Neutral Citation Number: [2021] EWCA Crim 128

Case No: 202100094 B1, 202100110 B1, 202100112 B1, 202100113 B1

IN THE COURT OF APPEAL (CRIMINAL DIVISION)
ON APPEAL FROM THE CROWN COURT AT LIVERPOOL
The Hon Mr Justice Dove

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 05/02/2021

Before:

THE RT HON THE LORD BURNETT OF MALDON,
LORD CHIEF JUSTICE OF ENGLAND AND WALES
THE RT HON LORD JUSTICE EDIS
and
THE HON MRS JUSTICE WHIPPLE

- -

Between:

A, B, D & C	**Appellant**
- and -	
REGINA	**Respondent**

- -
- -

Mr. Peter Wright, Q.C. and Mr. Ian Whitehurst for **A**
Mr. Matthew Ryder, Q.C. and Mr. Simon McKay for **B**
Mr. Andrew Radcliffe, Q.C. and Mr. Matthew Buckland for **D**
Mr. Rupert Bowers, Q.C. and Ms. Sarah Vine for **C**
All assigned by the Registrar of Criminal Appeals
Mr. Jonathan Kinnear, Q.C. and Mr. Tom Payne for the Prosecution

Hearing date: 20 January 2021

- -

Approved Judgment

THE LORD BURNETT OF MALDON CJ:

Introduction

1. The issue in this appeal is whether evidence obtained from a mobile phone system known as EncroChat ("the EncroChat material"), which was marketed to its users as totally secure, can be admitted in evidence in criminal proceedings or is excluded by the Investigatory Powers Act 2016 ("the 2016 Act"). The main question is whether the communications were intercepted at the time they were being transmitted or, as the judge found, were recovered (intercepted) from storage. If the judge was right, subject to a number of subsidiary arguments, the evidence would be admissible. As we shall explain, the security of the EncroChat system was breached by a French law enforcement agency.

Reporting restrictions

2. The appeal is against a ruling by Dove J in a preparatory hearing held under section 29 of the Criminal Procedure and Investigations Act 1996 ("the 1996 Act"). Pursuant to section 37 of the 1996 Act the reporting of these proceedings is prevented until the conclusion of the trial, save for specified basic facts such as the name of the accused and the offence, unless the court orders that the provisions do not apply. There is an identical restriction on reporting of the proceedings in the Crown Court. This is a *reporting* restriction. There is no bar on the decisions of this court and the Crown Court being shared among judges and legal professionals so that they may inform decisions in other cases involving the same issues. Those further decisions will also be subject to reporting restrictions. As will appear below, we make a direction under section 37(4) of the 1996 Act with the effect that this judgment (but not that of the Crown Court) can be reported.

The scope of the appeal

3. Dove J directed that a preparatory hearing should be held in order to decide whether the EncroChat material obtained by the National Crime Agency from the EncroChat system of communications is admissible as evidence against these appellants in the criminal proceedings which are pending against them. In a reserved written ruling handed down on 4 January 2021 he decided that it was.

4. The judge also rejected submissions:

    a. that he should exclude the EncroChat material under section 78 of the Police and Criminal Evidence Act 1984; and

    b. that he should stay the criminal proceedings as an abuse of the process of the court.

5. There is no appeal against these further two decisions. We deal only with the legal issue of the admissibility of the EncroChat material. That issue is not affected by the facts of the allegations against these appellants and it is not necessary for us to refer to those facts at all. The allegations are serious and have yet to be tried. Nothing in this judgment is capable of causing any prejudice to the trial. As will appear, there are a significant number of cases pending in England and Wales derived from EncroChat

material which otherwise are quite unconnected with this one. For this reason, it is important that the legal admissibility issues in this case should be determined in a judgment of this court which can now be published. For that reason, we direct under section 37(4) of 1996 Act that the restriction under section 37(1) shall not apply to this judgment. It may be published. The restrictions continue to apply in all other respects. This judgment is anonymised, and the names of the appellants must not be published until after the trial is concluded, in accordance with the statutory scheme which is varied only to the extent just identified.

6. The preparatory hearing appears to have lasted 15 days between the 16 November and 3 December 2020. It involved hearing a great deal of oral evidence including expert evidence. The judge set out that evidence and his conclusions on it with great care in a judgment which runs to 129 pages. Some of it is relevant to the legal issue before us, but much of it is not. It appears that the appellants conducted a lengthy and perhaps rather conjectural search for an abuse of process and, on the finding of the judge, failed to find anything. Other judges dealing with these cases will have the benefit of Dove J's ruling on that issue. If it is intended to repeat this kind of process in other pending cases involving EncroChat material, those involved should not be surprised if the trial judges deal with them rather more briskly.

