HIGH COURT OF AUSTRALIA

NOTICE OF FILING

This document was filed electronically in the High Court of Australia on 08 Jan 2025 and has been accepted for filing under the *High Court Rules 2004*. Details of filing and important additional information are provided below.

Details of Filing

File Number:	A24/2024
File Title:	CD & Anor v. Director of Public Prosecutions (SA) & Anor
Registry:	Adelaide
Document filed:	Form 27A - Appellants' submissions
Filing party:	Respondents
Date filed:	08 Jan 2025

Important Information

This Notice has been inserted as the cover page of the document which has been accepted for filing electronically. 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 and whenever the document is reproduced for use by the Court.

IN THE HIGH COURT OF AUSTRALIA
ADELAIDE REGISTRY

BETWEEN:

CD
First Appellant

TB
Second Appellant

and

DIRECTOR OF PUBLIC PROSECUTIONS (SA)
First Respondent

ATTORNEY-GENERAL OF THE COMMONWEALTH OF AUSTRALIA
Second Respondent

APPELLANTS' SUBMISSIONS

Part I: FORM OF SUBMISSIONS

1. These submissions are in a form suitable for publication on the internet.

Part II: ISSUES PRESENTED BY THE APPEAL

2. The primary issue presented by this appeal is determining when a "communication" in the form of a text message is "passing over"[1] the "telecommunications system"[2] for the purposes of the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIAA**).

3. That primary issue raises for consideration the proper construction of the deeming provision in s 5F of the TIAA which is directed to identifying the statutory window of time in which a communication is taken to start passing over a telecommunications system and when it is taken to end, the latter being determined by reference to when the message is available to the "intended recipient". A subsidiary issue arising is the

---

1 *Telecommunications (Interception and Access) Act 1979* (Cth) (hereafter **TIAA**), s 5F(a).
2 TIAA, s 5(1).

proper construction of the statutory term "intended recipient", which forms part of the deeming provision in s 5F(b) and is defined in s 5G of that Act.

4. The appellant contends that the South Australian Court of Appeal (**CA**) erred in its determination on those issues. That is, the appellants contend that the CA erred in determining that the communications in issue in this case, which were obtained covertly by the Australian Federal Police (**AFP**), were not obtained as a result of an unlawful interception under the TIAA.

Part III: SECTION 78B NOTICE

5. The appellants have considered whether notice should be given under section 78B of the *Judiciary Act 1903* (Cth) and consider that, at present,[3] no such notice is required. However, that position may need to be revisited in light of the potential application of the Confirmation Act.

Part IV: REPORT OF DECISIONS BELOW

6. The judgment of Kimber J is reported as *R v TB & Anor* (2023) 376 FLR 69 and its medium neutral citation is [2023] SASC 45.

7. The judgment of the Court of Appeal has not been reported. Its medium neutral citation is *Questions of Law Reserved (Numbers 1 and 2 of 2023)* [2024] SACA 82.

Part V: FACTS

8. The issues on appeal arise in the context of an AFP investigation named "Operation Ironside", the largest operation ever conducted by the AFP (together with overseas law enforcement authorities and later state police). The AFP received approximately 28 million messages sent by users of mobile phones between about October 2018 and June 2021.[4] The communications were sent via the use of an application on mobile phones known as "AN0M". The AFP facilitated the development of the AN0M application and organised for phones enabled with the AN0M application to be

---

3 The appellants note that on 10 December 2024 (thus, following the grant of special leave), the *Surveillance Legislation (Confirmation of Application) Act 2024* (Cth) received Royal Assent. At the time of writing, it is not clear whether the respondents intend to invoke that Act in this appeal, being an appeal in the strict sense.

4 Court of Appeal Reasons (CA Reasons) at [16]: **Amended Core Appeal Book** (**ACAB**) 70.

distributed[5] as part of Operation Ironside. The Operation was authorised under Part IAB of the *Crimes Act 1914* (Cth).

