Neutral Citation Number: [2024] EWCA Civ 1095

Case Nos: CA-2023-001940, CA-2023-001941,
CA-2023-001944, CA-2023-001946,
CA-2023-001953

IN THE COURT OF APPEAL (CIVIL DIVISION)
ON APPEAL FROM THE INVESTIGATORY POWERS TRIBUNAL
EDIS LJ, LADY CARMICHAEL, STEVEN SHAW KC
[2023] UKIP Trib 3

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 20/09/2024

Before :

LORD JUSTICE HOLROYDE
LORD JUSTICE DINGEMANS
and
LADY JUSTICE ELISABETH LAING

- -

Between :

(1) Connor Palmer and Anor **(2) Kulvir Singh Shergill** **(3) Usman Butt** **(4) Nasar Ahmed** **(5) ABC and Others**	**Appellants**
- and -	
National Crime Agency	**Respondent**

- -
- -

Matthew Ryder KC and **Daniel Cashman** (instructed by **Bindmans LLP**) for the **First Appellant**
Thomas Schofield (instructed by **Novate Direct Legal**) for the **Second Appellant**
Simon Csoka KC and **Oliver Cook** (instructed by **Eldwick Law**) for the **Third & Fourth Appellants**
Abbas Lakha KC and **Aneurin Brewer** (instructed by A**visons Solicitor**s) for the **Fifth Appellant**
David Perry KC, Richard O'Brien KC, Victoria Ailes and **Andrew Deakin** (instructed by **NCA Legal**) for the **Respondent**

Hearing date : 16 July 2024

- -

Approved Judgment

This judgment was handed down remotely at 14.00 hrs on 20.9.24 by circulation to the parties or their representatives by e-mail and by release to the National Archives.

.....

Lord Justice Holroyde, Lord Justice Dingemans and Lady Justice Elisabeth Laing:

Introduction

1. This is our judgment after an oral hearing of applications for permission to appeal from a decision of the Investigatory Powers Tribunal ('the IPT') in 11 linked proposed appeals. The National Crime Agency ('the NCA') is the respondent to the proposed appeals. The decision of the IPT concerned the application of the regime in the Investigatory Powers Act 2016 ('the IPA') to Operation Venetic. Operation Venetic was the NCA's response to EncroChat devices, which were telephone handsets which could be used to get access to EncroChat, an encrypted service which was either wholly, or very nearly wholly, used by criminals for criminal purposes. Users were given a randomly generated user name which did not identify them so that particular devices could not be attributed to a specific user. The NCA was not, therefore, able to attribute all EncroChat usernames to specific criminal targets, although it could identify some. It was estimated that there were about 9000 users in the United Kingdom.

2. The 'appellants' are applicants for permission to appeal, but for convenience we will refer to them in this judgment as 'appellants'. The First Appellant was represented by Matthew Ryder KC and Daniel Cashman, the Second Appellant by Thomas Schofield, the Third and Fourth Appellants by Simon Csoka KC and Oliver Cook, and the Fifth Appellant by Abbas Lakha KC and Aneurin Brewer. David Perry KC, Richard O'Brien KC, Victoria Ailes and Andrew Deakin represented the Respondent. All appellants relied on the same six grounds of appeal.

3. Section 67A(1) of the Regulation of Investigatory Powers Act 2000 ('RIPA') gives a right of appeal on a point of law from certain determinations of the IPT to this court. The leave of the IPT or of this court is required (section 67A(6)(b)). The IPT and this court must not give leave unless it considers that the appeal would 'raise an important point of principle or practice or there is another compelling reason for giving leave' (section 67A(7)).

4. At the start of the hearing, counsel were asked whether there should be any anonymity orders in this court. Counsel's general position, we were told, was that they did not have positive submissions to make about anonymity orders. That general position was subject to a potential exception in the case of the appellants represented by Mr Lakha KC. He was unable, however, to make detailed submissions about this at the hearing. We consider that, since no positive argument about prejudice was advanced in relation to the other appellants, they should not be the subject of anonymity orders. We invite further written submissions on this point from Mr Lakha, if he has any to make, in response to the circulation of this judgment in draft. Following the circulation of the draft judgment an application for the continued anonymisation of three applicants was made, and we have made an order preserving their anonymity until the conclusion of their Crown Court proceedings.

5. For the reasons given in this judgment, we have decided to refuse permission to appeal.

The facts

6. EncroChat was an encrypted communications platform. A joint investigative team of French and Dutch law enforcement agencies ('the JIT') intercepted communications sent by EncroChat. The National Crime Agency ('the NCA') learned that the French authorities could intercept EncroChat messages. The NCA wanted to see those communications. A Judicial Commissioner approved a targeted equipment interference warrant ('TEI 1') under Part 5 of the IPA. The Crown Prosecution Service ('the CPS') served a European Investigation Order ('EIO') on the French authorities asking for the product of the interceptions of EncroChat. The NCA sought the revocation of TEI 1 because the explanations it gave were not full enough. A second Judicial Commissioner then approved a second targeted equipment interference warrant ('TEI 2'). The proceedings in the IPT concerned TEI 2.

7. The IPT heard evidence from three current or former officers of the NCA: Wayne Jones, Luke Shrimpton and Emma Sweeting. It summarised their evidence about communications between the French authorities and the NCA in paragraphs 27-64. It carefully analysed that evidence, testing it by reference to the claimants' submissions that the NCA had not been candid with the Judicial Commissioner about their ignorance of the method of interception and that had the NCA been candid with the Judicial Commissioner, it would have been obvious that a bulk interception warrant was necessary. The IPT acknowledged that the NCA had a preference for the material to be admissible in criminal proceedings but that they had not closed their minds before a critical Europol meeting. The IPT accepted the 'core' of Ms Sweeting's account. She did not ask for formal confirmation because she knew she would not get it. That was not because she feared that the NCA would get an answer it did not want, but because she genuinely thought that the French authorities were reluctant to tell the NCA about the methods they intended to use to intercept the EncroChat messages. The relevant French official, Mr Decou, had confirmed the method as described in the application for the TEI warrant (paragraph 74).