The context of the legal issue

7. The EncroChat material was obtained by a Joint Investigation Team (JIT) of French and Dutch investigators and prosecutors by interfering in the EncroChat communications system. It was then supplied to the United Kingdom authorities where it was used in a large number of investigations, including the one which led to the present case. The judge was required to hear evidence about how this occurred, and then to make findings of fact. He then had to apply the United Kingdom domestic law governing the admissibility of such material, which is found in the 2016 Act.

8. The 2016 Act adopted a domestic law framework which is unique in Europe and which resembles previous regimes. Historically, intercept material (classically phone tapping, but not limited to that) could be lawfully obtained by the authorities. Subject to a number of immaterial exceptions, it could not be used in evidence in proceedings but was reserved for intelligence use. The policy justification for that approach has been debated on many occasions and centres around protecting sensitive capabilities and wider operational and practical concerns. All were discussed in *Intercept as Evidence*, December 2014 Cmnd 8989 which was the report of a review of Privy Councillors provided to Ministers. In many other jurisdictions, including France and the Netherlands, there is no blanket prohibition on the admission into evidence of intercept material. The 2016 Act superseded the law found in the Regulation of Investigatory Powers Act 2000, which itself replaced the Interception of Communications Act 1985. Major changes between the current regime and the one established in the 2000 Act concern the new regulatory and supervisory system established by the 2016 Act. The law relating to admissibility of intercept material, and the definition of what is and is not intercept material also changed in important ways.

9. The essential point before us is the submission, rejected by the judge, that the EncroChat material is intercept material and inadmissible in criminal proceedings because of section 56 of the 2016 Act, and further that it was unlawfully obtained under a Targeted Equipment Interference warrant, when its obtaining should have been

identified as a kind of interception which would require a Targeted Interception warrant. Targeted Equipment Interference warrants are governed by Part 5 of the 2016 Act and may produce material which can be used in evidence. Targeted Interception warrants are governed by Part 2 of the Act and the product is inadmissible in evidence in almost all criminal proceedings, including these. The judge found that the EncroChat material in this case was obtained under Part 5 warrants. These were approved by Sir Kenneth Parker, a Judicial Commissioner, on 5 March 2020, and Sir Brian Leveson, the Investigatory Powers Commissioner, on 26 March 2020, prior to the obtaining of the EncroChat material. The second warrant was needed in order to widen the scope of the first for reasons which are not material to the issues before us. The issue is whether that approach was correct, or whether on a true understanding of the way the data were obtained, and of the 2016 Act, they comprised material obtained unlawfully under the wrong warrant and, in any event, were inadmissible.

The facts as found by the judge

10. Much of the factual background to the issues in this appeal is set out by the Divisional Court (Singh LJ and Dove J) in a decision refusing permission to pursue judicial review proceedings challenging the European Investigation Order brought by C, one of the appellants in this case, see *R (C) v. Director of Public Prosecutions* [2020] EWHC 2967 Admin. The judge set out the evidence in relation to this aspect of the process in great detail and it is not necessary for us to rehearse that here. The judgment of the Divisional Court is in the public domain. The scheme for European Investigation Orders in the Criminal Justice (European Investigation Order) Regulations 2017, SI 2017 No. 730 ("the 2017 Regulations") in force at the material time is set out in that judgment. By regulation 7, a designated public prosecutor had the power to make or validate a European Investigation Order.

11. The judge summarised the nature of the EncroChat system in paragraph 4 of his ruling as follows:

> "EncroChat is a system of encrypted communication. It operates using specific handsets provided by the EncroChat system operator, and functions on the basis that the EncroChat devices can only communicate with other EncroChat devices. The EncroChat devices have dual operating systems, one being the EncroChat operating system itself, and the second being a standard Android system with no functionality. Depending upon how the handset is switched on, it will start in either the EncroChat or the Android system mode. In order for one user of EncroChat to speak to another it is necessary for them to know the unique user identification, or handle, of that person. Akin to other systems of encrypted communication, any message using the EncroChat system is encoded or encrypted as it passes through the EncroChat server between one handset and another, being decoded or de-encrypted at the receiving handset so that the user can read it."

12. The JIT called its harvesting of EncroChat material "Operation Emma". The judge explained how Operation Emma had come to the attention of the United Kingdom authorities and how it had proceeded. The important findings for the points which we

have to decide concern the way in which the material which was supplied to the United Kingdom authorities had been obtained. In short summary, the EncroChat servers were in France and the French Gendarmerie had discovered a way to send an implant to all EncroChat devices in the world under cover of an apparent update. That implant caused the device to transmit to the French police all the data held on it. This was called the Stage 1 process. It would capture all data which had not been erased, typically therefore 7 days' worth of communications. Thereafter, in the Stage 2 process, the implant collected messages which were created after Stage 1. The Stage 2 collections occurred after what was called "the infection", which was the point at which the implant first arrived on the device and executed Stage 1.