9. There is no real dispute as to how the AN0M platform operated[6], at least insofar as the computer programming experts were concerned[7], and most of the pertinent evidence was agreed or not disputed.[8] The Court of Appeal conveniently summarised the functionality of AN0M platform as follows:

> [21] By way of overview, the AN0M platform operated so that, unbeknown to the users of the AN0M application, and without their consent, communications sent from AN0M-enabled devices were copied and sent to the servers able to be accessed by the AFP.
>
> [22] More particularly, the AN0M application installed on the AN0M-enabled devices operated so that when a user (**User A**) composed a message (or attached a photo or voice memo) in the AN0M application, and pressed the 'send' icon, or activated the 'trigger', for the message to be transmitted to the recipient user (**User B**), a separate second message was created in the AN0M application. The second message included a copy of the message from User A to User B, as well as some additional data retrieved from User A's device for law enforcement purposes.
>
> [23] Both messages were then encrypted and sent as separate messages over the telecommunications system via a server using the Extensible Messaging and Presence Protocol (**XMPP**). As User A intended, the first message would be sent, via an XMPP server, to User B. However, without the knowledge of Users A or B, the second message (a copy of the first message with the additional data) would be sent, via an XMPP server, to a server with the username 'bot@anom.one' (**the iBot server**).
>
> [24] The messages received by the iBot server were then re-transmitted to the servers in Sydney that were able to be accessed by the AFP. The AFP obtained these messages using retrieval software, pursuant to the surveillance device warrants and computer access warrants mentioned earlier.

---

5 CA Reasons at [14]-[17]: ACAB 69-70.
6 CA Reasons at [59]: ACAB 77.
7 CA Reasons at [72]-[73] and [80]-[81]: ACAB 79 and 80-81 for the findings based on the evidence of Mr Khatri and Mr Jenkins.
8 It was an agreed fact between the parties that from October 2018, the AFP had the capacity to review communications addressed to the bot user, bot@anom.one, in real time. See also T641:5-11, T641:29 (Mansfield): **Appellants' Further Materials (AFM)** 10 Seneviratne Report (VDP12) at [79]: AFM 23; T1109:21-26 (Jenkins): AFM 16; T1504:8-11: AFM 18, T506:32-34 (Gaughan): AFM 19.

10. At first instance, Kimber J held that the AN0M application, or more precisely, the processes that took place in accordance with the manner in which the application was programmed to function, did not involve an unlawful interception under the TIAA. One basis upon which Kimber J reached that conclusion was that the mobile phones, and the AN0M application installed on them, were not part of the "telecommunications system".[9] That finding did not survive in the Court of Appeal. Relevantly, the Court of Appeal found that both the application and the mobile phones or telecommunications devices did form part of the telecommunications system.[10] This accorded with the appellants' contention in both courts. This issue now forms the subject of the second respondent's notice of contention in this Court.

11. The AFP never sought or obtained a warrant under the Act. This was a "considered decision" by the AFP.[11]

12. Following the "resolution" phase of Operation Ironside, more than 450 people were arrested with multiple corresponding prosecutions currently pending in the committal and trial courts across multiple States in Australia. This includes the appellants, who are currently detained on remand having been charged with a number of serious offences.

13. Relevantly, count 1 of the Information alleges the appellants participated in a "criminal organisation" as defined in s 83D(1) of the *Criminal Law Consolidation Act 1935* (SA) (**CLCA**). The offence charged is a breach of s 83E(1) by conduct, namely, storing and controlling access to a utility vehicle containing unlawful firearms. The DPP seeks to prove that count by recourse to the AN0M data (in the form of text messages), which messages South Australia Police received from the AFP, and seeks to have the AN0M data admitted for that purpose. Counts 2 to 4 and 8 to 14 are all offences alleging possession of prohibited items (either a firearm – s 9(1), or a sound moderator or parts of a firearm – s 39(1)) under the *Firearms Act 2015* (SA)). The DPP also seeks to prove those counts by reference to the same AN0M data but will also adduce other

---

9 *R v TB & Anor* [2023] SASC 45 at [101]-[102]: ACAB 40-41.
10 CA Reasons at [178]: ACAB 104.
11 CA Reasons at [139]: ACAB 93. See the evidence of Detective Superintendent Mansfield (DS Mansfield), to the effect that a deliberate decision was made not to apply for a warrant because it was assumed the Act did not apply, a matter which was of some surprise to the Inspector General of Intelligence and Security, the late Hon. Margaret Stone AO: at T552-553: AFM 6-7; T556:26-29: AFM 8 and T570:16-19. AFM 9.

evidence following the execution of a warrant on a property owned by another person (i.e. not the appellants) by South Australia Police where the vehicle was located and searched, and in which the firearms were discovered. However, regardless of this additional evidence, it is common ground that absent the AN0M data, there would be no, or no sufficient, evidence to connect the appellants to the offences charged.