8. The conduct described in TEI 2 involved two stages, which reflected Ms Sweeting's understanding of the way in which the implant worked. The first stage was 'Historical Data Collection'. The 'implant' would collect data stored on a device and transmit it to the French authorities. It would stay in the device for stage two, 'Forward Facing Collection', in which communications stored on the devices would be collected throughout stage two. They would only be collected once they were stored on the device. That meant, in the NCA's view, that this interception could be authorised by a TEI. The IPT held that the purpose of the warrant was to make the conduct of the JIT lawful, when it otherwise might have been an offence under the Computer Misuse Act 1990, which the NCA would commit as a secondary party by encouraging it. This enabled the NCA to ask the JIT for the material, which the JIT was going to acquire in any event. The Judicial Commissioner was not being asked to authorise anything apart from that.

9. As the IPT observed, the necessity and proportionality of getting the data were shown 'to a high degree' by the application for TEI 2. Even if, therefore, the Judicial Commissioner had had doubts about the method used for getting the data, he would 'inevitably' have granted the warrant. Any doubts about the later admissibility of the material 'would be for the criminal courts to resolve in due course'.

10. The Crown relied on the material gleaned from EncroChat in a number of prosecutions which led to trials. Several defendants in those trials challenged the admissibility of that material, on grounds which included an argument that the material had been intercepted in the course of transmission and was inadmissible under section 56 of the IPA. Those proceedings led to two decisions of the Criminal Division of this court ('the CACD'), including *R v A, B, D and C* [2021] EWCA (Crim) 128, reported as *R v A and others* [2021] QB 791 (*'A'*). As Mr Ryder reminded us, an issue which could not be challenged in the criminal trials was whether or not the warrant was lawful. The starting point for the trials and for any appeals from them was that the warrant was lawful. All attempts in criminal trials to exclude EncroChat material have so far failed. If the appellants' proposed appeals succeed and if the TEI is quashed, it seems likely that there will be applications in the Crown Court under section 59 of the Criminal Justice and Procedure Act 2001. For the purposes of these applications for permission to appeal, and in order to shorten this judgment, we, like the IPT, have assumed that we are not bound by the decision or reasoning in *A*. It is, nevertheless, strongly persuasive on the relevant issues of statutory construction.

The legal framework

The Regulation of Investigatory Powers Act 2000

11. Section 65 RIPA creates the IPT's jurisdiction. The IPT's jurisdiction includes any proceedings not falling within section 65(2)(a)-(c) and which fall within section 65(3) as may be allocated to it by the Secretary of State by order (section 56(2)(d)). Those proceedings include 'proceedings relating to the taking place in any challengeable circumstances' of any conduct in section 65(5). Conduct takes place in challengeable circumstances if it takes place under, or required, an authorisation (or consideration of whether an authorisation should be sought) of the types listed in section 65(8) (section 65(7)). The authorisations listed in section 65(8) include warrants under Part 5 of the IPA.

The Investigatory Powers Act 2016

12. Section 1(1) of the IPA declares that it 'sets out the extent which certain investigatory powers may be used to interfere with privacy'. Part 1 'imposes certain duties in relation to privacy and contains other protections for privacy' (section 1(2)). Section 2 enacts various 'general duties in relation to privacy'. Part 1 is headed 'General Privacy Protections'. Part 2 is headed 'Lawful interception of communications'. Chapter 1 of Part 2 provides for 'Interception and Examination with a Warrant', Chapter 2 for 'Other forms of lawful interception' and Chapter 3 for 'Restrictions on use of disclosure of material obtained under warrants etc'. Part 5 is headed 'Equipment Interference' and Part 6 'Bulk Warrants'. Subject to immaterial exceptions, the IPA extends to England and Wales, Scotland and Northern Ireland (section 272(4)).

13. Sections 3-10 are headed 'Prohibitions against unlawful interception'. The interception of communications in the United Kingdom is a criminal offence unless a person has lawful authority to do it (section 3(1) of the IPA). Section 3(3) introduces sections 4 and 5, which, respectively, make provision about the meaning of 'interception' and when interception is 'regarded as carried out in the United Kingdom'. Section 3(4) introduces section 6 which contains provisions about when a person has lawful authority to carry out an interception. Section 3 is bolstered by section 7, which gives the Investigatory

Powers Commissioner ('the Commissioner') power to serve a monetary penalty notice, if, among other things, a person has intercepted, in the United Kingdom, any communication in the course of its transmission by a public telecommunications system, without lawful authority, and without making any attempt to act in accordance with an interception warrant, but has not, in the opinion of the Commissioner, committed an offence under section 3(1) (section 7(3)). Section 8(1) imposes civil liability for certain interceptions carried out in the United Kingdom.

14. Section 4 defines 'interception'. It is divided into two groups of subsections. The first concerns 'Interception in relation to telecommunications systems' (section 4(1)-(6)). The second concerns 'Interception carried out in the United Kingdom' (section 4(8)). Section 4(1) makes clear that the definition of interception applies for 'the purposes of this Act', and that it is an exhaustive definition. A person intercepts a communication in the course of its transmission by means of a telecommunications system if that person does a 'relevant act' in relation to the system, the effect of which is to make any content of the communication available to a person who is not the sender or its intended recipient. 'Content' is defined in section 261(6).

15. A 'relevant act' in relation to a telecommunications system means modifying, or interfering with the system or its operation, monitoring transmissions made by means of the system, and monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system (section 4(2)). 'Modifying a telecommunications system' includes to attaching any apparatus to, or otherwise modifying or interfering with any part of the system, or any wireless telegraphy apparatus used for making transmissions to or from apparatus that is part of system (section 4(3)). 'The relevant time', in relation to a communication transmitted by a telecommunications system means any time while the communication is being transmitted, and any time when the communication is stored in or by the system (whether before or after its transmission) (section 4(4)). If the content of a communication is diverted or recorded at the relevant time, so as to be available to a person after the relevant time, it is to be treated as having been made available to that person at the relevant time (section 4(5)).

16. 'Wireless telegraphy' and 'wireless telegraphy apparatus' have the same meanings as in sections 116 and 117 of the Wireless Telegraphy Act 2006. So far as relevant, 'wireless telegraphy' means the emitting or receiving, over paths that are not provided by any material substance constructed or arranged for that purpose, electromagnetic energy of a frequency no greater than 3000 gigahertz which 'serves for conveying messages, sound or visual images (whether or not those are received by anyone) or for operating or controlling machinery or apparatus'. 'Wireless telegraphy apparatus' means apparatus for the emitting or receiving, over paths that are not provided by any material substance constructed or arranged for the purpose, of the energy described in the second sentence of this paragraph.