13. It was necessary for the judge to determine whether the EncroChat material was Part 2 Intercept material or Part 5 Equipment Interference material. The relevant background facts can be stated quite shortly:

i) The French had all the necessary legal instruments in place to undertake the extraction of the material from the devices all over the world lawfully as a matter of French law.

ii) The implant was loaded by the French authorities on to the EncroChat servers in Roubaix and then via the servers uploaded onto all the EncroChat devices worldwide.

iii) In response to the European Investigation Order issued by the United Kingdom authorities, the National Crime Agency was permitted by the French Authorities to have access to the data being obtained with effect from 1 April 2020. This was the date on which the French authorities started the collection of the data from the EncroChat devices.

iv) C3N is the French police digital crime unit. It gave its name, so far as these proceedings are concerned, to the implant and the means by which it extracted and preserved data. The judge found that the data which was harvested by the implant was sent by the device to the C3N server and then on to the server at Europol.

14. The judge then set out his findings of fact in a little more detail as to how the system worked in six important paragraphs:

> "148. Within each device there are two forms of memory: Realm, which holds an archive of apps and data for use on the device, and RAM which is a faster and temporary type of memory which holds apps and data whilst the app is running on the device and is used for the operation of the app and supporting the activity of the CPU. To make use of the EncroChat system the owner of a device needed, firstly, to open the app on the device. Upon launch, the app's program and some of its data would be drawn from Realm into RAM for use by the CPU in order to send and receive messages. <u>The owner would compose a message on the device for an identified contact and this would be held in RAM for the purposes of the app, and when instructed to send the message the app ensured its encryption, following</u>

which it would be sent to the radio chip and antenna for it to be transmitted out of the device to the EncroChat server. Having passed through the EncroChat server, via the receiver's message queue, the message would arrive on the receiving device when it was switched on and was running the EncroChat app. The message would be decrypted and then held in RAM, and married with other information on the receiving device which was relevant to the app, including for instance the receiving device owner's nickname for the sender. The message would then be held in RAM for the purposes, for instance of being displayed on the screen of the device, or being forwarded to other contacts. The message would be sent to Realm when either the app was closed down or the device was turned off, unless, of course the user had deleted it using the app prior to closing the app down. [underlining added].

149. It is very clear, indeed uncontroversial, that the effect of the implant was to lead to exfiltration of the messages from the devices: the messages were not taken after they had left the device of the sender or before they had arrived on the device of the receiver. This conclusion is supported by the fact that at the time that they were taken the messages were not encrypted, and had therefore been taken before encryption on the sending device and after decryption on the receiving device. The data which arrived at the C3N server from both the sending and the receiving device as a consequence of the implant was copied from data which was on the device. In relation to stage 1, this data was copied from the Realm part of the device's hardware and sent to C3N. It again appears to be common ground that the stage 1 operation of the implant, what Mr Campbell[1] described as a sweep, occurred several times on each device in the early days after the commencement of the operation of the implant. In relation to stage 2, it is clear that in relation to the sending device the data was copied from data held in the memory in RAM, whilst it was present in RAM as a consequence of the EncroChat app and the app working with the data. Mr Campbell's evidence in relation to the time taken between the creation of the message, the exfiltration of the data and its arrival at C3N provides some support for this conclusion. The analysis of both Mr Shrimpton[2] and Mr Campbell supports the existence of the two stages of the operation of the implant. As was explained, the data would remain in RAM and would not be removed to Realm for the period of time that the app was open on the device: that could obviously amount to a very lengthy period.

150. In relation to the receiving device, it is clear from the evidence relating to the nickname that by the time the received

[1] An expert called on behalf of the appellants.
[2] An officer of the National Crime Agency cyber crime unit, who gave evidence of fact and also explained how the system worked.

message came to be exfiltrated it had been packaged with data from Realm (or data which had previously been taken from Realm and was in RAM with the app) and was not being transmitted: it had arrived and was established as received after transmission on the device. Again, this data would remain in RAM on the device, with such data as had been joined with it, for so long as the app remained open on the phone and would only be transferred to Realm when the app was closed or the device turned off. Further, it is clear from the evidence, in particular in relation to the received messages, that the copied data extracted to the C3N server was not identical to that which had been sent from the sender's device to the receiver's device.