14. If the questions of law reserved are answered contrary to the Court of Appeal's answers, the covert messages obtained via AN0M are inadmissible under the TIAA.[12] The statutory prohibition in ss 63 and 77(1) of the TIAA preclude the application of any *Bunning v Cross* discretion.[13]

Part VI: ARGUMENT

GROUND 1: THE TEXT MESSAGES WERE INTERCEPTED

15. Properly construed, the terms of s 5F make clear that the copy messages sent to a server where they were obtained by the AFP were copies made within the statutory window of time established by s 5F, read with s 5G.

16. The point in time at which a communication starts passing over a telecommunications system is determined by s 5F(a) of the Act, a deeming provision[14] which makes clear that a communication "is *taken to start* passing over a telecommunications system when it is sent or transmitted *by the person* sending the communication".[15] The appellants contend that the user is only required to press "send" (or an equivalent "trigger") on the relevant application installed on the device to start the statutory process of the communication to be taken to have commenced "passing over" the telecommunications system. That construction does not depend on, or require the provision to have, an operation beyond that required to achieve its object. Quite the contrary, the appellants submit that that construction is entirely congruent with the

---

12 Sections 63 and 77(1) of the TIAA.

13 Sections 63 and 77(1) of the TIAA. See also *Bunning v Cross* (1978) 141 CLR 54 at [78] (Stephen and Aickin JJ) referring to *R v Ireland* (1970) 126 LR 321 at 335 (Barwick CJ).

14 *Coates v Commissioner for Railways* (1961) 78 WN (NSW) 377; *Wellington Capital Ltd v Australian Securities and Investments Commission* (2014) 254 CLR 288 at [51] Gageler J; *Queensland v Congoo* (2015) (2015) 256 CLR 239 at [165] (Gageler J); *Ellison v Sandini Pty Ltd* [2018] FCAFC 44 at [209]-[210] (Siopis, Logan and Jagot JJ); *Phonographic Performance Company of Australia Ltd v Federation of Australian Commercial Television Stations* [1998] HCA 39; (1998) 195 CLR 158 at [44].

15 Emphasis added.

statutory purpose evident in the text of the provision, namely, to render certain the period in which a communication is to be to be taken to be passing over a telecommunications system. The provision is meant to render certainty in the context of a statutory regime that is meant to be technologically neutral.[16] That is, the provision aims to avoid immaterially technological debates over functional aspects of telecommunications devices.

17. However, contrary to the appellants' contention, the Court of Appeal held that the communications were not copied in their passage over that system (and thus not unlawfully intercepted) notwithstanding that the mobile phone and AN0M application formed part of the telecommunications system.[17] While the Court of Appeal determined that after pressing "send" the message commenced "moving" over the system,[18] and the text message was indeed copied in the course of that movement,[19] it nevertheless held that the message did not commence "passing over" the telecommunications system until some later point in the process.

18. In particular, the Court of Appeal found that there were "preparatory steps"[20] some of which consisted of "movement" of the message or communication from and throughout the AN0M application and the different components of the mobile phone, and through parts of the telecommunications system. Nevertheless, the Court found that this "movement" was not "passing over" for the purposes of the TIAA. Rather, the Court of Appeal held that the relevant act of "passing over" commenced later,[21] when the message or communication data was converted into electromagnetic energy and was dispatched for transmission over the internet. As a result, the Court held that the copy was not made whilst in its "passage" over the system but, instead, before it commenced its "passage".[22]

19. The Court's conclusion is, with respect, erroneous. To conclude as it did was necessarily to engage in an exercise of compartmentalization of various technological

---

16 Blunn Report (A. Blunn AO, *Report of the Review of the Regulation of Access to Communications* (August 2015) page 14 at [1.1.5]. AFM 44.
17 CA Reasons at [178], [202]: ACAB 104, 110.
18 CA Reasons at [193]: ACAB 107.
19 CA Reasons at [210]: ACAB 112.
20 CA Reasons at [180]: ACAB 104; [191]-[200]: ACAB 107-110, esp [195].
21 Probably within a period of time so short that it is difficult for the human brain to comprehend. See: CA Reasons at [202]: ACAB 110.
22 CA Reasons at [197]-[201]: ACAB 109-110.

and functional operations and processes inconsistent with the text, context and evident purpose of s 5F read with ss 6(1) and 7(1) of the TIAA.