17. For the purposes of the IPA, the interception of a communication is carried out in the United Kingdom 'if and only if', among other things, the relevant act is carried out by conduct 'within the United Kingdom' (section 4(8)).

18. The parties agreed in the IPT that the acquisition of the EncroChat data was an 'interception' as defined in section 4 of the IPA.

19. Section 6 defines 'lawful authority'. Section 6(1) defines three situations in which a person has lawful authority for an interception (in section 6(1)(a), (b) and (c)). The first such situation is if the interception is done in accordance with a targeted interception warrant ('a TI') or a mutual assistance warrant ('an MA') under Chapter 1 of Part 2, or a bulk interception warrant under Chapter 1 of Part 6 (section 6(1)(a)). The third such situation includes, in the case of information stored in or by a telecommunications system, that the interception is done in accordance with a TEI under Part 5 or an MA, or a bulk equipment interference warrant under Chapter 1 of Part 6 (section 6(1)(c)(i)), or the interception is done in the exercise of a statutory power that is exercised for the purpose of obtaining information (section 6(1)(c)(ii)). If conduct is lawful under section 6(1)(a) or under section 6(1(b)), it is 'to be treated as lawful for all other purposes' (section 6(2)). There is no equivalent provision in relation to section 6(1)(c).

20. Section 9 is headed 'Restriction on requesting interception by overseas authorities'. It applies to a 'request for any authorities of a country …outside the United Kingdom to carry out the interception of communications sent by or intended for, an individual who the person making the request believes will be in the British Islands at the time of the interception' (section 9(1)). By subsection (2), a request to which section 9 applies may not be made by or on behalf of a person in the United Kingdom unless (a) a TI has been issued under Chapter 1 of Part 2 authorising the person to whom it is addressed to secure the interception of the communications sent by, or intended for, that individual, or (b) a targeted examination warrant has been issued authorising the selection of the contents of such communications for examination.

21. Section 10 is headed 'Restriction on requesting assistance under mutual assistance agreements etc'. At the relevant time it applied to requests 'for assistance in accordance with an EU mutual assistance instrument' and 'an international mutual assistance agreement so far as the assistance is in connection with, or in the form of, the interception of communications' (section 10(1)(a) and (b)). Section 10(2) is the relevant restriction. A request to which section 10 applied could not be made by or on behalf of a person in the United Kingdom to the competent authorities of a country outside the United Kingdom unless an MA had been issued under Chapter 1 of Part 2 authorising the making of the request.

22. Section 10(2A) was inserted on 30 July 2017 by paragraph 9 of Schedule 3 to the Criminal Justice (European Investigation Order) Regulations 2017 SI No 730 ('the Regulations'). It creates two exceptions to the restriction in section 10(2). The first exception is that section 10(2) does not apply in the case of a request for assistance in connection with, or in the form of, interception of a communication stored in or by a telecommunications device if the request is made in the exercise of a statutory power that is exercised for the purpose of obtaining information.

23. At the relevant time, 'EU mutual assistance instrument' was defined in section 10(3) as an EU instrument relating to the provision of mutual assistance in connection with or in the form of, the interception of communications, which requires the issue of a warrant or equivalent instrument in cases in which assistance is given, and is designated as such in regulations made by the Secretary of State. 'International mutual assistance agreement' was and is still defined in section 10(3) as an international agreement which relates to mutual assistance in connection with, or in the form of, the interception of communications, requires the issue of a warrant or equivalent authority in cases in

which assistance is given and is designated as such an agreement in regulations made by the Secretary of State.

24. Section 11 creates an offence of unlawfully obtaining communications data. It is committed by a person who, without lawful authority, knowingly or recklessly obtains data from a telecommunications or postal operator.

25. Part 2 is headed 'Lawful interception of communications', and Chapter 1, 'Interception and examination with a warrant'. Section 15 is in Chapter 1 of Part 2. It provides for the warrants which may be issued under that Chapter. They are TIs, targeted examination warrants and MAs. Chapter 1 contains a significant number of protections in relation to those warrants.

26. A TI is a warrant which authorises or requires a person 'to secure, by any conduct described in the warrant', any one or more of three things (section 15(2)). They are the interception, in the course of their transmission by a telecommunications system, of communications described in the warrant, the obtaining of secondary data and the disclosure of what is obtained under the warrant to the person to whom the warrant is addressed.

27. 'Mutual assistance warrant' is defined in section 15(4) as a warrant which (among other things) authorises or requires the person to whom it is addressed to secure, by any conduct described in the warrant, the making of a request, in accordance with an international mutual assistance agreement, for the provision of any assistance of a kind described in the warrant in connection with, or in the form of, an interception of communications. 'International mutual assistance agreement' has the meaning given by section 10(3): see section 60(1).

28. A TI and an MA also authorise the conduct described in section 15(5), in addition to the conduct described in the warrant. A warrant issued under Chapter 2 may relate to a particular person or organisation, or to a single set of premises (section 17(1)). All those warrants, apart from an MA, may also relate to a group of people who share a common purpose, or who carry on a particular activity, or to more than one person or organisation, or set of premises, where the conduct authorised by the warrant is for the purposes of a single investigation or operation or for testing or training activities (section 17(2)). Those who can apply for a warrant under Chapter 1 are listed in section 18(1) and include a person who is the competent authority of a country or territory outside the United Kingdom for the purposes of an international mutual assistance agreement. The formal requirements for such warrants are listed in section 31. A warrant which relates to a particular person must name that person (section 31(3)).

29. In most circumstances, a TI and MA must be issued by the Secretary of State, subject to the controls in sections 19 and 20. An important further control is the requirement imposed by section 23 that two aspects of a decision to issue a warrant under Chapter 2 (its necessity and proportionality) must be reviewed, applying judicial review principles, by a Judicial Commissioner (see also sections 24 and 25). A control in Chapter 1 is that a 'relevant mutual assistance warrant' may be issued by a senior official designated by the Secretary of State if the interception subject is outside the United Kingdom (section 40(1)(a)). If, however, the Secretary of State or a senior official believes that the person group or organisation named or described in the

warrant as the interception subject is in the United Kingdom, that person must cancel the warrant. Chapter 2 contains many other significant controls to protect privacy.