151. What is notable, in my view, is the correspondence in principle between these findings in relation to the operation of the implant and the description noted from the information at the Europol meeting by Ms Sweeting[3], along with the explanation which M. Decou[4] confirmed which had been written on her laptop. It was a two stage process in which, firstly, historic data was removed from the device and then, secondly, messages were gathered from the devices on an ongoing basis.

152. Turning to the application of the 2016 Act against the background of these factual matters, as set out above the first question is whether the EncroChat data falls within section 4(4)(a) or 4(4)(b) of the 2016 Act. Whatever adjectives were used in the evidence, this question falls to be determined on the basis of the application of the statutory provisions and not, for instance, whether a witness or document used the term "live" or "stored". The question of the status of the communication at the relevant time is whether it was at that time "being transmitted" or "is stored in or by the [telecommunication] system (whether before or after its transmission)". I have reached the conclusion that I am sure that the EncroChat data is properly regarded to be falling within section 4(4)(b) of the 2016 Act for the following reasons.

153. It is common ground that the communications must be either within section 4(4)(a) or section 4(4)(b): there is no third or alternative intermediate category. It is clear to me on the evidence that, firstly, at the relevant time when the messages were made available they were not "being transmitted". As set out above, they were not taken when the message was being transmitted from the sender's device to that of the receiver.[5] Furthermore, again as set out above, they were copied from data which was held on the device, and it was a copy which was sent

[3] An intelligence officer of the National Crime Agency.
[4] M. Decou is a French police officer who had given relevant evidence in a witness statement which the judge admitted as hearsay under Part 11, Chapter 2 of the Criminal Justice Act 2003
[5] This sentence is particularly criticised by the appellants, see paragraph 36(c) below.

> to the C3N server. It is, in my view, particularly clear from the evidence in relation to the data exfiltrated from the receiving device that the data was not made available whilst being transmitted. The incorporation of the nickname for the sender from the data held in the receiver's device (either from Realm or already available in RAM) demonstrates that the transmission process in respect of that data had conclusively finished and it cannot be said that the data was, at the stage it was taken, being transmitted. In relation to the sender, the message was also stored on the device in RAM and copied from there by the implant before being encrypted and leaving the device and being transmitted. It follows that the EncroChat data was not "being transmitted" at the time it was taken and was properly to be regarded as "stored in or by the system (whether before or after transmission)" and subject to section 4(4)(b) of the 2016 Act. I have no difficulty in concluding that the holding of the message data in RAM memory as described above is to be regarded as being stored in or by the system (either before or after transmission) for the purposes of the 2016 Act."

The positions of the parties before the judge

15. The principal question for the judge, as for us, is whether the communications fell within section 4(4)(b) of the Act, as the prosecution submitted or section 4(4)(a) of the Act, as the appellants submitted. This involves deciding whether, at the point when they were intercepted, they were "stored in or by" the telecommunications system by which they were transmitted, or whether they were "being transmitted" at that point. The appellants submitted that the EncroChat material was inadmissible by reason of the exclusionary rule in section 56 of the 2016 Act. That, in short, was said to be so because it was intercepted while it was "being transmitted".

16. The prosecution submitted that

    i) the EncroChat messages were admissible and fell within the exception provided by section 56(1) and schedule 3 paragraph 2 of the Act because the messages were "stored in or by the system" at the time when they were intercepted; and, in any event,

    ii) that the material was not obtained as a result of "interception related conduct" because none of the five classes of such conduct (as contained within section 56(2) of the Act) applied to the present case, alternatively it was not conduct carried out in the United Kingdom within the scope of section 4(8) of the Act.

17. There was a further issue as to whether the United Kingdom authorities had made an unlawful request for assistance to the French authorities contrary to prohibitions contained in sections 9 and 10 of the 2016 Act.

An agreement between the parties about handsets

18. The argument before the judge and before us has proceeded on the basis that the handsets are part of the "public telecommunications system", and therefore that

material stored on them is stored "in or by the system". The system in this case is a "public telecommunications system", as defined in section 261(8), (9) and (13) which are set out in the Appendix. We have reservations about whether handsets do ordinarily form part of the "system", given the nature of modern mobile phones which have many functions. In particular, section 4(3) extends the definition of an act of interception to include interference with any wireless telegraphy apparatus used for making transmissions to or from apparatus that is part of the system. Before us it was suggested that this would include mobile phone handsets. This extension would be unnecessary if the wireless telegraphy apparatus is part of the system. The extension of "relevant act" so that it extends to interference with handsets may be contrasted with the lack of any such extension in relation to the definition of the system for the purposes of considering the "relevant time". It would suggest that unless specifically provided otherwise, handsets are not part of "the system". Section 4(3) would not be necessary at all if the agreed position of the parties before us is right. This issue was not argued by the parties, and we will approach this appeal on the agreed basis that in respect of the EncroChat system the handsets are part of "the system". Whether that is right or not in general, it is possible to see how it could be true of this particular system in view of the findings of the judge about its nature, in paragraph 4 of his ruling set out above at our paragraph [11]. We do not decide the point, but proceed on the basis of the agreement between the parties reached in respect of this particular system. If the handsets were not part of the system, then interrogating them and extracting their content would not amount to interception at all, and the current issue of admissibility would not arise.