20. The Court of Appeal's reasoning necessarily implies that, notwithstanding that the user had done all they could do to send or transmit the message (the user having composed the message and pressed "send"), there was no interception of the message because it had not reached a specific *part* of the telecommunications system. That conclusion cannot sit within the terms of ss 5F and 5G and the defined terms critical to the operation of the scheme as a whole, such as "telecommunications system" and telecommunications device".

10 21. The terms of the TIAA, including ss 5G and 5F, are meant to give rise to a "technologically neutral"[23] application of the Act. That is to say, the TIAA is meant to apply to communications which pass over a telecommunications system facilitated by telecommunications devices, irrespective of the manner in which specific "applications" placed on mobile phones are programmed to operate, or indeed irrespective of the functionality or design of specific mobile phones. And yet it is that very objective that the respondents seek to negate by recourse to an argument that necessarily depends upon specific functionality of an application placed on an AN0M-enabled phone.

22. In accepting the respondents' overly compartmentalized approach to the critical issue
20 before the Court, the Court of Appeal erred. The errors are manifest in a number of interrelated ways.

23. *First*, the Court relied upon the purported separation of "layers" within the AN0M application and thereby the telecommunications system, to artificially divide the system into disparate parts,[24] such that a lawful interception could theoretically occur in some parts (e.g., in the "application layer")[25] but not in others (e.g., the "physical layer", the point at which the application interfaced with the mobile phone hardware)[26] despite the Court having found earlier in its reasons that the AN0M application did in

---

23 Blunn Report (A. Blunn AO, *Report of the Review of the Regulation of Access to Communications* (August 2015) page 14 at [1.1.5]. AFM 44.
24 See, e.g., CA Reasons at [199]: ACAB 109; see also [193]: ACAB 107 and [214]: ACAB 114.
25 CA Reasons at [196]: ACAB 108.
26 CA Reasons at [197]: ACAB 109.

fact form part of the telecommunications system.[27] If the AN0M application formed part of the telecommunications system (as found, correctly with respect, by the Court of Appeal), then the conclusion that the very same system could be understood as being composed of separate layers within which messages could be covertly copied and re-directed is incongruous and at odds with the terms of s 5F.

24. *Second*, it follows that the effect of the Court's finding is that the "telecommunications network" became the starting point for determining when a communication is "passing over" the network (that being when the communication is converted into electromagnetic energy), whereas the prohibition in the TIAA,[28] and the terms of s 5F(a), are broader and include the "telecommunications system" as a whole.

25. *Third,* the Court thereby erroneously narrowed the statutory window of when a communication is taken to be "passing over", one defined by reference to an unidentified moment of time when the communications data was converted to electromagnetic energy, rather than the statutory window prescribed by s 5F. In effect, the Court has side-stepped the very point of s 5F. That is, the Court avoided the clear effect of the statutorily prescribed window of time within which interceptions are deemed to occur by engaging in a deconstruction of the AN0M application that sought to separate its operation from the coverage of that aspect of the TIAA. Not only is that approach inconsistent with its finding that the AN0M application was part of the "telecommunications device" and thus part of the "telecommunication system", but it undermines one of the core features of the TIAA, namely, its avowed purpose of applying to applications on all telecommunications devices irrespective of the functionality of applications installed on those devices.