30. Section 56 is headed 'Exclusion of matters from legal proceedings'. The effect of section 56(1), subject to the exceptions in Schedule 3 to the IPA, is to make evidence which has the effects described in section 56(2) and (3) inadmissible in any legal proceedings. Those effects are the disclosure in any circumstances from which its origin in interception-related conduct may be inferred, of any content of an intercepted communication or any secondary data obtained from it, or of tending to suggest that any interception-related conduct has or may have occurred or may be going to occur. 'Interception-related conduct', a term which might be thought to have a potentially wide meaning, is defined in relatively narrow terms (in section 56(2)). It includes a breaches of sections 3, and of the prohibitions in sections 9 and 10 of the IPA. Paragraph 2(1) of Schedule 3 to the IPA provides that section 56(1) does not prohibit the disclosure of any content of a communication, or any related secondary data if the interception of the communication was lawful under section 6(1)(c) (among other provisions).

31. Part 5 is headed 'Equipment Interference'. Section 99 is headed 'Warrants under this Part: general'. There are two types of warrant which may be issued under Part 5. One is a TEI (section 99(1)(a)). A TEI authorises or requires the person to whom it is addressed to 'secure interference with any equipment for the purpose of obtaining' communications, equipment data, and any other information (section 99(2)). A TEI must also authorise or require the person to whom it is addressed to secure the obtaining of the matters to which the warrant relates, and may also authorise that person to secure 'the disclosure, in any manner described in the warrant, of anything obtained under the warrant by virtue of section 99(3)(a)' (section 99(3)). The obtaining of communications or of any other information includes doing so by monitoring etc a person's communications or other activities, or by recording anything which is monitored etc (section 99(4)).

32. A TEI also authorises any conduct which is necessary in order to do what is expressly authorised or required by the warrant, including conduct for the obtaining of communications, equipment data or other information, and any conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance in giving effect to the warrant (section 99(5)). It may not authorise or require, by virtue of section 99(3), conduct in relation to a communication other than a stored communication which would (unless done with lawful authority) constitute an offence under section 3(1) (unlawful interception) (section 99(6)). 'Stored' means 'stored in or by a telecommunication system (whether before or after its transmission)' (section 99(8)). Any conduct carried out in accordance with a warrant under Part 5 is lawful for all purposes (section 99(11)).

33. 'Equipment data' is widely defined in section 100. It includes 'systems data' and 'identifying data' within section 100(2). 'Systems data' and 'identifying data' are defined in section 263. Section 101 is headed 'Subject-matter of warrants'. Section 101(1) lists the eight matters, to any one or more of which a TEI may relate. One is 'equipment belonging to, used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation': section 101(1)(c).

34. Section 106(1) and (3) gives various 'law enforcement chiefs' power to issue a TEI on an application made by an 'appropriate law enforcement officer' if the four conditions in section 106(1), or, as the case may be, section 106(3), are met. Section 107 enacts restrictions on the power of law enforcement chiefs to issue a TEI under section 106. Unless one of the exceptions specified in section 107(1) or 107(3) applies, a TEI may be issued whether or not the person who has power to issue the warrant considers that there is a 'British Islands connection'. That phrase is defined in section 107(4).

35. Section 108 provides for the approval by a Judicial Commissioner of warrants issued under Part 5 of the IPA. Section 135 defines 'communication', and 'equipment', among other things.

36. Part 6 is headed 'Bulk Warrants'. Chapter 1 provides for bulk interception warrants, Chapter 2 for bulk acquisition warrants, and Chapter 3 for bulk equipment interference warrants. None of these types of warrant is relevant to this case because the communications/information at issue in this case are not 'overseas-related' as defined in section 136(3) or section 176(2), and see section 158(3)). Parts 7, 7A and 7B concern activities of the intelligence services: respectively warrants relating to 'bulk personal datasets' retained by the intelligence services, bulk personal dataset authorisations, and third party bulk personal datasets.

37. The European Investigation Order ('EIO') in this case was made under the Regulations. The Regulations have now been repealed. When they were in force, regulation 7(1) provided that if it appeared to a prosecutor that an offence had been committed or that there were reasonable grounds for suspecting that an offence had been committed, and proceedings had been instituted in respect of the offence, or it was being investigated, the prosecutor might make an order under regulation 7. An order made under regulation 7 was an order specifying one or more investigative measures to be carried out in a participating State ('the executing State') for the purpose of obtaining evidence for use either in the investigation or the proceedings or both (regulation 7(3)). The prosecutor could only make the order if it appeared to him that the 'investigative measures to be specified in the order could lawfully have been ordered or undertaken under the same conditions in a similar domestic case'. Regulation 11(1) provided that in applying that test the prosecutor should consider various matters. Those included, where the investigative measure requested would require authorisation under an enactment before it could lawfully be done in the United Kingdom, whether such authorisation has been, or could have been, granted, taking into account various matters and the provisions of the enactment which apply to the granting of such an authorisation (regulation 7(3)). When the measure is in connection with, or in the form of, the interception of communications, the relevant authority must consider whether any additional requirements imposed by any enactment other than the Regulations have been complied with (regulation 7(4)).

The relevant reasoning in A

38. *A* was an appeal against a decision of Dove J, made at a preparatory hearing, that EncroChat material would be admissible in the criminal trials of several defendants. It was common ground that the EncroChat handsets were part of a telecommunications system. One issue on which the admissibility of the material turned was whether, at the time of the interception, the material was being transmitted (within the meaning of section 4(4)(a)) or was being stored, (within the meaning of section 4(4)(b)). Dove J

decided that it was being stored, and that it was therefore covered by paragraph 2(1) of Schedule 3, and, therefore, admissible. The CACD described that as 'the critical issue' in the appeal (paragraph 51), and as 'the only substantial question which the judge was required to answer', in paragraph 79. It upheld Dove J on that question (see paragraphs 51-69). The 'harvesting' was 'interception' which was made lawful by the TEI and by section 6(1)(c). Paragraph 2 of Schedule 3 made that product of the interception admissible (paragraphs 67 and 69).

39. The CACD added that it was 'necessary to say something about Grounds 3 and 4' while acknowledging that even if section 9 or 10 had been breached, that would not affect the admissibility of the material. Breaches of sections 9 and 10 might give rise to arguments under section 78 of the Police and Criminal Evidence Act 1984, although the CACD observed that it would be a 'surprising exercise of' of that power to exclude evidence which 'Parliament has provided in clear terms should be admissible' (paragraph 71).

