021-1022 (Prof. Seneviratne)).

system.[106]

49. The critical finding of the CoA was that the relevant act of copying the communication occurred prior to moving from the physical layer of the device and being converted into electromagnetic energy for transmission toward its destination.[107] Given the construction preferred in relation to s 5F, this finding was decisive. The evidence is only consistent with the conclusion that the message to the bot user was created within the sending device prior to the message being encrypted, specifically by execution of the ANOM application's code, and thus prior to being converted into electromagnetic energy and being transmitted over a telecommunications system.[108]

50. The correctness of this construction is illustrated by the logical consequence of the Appellants' argument – that there would be an interception even if the message was never sent to its intended recipient. As outlined at [30] above, the Appellants' construction introduces an unintended asynchronous operation of s 5F, by tying s 5F(a) to a non-technical event (pressing send) whilst s 5F(b) is tied, by virtue of s 5G, to a technical event. As illustrated by the "draft email" scenario, the Appellants' construction introduces uncertainty which the legislature specifically sought to dispel.[109]

Second ground: interception by the iBot application receiving the second message?[110]

51. The Appellants' argument, which contends that s 5F(a) TIAA *was* engaged in the transmission of the communication to the bot user, advances a submission that s 5F(b) *was not* engaged, because the bot user was not the "intended recipient" of the person sending the communication. On the Appellants' construction of "intended recipient," the communication never ceases its passage over a telecommunications system – despite the communication coming to rest on an end system to which the communication was addressed by the sender's telecommunications device.

52. The construction advanced by the Appellants frustrates the concept of "passing over" that Parliament intended to regulate. It ignores the functionality of telecommunications devices borne out by the evidence in this case. It ignores s 5G, which defines the intended recipient. And it has the result of a communication that has become accessible to the recipient to

[106] RBFM 166-167 (T1030-1031 (Prof. Seneviratne)), *R v Giaccio* (1997) 68 SASR 484 at 491 (Cox J, Millhouse and Perry JJ agreeing).

[107] CoA Reasons [200], ACAB 109-110.

[108] E.g. RBFM 27-29, 86-87, 124, 156-158, 161-164, 166-167 (T714-716, 775-776, 815, 1020-1022, 1025-1028, & 1030-1031 (Prof. Seneviratne)), 171-172, 174, 180-182 (Exhibit VDP12 at [17]-[18], [25], [46]-[50]), 393-394 & 445 (T1082-1083, T1144 (Jenkins)).

[109] SEM (p 3).

[110] AWS [34]-[38], ACAB 165, Ground 3.

which it was addressed never ceasing to be in its passage.

53. Sections 5F and 5G contemplate that the "intended recipient" will be the address to which the communication is directed at the time it is sent or transmitted and not, as the Appellants contend, the subjective intention of the sender. The evidence established that the second message was addressed by the sending device to the bot user (bot@anom.one), as distinct from being diverted or copied to that user after the communication commenced its passage.[111] The exchange of encryption keys between the sender and the bot user was such that only the bot user could decrypt the second message.[112] Decryption occurred when the communication became accessible to the iBot server within the meaning of s 5H.

54. Consistent with the findings of the trial Judge at first instance, the CoA correctly held that, applying the definition in s 5G, the intended recipient was the bot user to which the second messages were addressed, or at least the operator of the iBot server – with the result that anything done with respect to the second message from the moment it arrived at the iBot server was not an interception in breach of s 7(1) TIAA.

55. For the reasons given, should the grant of special leave not be rescinded, the appeal should be dismissed.

PART VI: NOTICE OF CONTENTION

56. The DPP adopts the submissions of the Second Respondent.

PART VII: TIME ESTIMATE

57. The DPP estimates that 1.5 hours will be required for presentation of its oral argument.

Dated: 17 April 2025

M G Hinton KC
(08) 7322 7055
dpp@sa.gov.au

A F Cairney
(08) 7322 7055
amelia.cairney@sa.gov.au

W M Scobie
(08) 7322 7055
william.scobie@sa.gov.au

P L Schaefer
(08) 7322 7055
patrick.schaefer@sa.gov.au

[111] RBFM 241-248 (T901-908 (Khatri)), 342-344 (Exhibit VDP16 at [92]-[103]), 392-394 (T1081-1083 (Jenkins)), 38 (T725 (Prof. Seneviratne).

[112] E.g. RBFM 239-240, 243, 267-268, 293 (T899-900, 903, 927-928, 953 (Khatri)), 408-409 (T1097-1098 (Jenkins)), 132 (T823 (Prof. Seneviratne)), 187-188 (Exhibit VDP12 at [71]-[74]), 356 (Exhibit VDP16 at [186]).

ANNEXURE TO RESPONDENT'S SUBMISSIONS

No	Description	Version	Provision(s)	Reason for providing this version	Applicable date or dates
1	*Surveillance Legislation (Confirmation of Application) Act 2024* (Cth)	As made No. 130 of 2024	4, 5, 6, 7	The Act as passed. No amendments have been made.	N/A
2	*Telecommunications (Interception and Access) Act 1979* (Cth)	Compilation No. 106	5, 5F, 5G, 5H, 6, 7, 63 & 77	The versions of the Act at the time of communications sought to be led at the trial of the Appellants. The relevant provisions remained unchanged.	17 October 2019 – – 7 June 2021 (the period during which the Appellants are alleged to have used ANOM).
3		Compilation No. 107			
4		Compilation No. 108			
5		Compilation No. 109			
6	*Telecommunications Act 1997* (Cth)	Compilation No. 93	7, 56, 87, Part 2	The versions of the Act at the start and end of the period during which communications sought to be led at the trial of the Appellants were sent. The definition of "carrier" and "carriage service provider" remained unchanged throughout.	
7		Compilation No. 99			
8	*Acts Interpretation Act 1901* (Cth)	Compilation No. 38	2B, 2C, 15AA & 15AB	The version of the Act at the time of filing these submissions.	N/A
9	*Telecommunications (Interception) Amendment Act 2006* (Cth)	As made No. 40 of 2006	Schedule 1, Part 1	This was the version of the Amendment Act that inserted ss 5F-5G into the	N/A

				Telecommunications (Interception and Access) Act 1979 (Cth)	
10	*Telephonic Communications (Interception) Act 1960* (Cth)	As made No. 27 of 1960	4 & 5	This Act introduced the prohibition against intercepting communications passing over a telephone system (the equivalent of s 6 and 7 of the *Telecommunications (Interception and Access) Act 1979* (Cth))	N/A