26. *Fourth,* the prohibition in ss 6 and 7 of the Act apply to a "communication", which is defined in s 5(1) in broad and extensive terms capturing data, text, visual images, signals "or in any other form or combination of forms". So understood, the text, data, and signals, which comprise a text message in the AN0M application, are an inseparable part of the application on the telecommunications device and which are operating on the telecommunications system. It follows that the Court ought to have

---

27 CA Reasons at [178]: ACAB 104.
28 Section 6(1) of the Act.

found, consistently with its observation at [178] of the Reasons, that the AN0M application formed part of, and was inseparable from, the telecommunications device and thus formed part of the telecommunications system. However, inconsistently with its finding at [178], the Court disaggregated the process into what were said to be sequential steps between pressing "send", the making of the covert copy of the message, the "movement" of the data, and the transmission of the data.[29] That reasoning introduced non-statutory "preparatory steps" into a statutory scheme (with an all-encompassing definition of "communication") utilising a deeming provision (s 5F(a)) that textually and contextually points decisively against recourse to such reasoning. As the text of s 5F(a) makes plain, the time in which a communication is deemed to start passing over a telecommunication system is at the point the user presses "send". That also serves one of the evident purposes underlying the scheme as a whole, which is to protect the privacy of communications from the point at which the user presses "send" until the message becomes accessible to the intended recipient.

27. *Fifth,* to the extent that that evidence concerning the operation of the AN0M application was to be brought to bear on the exercise of construction, the Court's conclusion negates the evidence that the pressing of "send" set in train a process that was inevitable, irreversible and beyond the user's control.[30] That evidence is inconsistent with the manner in which the Court disaggregated and compartmentalized the process into the various "preparatory" steps as if those steps had some independent (or independently definable) statutory consequence. They did not. The pressing of "send" – the statutory moment captured by s 5F(a) – is the point at which Parliament determined that a message is to be "taken" to commence its passage over the telecommunication system. On the evidence, it is only once that step was taken that the text message was copied and had additional data attached to it. So understood, the text message was copied in its passage over the "telecommunications system" and was thereby intercepted for the purposes of ss 6 and 7(1) of the Act.

28. Because both the AN0M application and the mobile device were part of the telecommunications system,[31] and the evidence being that the copying process only

---

29 CA Reasons at [192]-[196] and [200]: ACAB 107-108 and 109.
30 CA Reasons at [83]: ACAB 81; Khatri: T918: 27-38: AFM 12; Jenkins T1090: 14. It was also effectively instantaneous: Jenkins T1090: 32-T1091: 2 AFM 14-15.
31 CA Reasons at [178]: ACAB 104.

occurred *after* the user activated the send function,[32] s 5F(a) was engaged. That is, s 5F(a) requires no more than a user activating the send function of the application (i.e., by the person pressing send). That event was the start of the statutorily prescribed time identifying when a communication is "passing over" the telecommunications system. The relevant interception occurred, therefore, from the moment the user pressed "send" because it occurred within the period identified by s 5F, not outside that period. All of the steps that occurred in accordance with the manner the AN0M application was programmed necessarily took place within the period identified by s 5F and therefore were steps taken as the "communication" passed over the telecommunications system. Consequently, any act of copying or recording after that statutory moment is an unmistakable breach of ss 7(1)(b) and (c) as read with ss 5G, 5F and 5(1).

29. The appellants' primary contention is that s 5F establishes the statutory window of time defined by its commencement point (s 5F(a)) and its end point (s 5F(b)). The purpose of doing so is to remove any ambiguity which could be said to exist about the identification of those two statutory points of time.[33] The same deeming provisions facilitate one of the important purposes underlying the TIAA, namely, to protect the privacy of communications and the integrity of the telecommunications system. The Court must be taken to have rejected these propositions, notwithstanding the clear words in s 5F itself.[34]

30. The Court failed to construe s 5F(a) in accordance with well-known principles of statutory construction[35] and, in particular, failed to give the words in the Act their ordinary and natural meaning. In particular, it failed correctly to address that s 5F(a) provides the "start" of the process activated "by the person *sending*" the communication. The purpose of s 5F(a), manifest by the text, is to require the identification of the start of the statutory point in time which commences with an event created by a user of a device, namely, pressing "send". The Court of Appeal's

---

32 CA Reasons at [22]: ACAB 70; CA Reasons at [72]: ACAB 79, CA Reasons at [80]: ACAB 80.

33 *Coates v Commissioner for Railways* (1961) 78 WN (NSW) 377; *Wellington Capital Ltd v Australia Securities Investments Commission* (2014) 254 CLR 288 at [51] (Gageler J); *Queensland v Congoo* (2015) 256 CLR at [165] (Gageler J); *Ellison v Sandini Pty Ltd* [2018] FCAFC 44 at [209]-[210] (Siopis, Logan and Jagot JJ).