40. The CACD considered Ground 3, which was based on section 10, in paragraphs 72-75. It recorded Dove J's conclusion that since the JIT was intending to go ahead with its plan in any event, the NCA had not made a request for any interception, but for the product of any such interception. The CACD did not approve that reasoning. The EIO appeared to the CACD, by reference to the statutory context, to be a request for assistance 'in connection with' the interception of communications. Unless section 10(2A) applied, it was unlawful because there was no MA (see section 15). Dove J had held that section 10(2A) did apply and that the relevant statutory power was that conferred by regulation 7 of the Regulations. The CACD noted that section 10(2A) was inserted in the IPA by the Regulations. It concluded that the purpose of the Regulations and of section 10(2A) was to 'incorporate the EU investigation order system into domestic law' (paragraph 73).

41. It would be inconsistent with that purpose to construe section 10 'so narrowly' as to exclude an EIO like the EIO in this case. The EIO was expressed to be 'a request for assistance in connection with, or in the form of, interception of a communication stored in or by a telecommunications system'. Those terms had broad meanings. A request made in order to obtain the results of interception of communications 'appears to us to be a request for assistance in connection with interception' (paragraph 74). In just the same way as the prosecution could not deny that the EIO was not 'a request for the purposes of section 10' it was impossible for the defendants to contend that the EIO was not made 'in the exercise of a statutory power' for the purposes of section 10(2A), which was enacted precisely in order to include EIOs (paragraph 75).

42. Ground 4 was based on section 9. The CACD considered ground 4 in paragraphs 76-78. There was no relevant warrant. Unlike section 10, section 9 does not refer to communications which are stored in or by a system. The defendants argued that activity which was lawful by virtue of section 6(1)(c), and by section 10(2A), was made unlawful by section 9. 'That would be an extraordinary outcome' (paragraph 76).

43. Dove J had held that there was no relevant request. The CACD did not consider it 'necessary to review' his conclusion about the facts. Whether that was right or wrong, Dove J had also ruled against the defendants on the construction of section 9. He held that 'on its proper construction, section 9… applies to requests for the interception of targeted interception material and not targeted interference material' so that it did not

apply on the facts. He considered that the reference in section 9 to interception of communications was to the interception of communications governed by Part 2 and by section 15. That was reinforced by the reference in section 9(2) to TIs 'under Part 2 of this Act'. The clear intention of section 9 was to prevent 'the circumvention of the regulation of Part 2 activity by the commissioning of overseas authorities to carry it out on behalf of the UK authorities'. To read section 9 as applying to conduct authorised by section 99 would cut across 'the breadth' of section 99(5) and would require a TI in relation to TEI material. That would not 'sit well' with the legislation which clearly provides separate regimes for targeted interception and TEI material.

44. The CACD agreed with Dove J that section 9 'should be construed so that it is restricted to prohibiting' a request to a foreign state to carry out interception which would need a TI if done in the United Kingdom by the authorities in the United Kingdom, unless the United Kingdom authorities have a TI. Section 10 covers a request made under an EIO or under an international mutual assistance agreement. By 'necessary implication' section 10 requires section 9 to be construed so that it 'does not apply to cases within section 10'. It only governs a 'request' made by means other than an EU mutual assistance agreement or an international mutual assistance agreement (paragraph 78).

> " section 9 of the 2016 Act should be construed so that it is restricted to prohibiting the requesting of a foreign state to carry out interception which would require a Part 2 targeted interception warrant if carried out in the United Kingdom by the United Kingdom authorities, unless such a warrant is in place. The position which applies if the request is made under an EU mutual assistance instrument or an international mutual assistance agreement is governed by section 10 so far as the assistance is in connection with or in the form of the interception of communications. That provision by necessary implication requires section 9 to be construed so that it does not apply to cases within section 10. It governs only a request made by means other than an EU mutual assistance instrument or an international mutual assistance agreement"

45. The CACD did not endorse the judge's reasoning that the NCA had not made a relevant "request" for the purposes of sections 9 or 10 (see paragraphs 72 and 77).

The relevant reasoning of the IPT

46. The issues which the IPT decided are described in paragraph 6 of its judgment. They included whether section 10 required the NCA to get an MA (and whether the absence of such a warrant made the EIO unlawful), whether section 9 required the NCA to get a TI, and whether the NCA was required to get a bulk equipment interference warrant. The IPT held that it did not have jurisdiction to decide whether or not the EIO was made lawfully, and that the NCA was not required to get a TI or a bulk equipment interference warrant.

47. In paragraph 36 the IPT recorded the NCA's understanding that the JIT had legal authority to carry out the relevant activity, and its understanding that it needed domestic authority to enable it to use the data acquired by the JIT. In paragraph 77 the IPT set out

the material parts of the description of the conduct which was the subject of the TEI. The IPT then held, in paragraph 78, that 'The purpose of the warrant was to render the conduct of the JIT lawful, when otherwise it might have been an offence under the Computer Misuse Act which the NCA might therefore commit as a secondary party by encouraging it. It therefore enabled the NCA to request the material from the JIT, which it was going to acquire in any event'. The Judicial Commissioner was being asked to authorise the collection and sharing of stored data from the devices. He was not being asked to authorise anything else.

48. In paragraphs 79-82 the IPT described the legislative provisions which were relevant to the arguments about sections 9 and 10 of the IPA. The IPT set out sections 9 and 10 of the IPA, and regulations 7 and 11 of the Regulations, commenting that the 'designated public prosecutor' for the purposes of the Regulations was the Director of Public Prosecutions ('the DPP') and any Crown Prosecutor, and that regulation 59 designated Directive 2014/41/EU regarding the European Investigation Order in criminal matters as an EU mutual assistance instrument for the purposes of section 10 of the IPA. Paragraph 9 of the Regulations amended the IPA by inserting section 10(2A).

49. In paragraphs 83-108 the IPT considered the arguments about section 10, under the heading 'Issue (b): The tribunal's jurisdiction in relation to the claims that the EIO was unlawful, and the claim that the NCA breached section 10 of the IPA'. It summarised the parties' submissions in paragraphs 83-87.

50. It concluded that the claims were claims that the claimants' human rights had been breached and that the IPT was the only appropriate tribunal to deal with those claims (section 65(3)(d) of RIPA). The IPT only had jurisdiction if the proceedings related to 'the taking place in any challengeable circumstances' of any conduct in section 65(5). Conduct takes place in such circumstances if it is conduct that took place under, required the grant of, or at least consideration of seeking, a warrant of the types listed in section 65(8) (section 65(7)).