The relevant statutory provisions

19. The Appendix to this judgment contains an explanation of the relevant statutory scheme and sets out the most relevant provisions. The key provisions for us are sections 3, 4, 6, 99, and 56 of, and Schedule 3 to, the 2016 Act. These are connected to sections 9 and 10 which govern the warrantry requirements for cases involving international co-operation. It is worth recording that section 10 has changed materially since the end of 2020 because of the United Kingdom's withdrawal from the European Union, and we are dealing with the law as it was at the time when the relevant activity took place in this case, and when the issues were decided by the judge. Sections 9 and 10, as they were in force at the relevant time, are set out in the Appendix.

20. The provision which is central to this appeal is section 4. The statutory context of section 4 is that it defines terms which are used in section 3 and section 56, both of which are set out so far as relevant in the Appendix. Section 3 is the offence creating provision. It provides, among other things, that it is an offence to intercept intentionally a communication in the course of its transmission by a public telecommunications system where the interception is carried out in the United Kingdom and the person does not have lawful authority to carry out the interception.

21. Section 56(1) provides for the exclusion of, among other things, evidence in legal proceedings:

> "…….which (in any manner) —
>
> (a) discloses, in circumstances from which its origin in interception-related conduct may be inferred—

(i) any content of an intercepted communication, or

(ii) any secondary data obtained from a communication, or

(b) tends to suggest that any interception-related conduct has or may have occurred or may be going to occur.

This is subject to Schedule 3 (exceptions)."

22. Section 56(2) defines "interception-related conduct". It includes, by section 56(1)(a) conduct by defined United Kingdom authorities which is, or in the absence of any lawful authority would be, an offence under section 3(1). This is the provision designed to keep interception techniques secret for the policy reasons identified at paragraph [8] above. Parliament has preserved that policy but also provided that it does not extend to the material described in Schedule 3. The Schedule 3 exceptions include, in paragraph 2:

> "(1) Section 56(1)(a) does not prohibit the disclosure of any content of a communication, or any secondary data obtained from a communication, if the interception of that communication was lawful by virtue of any of the following provisions—
>
> (a) sections 6(1)(c)"

23. Section 6 defines what "lawful authority" means for the purposes of these provisions. Subsection (1)(c) includes the following:

> **"6. Definition of "lawful authority"**
> (1) For the purposes of this Act, a person has lawful authority to carry out an interception if, and only if—
> …….
> (c) in the case of a communication stored in or by a telecommunication system, the interception—
> (i) is carried out in accordance with a targeted equipment interference warrant under Part 5."

24. Part 5 of the Act provides for the issue and consequences of a type of warrant called a Targeted Equipment Interference warrant, defined in section 99. This type of warrant may be one which authorises or requires the person to whom it is addressed to secure interference with any equipment for the purpose of obtaining communications, but it may also authorise conduct which is not related to communications at all. Where the authorised conduct amounts to interception of communications, its product is admissible in evidence under section 6(1)(c). It would appear that Parliament has decided that the need to keep the techniques used in the interception of communications secret does not extend to techniques used in extracting data from equipment even if they may recover communications. The way in which that policy decision is given effect in the 2016 Act is by providing for the different treatment of what it describes as communications "stored in or by a telecommunication system", a phrase which we have seen in section 6(1)(c) and which originates in section 4, to which we now turn.

25. Section 4 is more fully set out in the Appendix to this judgment, but to assist the narrative we will set out the parts which are fundamental to the resolution of the issue in this appeal:

> **"4 Definition of "interception" etc.**
> Interception in relation to telecommunication systems
> (1) For the purposes of this Act, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if—
> (a) the person does a relevant act in relation to the system, and
> (b) the effect of the relevant act is to make any content of the communication available, at a relevant time, to a person who is not the sender or intended recipient of the communication.
> For the meaning of "content" in relation to a communication, see section 261(6).
> (2) In this section "relevant act", in relation to a telecommunication system, means—
> (a) modifying, or interfering with, the system or its operation;
> (b) monitoring transmissions made by means of the system;
> (c) monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system.
> (3) For the purposes of this section references to modifying a telecommunication system include references to attaching any apparatus to, or otherwise modifying or interfering with—
> (a) any part of the system, or
> (b) any wireless telegraphy apparatus used for making transmissions to or from apparatus that is part of the system.
> (4) In this section "relevant time", in relation to a communication transmitted by means of a telecommunication system, means—
> (a) any time while the communication is being transmitted, and
> (b) any time when the communication is stored in or by the system (whether before or after its transmission)."