34 *Collector of Customs v Agfa-Gevaert Ltd* (1996) 186 CLR 389; [1996] HCA 36.

35 *SZTAL v Minister for Immigration and Border Protection* (2017) 262 CLR 362 at [14]; [2017] HCA 34. See also CA Reasons at [141]-[142].

reasoning negates the underlying significance of the concept of a person *sending*[36] the communication. That is to say, it is the act of *sending* which commences the process that *is* taken to start that is identified in s 5F(a).

31. Rather than construe the terms of s 5F(a) in their ordinary and natural sense, the Court construed the terms "sent or transmitted"[37] by reference to broader contextual considerations such as the notion of communications being "carried" as a relevant descriptor for the transport of communications by means of electromagnetic energy.[38] While recourse to contextual considerations is by no means erroneous, here the Court erroneously focused upon "the movement or transport of communications while they are in the form of electromagnetic energy"[39] to define the starting point for "passing over". That reasoning inverts the proper analysis. The proper analysis begins with the terms of s 5F(a) which controls when a communication is to be taken to be passing over a telecommunications system. That was not the approach of the Court of Appeal. Instead, the Court of Appeal focused upon disparate moments of "movement", which led the Court to exclude the so-called "preparatory steps"[40] from the "telecommunications system" and the operation of s 5F(a). There is no statutory support for that approach, indeed, it is inconsistent with the text of the scheme.

32. The Court further erred when applying the evidence to s 5F(a) in that it construed the words in s 5F(a) as if they read "had been" or "have been" sent or transmitted in their past tense.[41] Those additional words cast in the past tense do not appear in the Act. Indeed, recourse to the past tense is not warranted by the terms of s 5F(a).

33. The appellants further submit that the Court's finding that "*the data representing the message remained within the control of User A, or at least the application and other software on User A's device, up to at least the point where it was in the physical layer and converted into electromagnetic energy for transmission towards its destination*"[42]

---

36 On the meaning of "send" or "sending" see *Pinkstone v The Queen* (2004) 219 CLR 444 at [51]-[52]; [2004] HCA 23.
37 CA Reasons at [188]: ACAB 106.
38 CA Reasons at [184]: ACAB 105.
39 CA Reasons at [181]: ACAB 104; [CA Reasons at 182]: ACAB 105; CA Reasons at [184]: ACAB 105; CA Reasons at [185]: ACAB 105; CA Reasons at [189]-[192]: ACAB 106-107, CA Reasons at [197]-[198]: ACAB 109 and [208]: ACAB 112.
40 CA Reasons at [192]-[193] and [195]-[196]: ACAB 107 and 108.
41 CA Reasons at [193], [195] and [197]-[200]: ACAB 107-108 and 109.
42 CA Reasons at [212]: ACAB 113.

is not supported by the evidence. On the contrary, the preponderance of the evidence on this issue was directly contrary to this conclusion.[43] That is, the pressing of "send" set in train an inexorable process that was beyond the control of the user. There was no "control" left for User A to exert over the process after User A pressed "send". That being so, the Court of Appeal's finding that control remained with User A cannot stand.

GROUND 2: THE AFP'S "IBOT" IS NOT THE INTENDED RECIPIENT

34. Ground 2 concerns the proper construction of "intended recipient" in s 5G of the Act, which is critical to identifying the point at which a communication has *ceased* its passage over a telecommunications system for the purposes of s 5F(b).

35. Relevantly, the appellants submit that the Court erred in finding that the "iBot" (a computer or server programmed to receive the communication that had been covertly copied) was the "intended recipient" within the meaning of s 5G of the Act. The Court made that finding notwithstanding that the user of the device did not know that a copy of their communication was being secretly made, addressed, and sent to the "iBot".[44] It is to be recalled that the entire point behind the AN0M-enabled phones was for the AFP to receive the text messages sent between users without their knowledge. The fact that it was a covert operation depended on the absence of such knowledge by the intended users of the AN0M-enabled phones.

36. The appellants submit that the Court failed to give the words "intended" and "addressed" or "by the person" any, or any sufficient, work to do.