51. The IPT stated that the claimants' characterisation of the 'conduct' was not consistent: they accepted that the EIO had asked for help with the interception of communications; but, they said, the 'conduct' was in 'challengeable circumstances' because it was done under the authority of a 'purported' warrant under Part 5 of the IPA. Those 'competing' characterisations conflated the roles of the DPP and of the NCA. The DPP made the request. For the purposes of section 10, the conduct was the making of the request. That was 'potentially prohibited' by section 10(2). The purpose of the EIO was to get the results of the interception of communications. It was a request for assistance 'in connection with interception'. This was consistent with paragraphs 72-75 of the decision in *A*.

52. At a late stage the NCA had argued that the NCA might not have needed a Part 5 warrant. If the NCA did need a Part 5 warrant, the conduct was within section 65(5)(czm) of RIPA, because it was in connection with conduct within section 65(5)(czd) of RIPA. The IPT did not consider that there were 'challengeable circumstances', however. The 'conduct' for this purpose was making a request for data obtained by the French authorities. The making of that request did not take place with the purported authority of a Part 5 warrant. No warrant under Part 5 was required, or

apt, to authorise the making of this kind of request. The existence of a TEI is not a lawful precondition for such a request.

53. Regulation 11 of the Regulations did not suggest otherwise. Where an investigative measure, if carried out in the United Kingdom, would require authorisation under an enactment, the maker of the request must consider whether such authorisation has been, or could have been, granted. The investigative measure specified in the EIO was a request for access to data obtained by the French authorities in respect of the EncroChat devices which were in the United Kingdom. The maker of the request was not asking for an investigative measure to be pursued, but for the fruits of an investigation.

54. The IPT also considered whether there were challengeable circumstances because the conduct needed the authority of an MA. No MA was required. The IPT agreed with the reasoning in *A* on this point. That reasoning was not binding but was 'highly persuasive'.

55. The reasoning in *A* was that the EIO was a request for assistance under an EU mutual assistance instrument in connection with the interception of communications. Section 10(2A) applied because the request was made in the exercise of a statutory power (the power of a prosecutor to make or to validate an EIO under regulation 7 of the Regulations). The purpose of the regulations and of section 10(2A) was 'to incorporate the EIO system into domestic law'. It was inconsistent with that purpose to construe section 10(1) and (2A) so as to remove an EIO from their scope. The CACD rejected the argument that a mutual assistance warrant was necessary for a lawful request for assistance in connection with the interception of communications.

56. If, therefore, the IPT had had jurisdiction, it would have rejected that challenge for the same reasons as were given in *A*.

57. The next issue which the IPT considered was whether a TI or a targeted examination warrant under section 15 was required. The claimants submitted that section 9 was engaged on the facts. It was argued that the NCA and the Judicial Commissioner had erred in law by relying on a Part 5 warrant. Section 9 does not distinguish between live and stored communications because foreign authorities would not be prepared to disclose their methods. A TI covered both interception in the course of transmission and the interception of stored material.

58. The IPT again agreed with the reasoning of the CACD in *A* (in paragraphs 76-79 of *A*). The IPT held that section 9 applies to requests for the interception of targeted interception material and did not apply here. The intention of section 9 was to stop the authorities in the United Kingdom from evading the regulation of activity within Part 2 by commissioning overseas authorities to do it in the United Kingdom on their behalf, and it should be construed accordingly. Section 10 governed requests made under an EU mutual assistance instrument (or under an international mutual assistance agreement) if the assistance was in connection with or in the form of the interception of communications. By necessary implication, section 9 did not apply to situations covered by section 10. Section 9 only applied to requests other than by means of an EU mutual assistance instrument or an international mutual assistance agreement. The IPT considered that section 6(1)(c) and section 10(2A) made the conduct lawful.

59. The IPT made a number of further observations which it considered supported the CACD's construction of sections 9 and 10 in *A*. The IPT noted that section 9 requires a TI. TI material is inadmissible (section 56 and paragraph 2 of Schedule 3). The IPT considered that it was difficult to see why Parliament would have chosen to make all material which came from requests to foreign authorities inadmissible. That was the consequence of the claimants' construction of section 9. That approach even applied to stored material. The refusal to admit material obtained by interception in the course of transmission was a policy choice to preserve the value of the use of that technique for intelligence purposes. It has nothing to do with fairness or Convention rights. It is not designed to protect the individual, but coincidentally gives 'a windfall benefit to defendants against whom the Crown cannot use evidence secured by those means'. There was no obvious reason why that windfall should also apply where the material was stored material, 'simply because a foreign agency, rather than a domestic one, had intercepted the material'.

60. The IPT then considered whether a bulk interference warrant was required. It was common ground that such a warrant could not have been granted to the NCA. The evidence did not entirely support the contention of exclusive criminal use. 294 out of 7407 phones which had been examined had not 'demonstrated a clear link to criminality'. 173 of those had no content, and the others held 'limited data'. The NCA relied on section 101(1)(c) of the IPA.

61. The IPT rejected the claimants' submissions. It was satisfied that the aim of Operation Venetic was 'to obtain material from one source, namely the EncroChat system. It was material about a large group of people, who were all users of the system. The NCA's approach was based on its assessment that the use of EncroChat was exclusively for criminal purposes'. Section 101(1)(c) was widely drawn. That width did not support the supposed limitations on which the claimants' arguments rested. There was no error of law in characterising the investigation as an investigation into the criminal use of technology. The IPT referred to paragraph 120 of *A*. This supported the view which the IPT had independently reached.

62. The claimants' argument could only succeed if they could undermine the NCA's assessment (when the NCA applied for the warrant) about the criminal use of EncroChat. No material provided to the IPT had that effect. The assessment dated from 2019 (that is, the 2019 strategic assessment which was referred to in the warrant). The assessment was not created for the purposes of the application. The material which had emerged more recently was irrelevant to the IPT's assessment. In any event, that material did not show non-criminal use of the system. It showed 'very extensive use…for criminal purposes'. There were a few cases in which there was not enough information to tell for what purpose the handset had been used.

63. The IPT also rejected the claimants' argument that the NCA had breached its duty of candour about collateral intrusion. The application for the warrant was not misleading.