26. This definition of interception applies for the purposes of the offence creating provision, section 3. The policy of the 2016 Act is that all conduct caught within the section 4 definition should be criminal, unless done lawfully under an appropriate warrant and by an appropriate person. This includes an act whose effect is to make content of communications available to a third party both "while the communication is being transmitted" (section 4(4)(a)) and "any time when" it "is stored in or by the system" (section 4(4)(b)). However, as we have seen, in relation to "stored" communications a different policy as to secrecy applies. There is no necessary connection between these two policies. An act may be criminalised, and its nature and product may also be protected from disclosure, or it may be criminalised and there need be no such protection. These are policy decisions for Parliament.

27. It was agreed between the parties before us and before the judge that for the purposes of section 4(4), a communication at the time of the "relevant act" must be either "being transmitted" or "stored in or by the system (whether before or after its transmission)". Section 4(1) says that in either case the communication is "in the course of its transmission" at the time of its interception. We shall return to this agreed position later in this judgment.

28. The prosecution has submitted that the exclusionary regime in section 56 does not, on a true construction of the whole of the 2016 Act, apply to material obtained under a Part 5 warrant issued under section 99 of the 2016 Act. They submit that the exclusionary regime applies only to material obtained under Part 2 warrants for interception of the kind which cannot be authorised by a Part 5 warrant. Mr. Kinnear, Q.C, for the prosecution, called this "old school" interception, which would include phone tapping resulting in telephone conversations being overheard while they were taking place. We shall deal with that submission below, without setting out or summarising here all the parts of the 2016 Act on which Mr. Kinnear relied.

The conclusions of the judge

29. The key question was whether at the relevant time the communications were "being transmitted" or were "stored in or by the telecommunication system." The judge found the latter to be the case. The EncroChat messages were properly regarded as falling within section 4(4)(b) of the 2016 Act and they had been obtained in accordance with a Targeted Equipment Interference warrant. He decided that for the following reasons:

    i) At the relevant time when the messages were made available they were not "being transmitted;" it was clear from the evidence in relation to the data exfiltrated from the receiving device that the data was not made available whilst being transmitted. The incorporation of the nickname for the sender from the data held in the receiver's device demonstrated that the transmission process of the data had finished. The judge indicated that he had no trouble in concluding that the EncroChat data was not being transmitted at the time that it was taken and was properly to be regarded as "stored in or by the system (whether before or after transmission)" and subject to section 4(4)(b) of the 2016 Act. The judge ruled that he did not consider that the distinction between RAM and Realm as described by the defence experts equated to the distinction between "being transmitted" and being "stored" as set out in the statutory provisions. The defence approach sought to extend the notion of transmission well beyond anything which was contemplated by the 2016 Act.

    ii) The Equipment Interference Code of Practice was published pursuant to Schedule 7 of the 2016 Act and was admissible as evidence in criminal proceedings. It addressed the exercise of functions under Part 5 of the 2016 Act and the authorisation of Targeted Equipment Interference warrants and their operation. The judge considered that these provisions from this Code of Practice were consistent with the conclusions that he had already made in relation to this issue.

    iii) Having considered the provisions of section 99 of the 2016 Act, which contained the power to make a Targeted Equipment Interference warrant and the scope of such a warrant, the judge decided that the interceptions were carried out in

accordance with the warrant that had been obtained. The warrant application accurately described the way in which the implant was to operate and the warrant authorised what was then done. This was a finding of fact set out in paragraphs 161 and 162 of the judge's ruling. It was a finding of fact to which he was entitled to come, and there is no challenge to it in this appeal. On the contrary, before us Mr. Ryder, Q.C., making submissions on behalf of all appellants, relies on it in support of his submission that the warrant was a request to the French authorities for the purposes of his argument on sections 9 and 10 of the 2016 Act.