37. Self-evidently, the communication was not "addressed" to the "iBot" "by the person sending the communication", within the meaning of s 5G read with s 5F(a). The covert communication (i.e. the copy message) was not "addressed" by the person making or sending the communication at all. The word "addressed" (in this context used as a verb) must be read with the requirement that it be done "by the person sending the communication" as contemplated by s 5F(a). Put differently, there is no "person" within the meaning of s 5F(a) who addressed the covert communication to the "iBot". Selecting (or typing) an address on a mobile phone necessarily involves knowledge on

---

43 CA Reasons at [83]: ACAB 81; T918: 27-38 (Khatri): AFM 12; T1090: 15-28 (Jenkins): AFM 14. It was also effectively instantaneous: T1090: 32- T1091: 2 (Jenkins): AFM: 14-15.

44 CA Reasons at [237]-[239]: ACAB 119-120.

the part of the person entering the address of the intended recipient (irrespective of whether that address is entered correctly).[45]

38. So understood, the appellants submit that a user must enter the address of the intended recipient and make that communication intentionally and with knowledge in order for the addressee to be an "intended recipient". The deception deployed by AN0M application which covertly copied the message and sent that message to the "iBot" (as programmed) stands in stark contrast to a person knowingly entering an address to an intended recipient of a communication.[46]

CONCLUSION

39. The Court of Appeal's construction of the TIAA, which led it to answer the questions of law reserved in the manner in which it did was erroneous for the reasons identified above. The appellants therefore seek the orders sought below.[47]

40. Notice of Contention: The appellants will respond to the notice of contention filed and served by the Commonwealth Attorney-General following service of the Commonwealth Attorney-General's submissions.

Part VII: ORDERS SOUGHT

41. That the appeal be allowed.

42. That the answers to the first and second questions of law reserved given by the Court of Appeal on 27 June 2024 be set aside and that those questions be answered as follows:

    a. As to question 1, Yes.

    b. As to question 2, Yes.

---

45 *cf.* CA Reasons at [235]: ACAB 119.
46 See the contextual considerations in s 6(1) ("knowledge of the person making the communication") and in s 5F(a).
47 *Judiciary Act 1903* (Cth), s 35A(b).

Part VIII: ESTIMATED TIME

43. The appellants estimate that 2 hours will be required to present oral argument (including reply).

Dated 8 January 2025

Bret Walker

10 T: (02) 8257 2500

E: caroline.davoren@stjames.net.au

Damian O'Leary

(08) 8205 2966

doleary@barchambers.com.au

ANNEXURE TO APPELLANT'S SUBMISSIONS

No	Description	Provisions	Version	Reason for providing this version	Applicable date or dates (to what event(s), if any, does this version apply
1	*Telecommunications (Interception and Access) Act 1979* (Cth)	s 5, 5F, 5G, 5H, 6, 7, 63, 77(1)	Compilation No. 108 Compilation date: 13 December 2019 Includes amendments up to: Act No. 124, 2019 Registered: 13 January 2020	This is the Act as it stood at the time of the alleged offences as charged in the Information.	20 January 2020 (being the date of the charges in the Information)
2	*Telecommunications (Interception and Access) Act 1979* (Cth)	s 5, 5F, 5G, 5H, 6, 7, 63, 77(1)	Compilation No. 126 Compilation date: 22 May 2024 Includes amendments: Act No. 24, 2024 Registered: 29 May 2024	This is the Act as it stood at the time of the judgment of the Court of Appeal. The provisions relied upon are in identical form.	27 June 2024 (being the date of the Court of Appeal judgment)
3	*Surveillance Legislation (Confirmation of Application) Act 2024* (Cth)	3, 4, 5, 6, 7, 8	10 December 2024	This is the current and only version, no amendment having been made since the passage of the Act.	10 December 2024 (being the date of the receipt of Royal Assent)
4	*Criminal Law Consolidation Act 1935* (SA)	83D, 83E	As at 20 January 2020	This is a current version but all relevant provisions are the same	20 January 2020 (being the date of the charges in the Information)
5	*Firearms Act 2015* (SA)	ss 9, 29, 31, 32, 39,	As at 20 January 2020	This is a current version and all relevant provisions are the same	20 January 2020 (being the date of the charges in the Information)