The IPT's reasons for refusing permission to appeal

64. It is only necessary to refer to paragraphs 8 and 9 of the IPT's reasons for refusing permission to appeal. The IPT said that it had held that the purpose of the TEI was as described in paragraph 78 of the judgment (see paragraph 47, above). That was not an improper purpose. Whether or not the NCA's analysis of that issue, when it applied for

the warrant, was flawed, that was not an improper purpose. If, as the NCA had submitted, at a late stage in the hearing, a TEI was, in any event, unnecessary, it did not matter whether the purpose was a proper purpose or not.

The grounds of appeal

65. There are six grounds of appeal which raise six broad issues.

    1. Did section 9 require the NCA to get a TI?

    2. Was the TEI obtained under Part 5 of the IPA obtained for an improper purpose?

    3. Did the IPT err in law in holding that it had no jurisdiction to consider whether the NCA had breached section 10 of the Act by not having a mutual legal assistance warrant, and that no such warrant was needed?

    4. Was Operation Venetic a 'single investigation' for the purposes of section 101(1)(c) of the IPA?

    5. Did the IPT blur the distinction between thematic and bulk interception warrants in a way which interfered with the appellants' article 8 rights?

    6. Did the IPT err in holding that EncroChat was used exclusively, or very nearly exclusively, for criminal purposes?

The submissions

66. Mr Ryder KC put his submissions on ground 1 under three headings. First, the circumstances were clearly within section 9 on straightforward reading; second, the IPT misread section 9, and third, *A* is not binding. As the IPT did not hold that it was bound by *A*, and we have assumed, for the purposes of these applications, that we are not, we say nothing further about the third heading.

67. Mr Ryder relied on the definitions of 'interception' and of 'lawful authority' in section 4 and section 6, respectively. A TEI can only be used to intercept stored communications, whereas a TI applies both to live and to stored communications. The NCA was requiring or requesting the French authorities to intercept communications. Section 9 made it clear that a TI was necessary in this case. Section 9(1) did not have a 'carve out' for stored data. Had the NCA asked which warrant was appropriate, the only answer was a TI. The IPT's purposive interpretation of section 9 (see paragraph 58, above) did not explain which warrant was necessary.

68. The IPT's 'windfall' argument was wrong. The decision to mandate a TI was a policy decision by Parliament. Unless the appellants' construction was linguistically impossible, this court should give effect to the plain language of section 9. Foreign states did not distinguish between the interception of live and stored communications because they did not want to disclose their methods. It was not surprising that Parliament had taken a strict approach to the interception by a foreign state of communications to and from a person in the United Kingdom. The question for the IPT was which was the right warrant; and the answer was given by section 9.

69. The IPT did not address the question whether the TEI had a lawful purpose, but did address the question in its reasons for refusing permission to appeal. The purpose of the TEI was to make the conduct of the JIT lawful; and that was not a proper purpose. A TEI can only be issued for a statutory purpose, that is, to authorise the conduct described in the TEI.

70. Mr Ryder's main argument about section 10 was that the approach of the IPT was circular. If the EIO is the 'statutory power' referred to in section 10(2A)(a), the exception created by section 10(2A)(a) is redundant, because the necessary statutory power is always present.

71. On grounds 4 and 5, Mr Lakha KC argued that the IPT's interpretation of section 101(1)(c) drove a coach and horses through the distinction between a TEI and a bulk interference warrant. The 'criminal use of technology' is not a defined subject. The IPT's approach meant that a TEI could be used for any platform, such as WhatsApp. It was inconsistent with an opinion of Lord Anderson KC, with paragraph 298 of the Explanatory Notes for the Bill which became the IPA, and with the Code of Practice. The conduct described in the application for the TEI could not reasonably be described as being 'for the purpose of a single investigation or operation'. The blurring of that important distinction was a breach of the appellants' article 8 rights. The consequent interference with their article 8 rights was not 'in accordance with the law', and entirely arbitrary.

72. Mr Csoka KC argued, on ground 6, that the IPT had referred, in paragraph 110, to a confidential version of the NCA's 'National Strategic Assessment of Serious and Organised Crime' for 2019. This had been provided after Mr Johns had given evidence. The IPT's assumption that this was not created for the purposes of the application for the TEI was 'contrary to reason'. The NCA had intended to use its own implant at one stage. The factual basis of the IPT's assessment in paragraph 136 was no more than an assumption. The right to a fair trial (article 6) was engaged. The IPT's finding in paragraph 136 was made without any adversarial process.

Discussion

General remarks

73. We assume for the purposes of this judgment that there was a relevant 'request'; that, for the purposes of the definition in section 4 of the IPA, as the parties agreed in *A* and in the IPT in this case, the JIT were engaged in the interception of communications; and that the IPT had jurisdiction to consider the Appellants' complaints.

74. The IPA is a detailed framework. Its evident purpose is to protect privacy, while at the same time ensuring that those who apply for, issue, and approve warrants are governed by coherent and comprehensible rules which will enable them, sometimes in urgent circumstances, to ensure that any criminal liability, unlawful acts, exposure to civil liability, or to the payment of penalty are not incurred. It is unlikely, in that context, that there is any significant overlap between the cases covered by the restrictions in sections 9 and 10, as that is an obvious potential source of difficulty for all those bodies.

75. The exact words of these two provisions must be construed against the background of the more detailed provisions about TIs, MAs, and TEIs, to which sections 9 and 10 refer.

76. Section 9 prohibits a narrow class of requests to foreign authorities to intercept communications sent to or by an individual who is believed to be in the United Kingdom. Its obvious purpose is to bolster the prohibition created by the section 3 offence, by ensuring that the requests to which it applies cannot be made without the authority of a TI. It applies only to a request to intercept communications 'sent by, or intended for, an individual' who is believed to be in the United Kingdom at the relevant time. No such request may be made unless a TI has been issued which authorises the interception of communications 'sent by, or intended for, that individual'.

77. There are two significant and independent points about the provisions governing TIs which help with the construction of section 9.

78. A TI authorises the interception of communications in the course of their transmission. There is no reference in section 15 to material which is stored in a system.

79. A TI may authorise the interception of communications relating to a particular person or organisation, or to a group. If the TI is aimed at an individual, that individual must be named in the TI.