30. In that context, the appellants contended that if the interception was carried out in accordance with the warrant then the court must conclude that what occurred was the National Crime Agency requesting or requiring the JIT "to carry out the interception of the 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." As such the activity was subject to the provisions of section 9 of the 2016 Act and a Targeted Interception warrant should have been in place. The judge rejected this submission: the National Crime Agency could not require the French authorities to undertake Operation Emma and had not requested them to do so. They were intent on pursuing it and would have executed it any event. They implanted malware in all EncroChat devices wherever they were located. This would affect devices in the United Kingdom. A "request" to do this was unnecessary, and none was made. In addition, on its proper construction, the judge held that section 9 of the 2016 Act was only applicable to requests for the interception of material and not to equipment interference, therefore it was of no application to the present case.

31. The judge also rejected the further alternative contention by the appellants that the provisions of section 10 and therefore section 56(2)(c) of the 2016 Act were engaged in the present case. The European Investigation Order was not requesting assistance in relation to communications but rather seeking "information already in the possession of the executing authority" on the basis that the French authorities were going to undertake the operation in any event. The judge also ruled that the scope of section 10(2) could not be narrowed to permit the defence interpretation that this only applied to a court order.

32. The judge ruled that the EncroChat data were admissible evidence and that the exclusionary provisions of section 56 of the Act did not apply. There had been detailed argument about what the position would be were the court to find that the data fell within section 4(4)(a) of the Act. The appellants submitted that there would have been an offence under section 3(1) of the Act, that section 56(2)(a) would apply and the EncroChat material would be inadmissible. The prosecution submitted that such an offence would not have been committed as the interception had not been "carried out in the United Kingdom" as required by section 3(1)(b) of the 2016 Act, given that by section 4(8) this required that the relevant act be "carried out by conduct within the United Kingdom." The judge rejected the appellants' submissions. He ruled that it was necessary to pay close attention to the language used in section 4 to define the term "interception" and in particular the definition of when interception was to be considered as having been carried out in the United Kingdom for the purpose of the definition set out in section 4(8)(a). This requires "conduct within the United Kingdom" by which the relevant act is "carried out". The judge described this as a "bespoke" definition,

which he contrasted with the approach taken to the place where conduct occurs for the purposes of determining the geographical jurisdiction of the criminal court. He held that the relevant conduct in this case, namely the modifying or interference with the EncroChat system, occurred in France when action was taken there which affected the servers which were also there.

The challenge on appeal

33. The appellants have jointly lodged Grounds of Appeal. They challenge four rulings by the judge, complaining that each of these rulings was wrong. They are:

> "(1) The ruling that the EncroChat communications were not intercepted while they were being transmitted (within s4(4)(a) of the 2016 Act), but were intercepted while they were stored before or after transmission, (within the definition of s4(4)(b).
>
> (2) The ruling that, in the alternative to (1), s56(2)(a), (relating to the offence under s3 of the 2016 Act), could not apply, because the interceptions were not carried out by conduct in the UK, as defined by s4(8) of the Act.
>
> (3) The ruling that s56(2)(c), relating to the restriction on requesting mutual assistance in s10 of the Act, does not apply, because the European Investigation Order made no request that fell within s10(1)(a) or, in the alternative, the request in the EIO was the exercise of a statutory power for the purposes of s10(2A).
>
> (4) The ruling that s56(2)(b), relating to the prohibition on an overseas authority to carry out the interception of communications imposed by s9 of the 2016 Act, did not apply because the JIT's activity, while 'in accordance with the Targeted Equipment Interference warrant' was nevertheless not pursuant to a request by UK authorities to carry out the interception."

The submissions of the parties on the appeal

The appellants

34. Mr. Ryder on behalf of all appellants for the purposes of this appeal set out a series of factual propositions which we summarise:

i) The interceptions were effected by malware which was implanted onto phones in the United Kingdom. They were being used entirely to communicate with other phones in the United Kingdom. The Targeted Equipment Interference warrants and the European Investigation Order were all in force before the interception started. There was a delay between the transmission of the message and its receipt by the NCA which was sometimes a few hours, sometimes much less and sometimes as short as 20 minutes. There were admissions about this before the judge, which we have seen.

ii) It is not known when or how the malware extracted the messages. There was no evidence about this. No-one who gave evidence knew exactly how the malware works, and the French authorities were concerned that this should continue to be the case. He said that the burden of the evidence was that the communications were extracted from the RAM of the devices. In the case of the sender this was probably after the user had pressed "Send". In the case of the recipient it was after the message had arrived on the machine but before the recipient was able to view it. He provided us with references to the evidence to make this good.

iii) The Targeted Equipment Interference warrant was obtained and approved by the Investigatory Powers Commissioner because the National Crime Agency was concerned that otherwise there was a risk that it would be complicit in an offence under the Computer Misuse Act 1990.