80. Those points show that section 9 is directed at the interception, during their transmission, of communications sent by or intended for a individual whose name is known to the authorities. In other words, section 9 does not address communications relating to an unidentified or unidentifiable person, or people. Nor does it address requests which relate to material stored in a system. We agree that 'interception' must be interpreted consistently throughout the IPA. The point here is that the coverage of section 9 is confined, not by that general definition, but by the need to interpret section 9 consistently with the provisions governing TIs.

81. Section 10 addresses a different situation from section 9. It applies to requests for help from foreign authorities. It applies to a potentially wider class of requests than section 9 does, because, for example, it is not limited to requests concerning an individual who is believed to be in the United Kingdom. The general rule is that such requests cannot be made without an MA. If, however, the request is 'in connection with, or in the form of, a request for the interception of communications', and it relates to the interception of a communication which is stored in or by a telecommunications system, then such a request may be made if the conditions in section 10(2A) are met. The request in this case, if it is assumed that such a request was made, was not a request to which section 9 could apply, for the reasons given in paragraphs 78 and 79, above. It was however, a request to which section 10(1) and 10(2), but also, the exception in section 10(2A), could apply.

Grounds 1-3

82. An important issue raised by grounds 1 and 3 is whether the conduct of the NCA in this case infringed one or other of the restrictions imposed by sections 9 and 10, respectively. Mr Ryder argued that section 9 and section 10 cover the same field, and that whether or not the requirements of section 10 are met, the NCA must still comply

with section 9, which is not expressly limited to the interception of live communications. The consequence of his interpretation would be that whether or not section 10 is satisfied, section 9 would still require a TI on these facts.

83. The word 'intercept' is defined in section 4 as including the 'interception' of stored material (see section 4(1) read with section 4(4)(b)). Mr Ryder further argued that there is nothing in the express language of section 9 which excludes stored material from the ambit of 'interception' in section 9(1). On its face, therefore, section 9 is not limited to the interception of live communications. It also applies to the interception of stored communications.

84. In *A*, the CACD relied on the reasoning of the judge in that case for the conclusion that section 9 applies to 'requests for the interception of targeted interception material and not targeted equipment interference material, and it is therefore of no application in the present circumstances'. It added that section 9 should only be read as applying to a request to a foreign state to intercept communications where that interception would need a TI if done in the United Kingdom.

85. We accept the respondent's submission that Mr Ryder's arguments under ground 1 are fundamentally inconsistent with the decision of the CACD in *A*. As we have indicated, we are prepared to assume for present purposes, without deciding, that that decision is not binding on the civil division of this court. Nevertheless, it is a recent decision of the CACD and directly on point, and therefore strongly persuasive. Whether or not we are bound by that decision, we accept it is correct; and we agree with the IPT that its further observation (noted in paragraph 34 above) provides additional support for the construction which the CACD gave to sections 9 and 10. We see no arguable basis on which the reasoning in *A* can be rejected, distinguished or sidestepped as Mr Ryder invites us to do. We also consider that the further points which we have made in the first section of this part of our judgment provide further support, if that is needed, for the reasoning and conclusions of the IPT and of the CACD in relation to this ground of appeal.

86. It follows that the IPT was not, even arguably, wrong to decide that section 9 should be construed in the way indicated by the CACD in *A*. Ground 1 therefore raises no arguable point of law. Nor does it raise any important point of principle or practice about whether one division of this court is bound by a decision of the other division, because we have assumed that we are not bound by the decision in *A*.

87. We turn to the arguments on section 10. We do not accept that Mr Ryder's main point is arguable, for two reasons. First, the restriction in section 10(2) applies, by virtue of section 10(1), both to requests under an EU mutual assistance instrument and to requests made under other international mutual assistance agreements. In the case of the former the nature of the request is not limited. In the case of the latter, the request is limited to a request 'in so far as the assistance is in connection with or in the form of, a request for the interception of communications'. The exception in section 10(2A), by contrast, only applies to requests made in the exercise of a relevant statutory power, or in accordance with a relevant court order, and which are made in relation to a stored communications. It is, therefore, a specific and limited exception to the general restriction enacted by section 10(2). We note the echo, in the language of section 10(2A)(a), of the words of section 6(1)(c)(ii). We accept that section 10(2A) was inserted to deal with EIOs. Those factors mean, however, that that exception is not

always met by all EIOs. An EIO in relation to the interception of live communications will never fall within the exception, and there may be other requests for international mutual assistance which are made in the exercise of a statutory power, or in accordance with a court order. The contrary is not arguable.

88. We do not consider that there is any arguable error of law in the IPT's implicit approach to the question whether the TEI was obtained for an improper purpose. As the IPT observed, it may be that no TEI was required at all (a late argument relied on by the NCA on which the IPT did not find it necessary to rule). But we do not consider that it is arguable, either that, if the NCA was wrong in supposing that a TEI was required, it applied for the TEI for an improper purpose, or that if it was right to think that a TEI was required, the NCA had an improper purpose in seeking the authority of a warrant for the conduct described in the application for the warrant. A recurrent theme of the IPA is that the relevant authorities must apply for the warrant which will make their proposed activity lawful, but also that they must conscientiously consider, in relation to interception and related matters, whether any, and if so what, warrant may be necessary, as section 7(3)(c) shows.

89. For those reasons, grounds 1-3 do not raise an arguable point of law. Nor do we consider that the test in section 67A(7) of RIPA is met (see paragraph 3, above).

Grounds 4-6

90. The IPT had evidence, which it was entitled to accept, that the NCA's contemporaneous assessment was that EncroChat was exclusively, or almost exclusively, used for criminal purposes. There was, as we understand it, no evidence to suggest that it was not. There were a few cases in which there was not enough evidence to show what use was being made of the EncroChat handset in question, but no evidence of any use for purposes which were not criminal. The contrary is not arguable. Nor do we consider that it is arguable that the IPT erred in law in concluding, by applying the words of section 101(1)(c) to the facts which it was entitled to find, that Operation Venetic was 'a single operation or investigation'. It is significant not only that Operation Venetic was an operation or investigation in relation to EncroChat but also that its limits were co-terminous with the activities of the French authorities, that is, the deployment of the implant on 2 April 2020, and its use for the period described as 'stage 2' in the application for the TEI.

91. For those reasons, grounds 4-6 do not raise an arguable point of law. Nor do we consider that the test in section 67A(7) of RIPA is met (see paragraph 3, above).

Conclusion

92. For all those reasons, we refuse permission to appeal on grounds 1-6.