35. Relying on the agreed position of the parties that section 4(4) should be construed as meaning that if a communication was "being transmitted" it could not be "stored by or in the system" at the same time, Mr. Ryder submitted that the expert evidence meant that the communications were extracted while being transmitted and could not therefore be "stored" within section 4(4)(b). He complained that the judge's ruling does not define when transmission begins and ends. He described the approach of the judge as being that if the communication came from RAM then it was being stored and not transmitted. He said that transmission must start when the user presses "send" and ends when the communication is accessible by a human recipient. It is not accessible by a human recipient when it is in RAM. Precisely when transmission begins and ends will depend on the nuances of the system.

36. Mr. Ryder then identified what he called "Five Steps" to his argument, although with respect to him, they can be condensed a little. The points he made appeared to us to be these:

i) He reviewed cases decided under previous statutory regimes, which are summarised in *R v. Coulson* [2014] 1 WLR 1119, and *Coulson* itself. These were not only decided under different regimes, but also concerned different forms of communication, quite commonly telephone calls.

ii) Then he took us to the European Directives discussed at paragraphs [29]-[43] of *Coulson*. As the court there observed, the Directives include material, including Recitals 22 and 27, which seek to define their objective and include some material which may assist.

iii) Mr. Ryder criticised the passage in paragraph 153 of the judge's ruling set out above which, he said, showed that the judge had no clear definition of transmission. His observation that the communications were not taken when the message was being transmitted from the sender's device to that of the receiver appeared to suggest that he adopted a definition of "transmission" which was inconsistent with the authorities. He argued that it has never been held that "transmission" starts only when the communication leaves the sending device by means of its "transmitter". He also submitted that the judge had regarded the length of time when the communication might be in RAM as relevant, when it

is not, and had in any event not fully reflected the evidence which was given on that question.

iv) As appears from paragraphs 148 and 153 of the ruling the judge concluded that the application of a nickname to the communication by the receiving phone must mark a point by which transmission had ended. That is because the nickname is not part of the communication and is held in the database of the receiving phone. It is applied to the communication by processing while the communication is in RAM. Mr. Ryder took us through the expert evidence on this issue which was largely dealt with in cross-examination of Mr. Campbell by Mr. Kinnear. The point is made that in the case of a telephone call, the name of the caller appears on the recipient's screen before the call starts. It is suggested that the judge gave too much weight to this point which, in truth, was irrelevant.

37. We have set out a summary of Mr. Ryder's oral submissions, and we also have in mind the way in which the arguments were presented before the judge and in writing before us.

38. By Ground 2, Mr. Ryder submitted that the judge erred in identifying a "bespoke" or exceptional interpretation of the word "conduct" in section 4(8) of the 2016 Act which is inconsistent with its established meaning in common law and how it should be interpreted in relation to criminal offences. He relied on the speech of Lord Hope in *Office of the King's Prosecutor, Brussels v. Cando Armas and another* [2006] 2 AC 1 at paragraph [30] in support of his submission that the phrase "conduct within the United Kingdom" found in section 4(8)(a) of the 2016 Act should be construed to include conduct whose impact was felt in the United Kingdom, even if it was actually carried out entirely abroad. He submitted that otherwise a phone hacker could simply travel to France to listen to the stored messages (taking the facts of *Coulson* as an example) and avoid criminal liability.

39. Mr. Ryder and Mr. Bowers Q.C., on behalf of C, both made submissions about Ground 3, which concerns the application of section 10 of the 2016 Act, which is set out in the Appendix at paragraph 5. The first submission is that the European Investigation Order was a request for assistance under an EU mutual assistance instrument for assistance in connection with, or in the form of, the interception of communications. It is suggested that this is a broad definition and that the judge was wrong to hold that the European Investigation Order was not such a request because the French authorities were going to implement the interception anyway, and because the request was not for interception but for its product. In relation to the exclusion from the requirement for a Part 2 warrant which appears in sub-section (2A), they submitted that the Prosecution had first suggested that the Targeted Equipment Interference warrant was the statutory power and that this was a concession for the purposes of Ground 3. They also submitted that the judge's ruling that the statutory power was the power to make or designate a European Investigation Order under regulation 7 of the 2017 Regulations involved circularity and, for that reason, must be wrong. Mr. Bowers made a supporting submission, relying in particular on the close way in which the National Crime Agency worked with the JIT on this process.

40. By Ground 4 the appellants contend that the prohibition on an overseas authority carrying out the interception of communications imposed by section 9 of the 2016 Act

(Appendix at paragraph 5) did apply because the JIT's activity, "in accordance with" a Part 5 warrant, must inevitably have been pursuant to a request by United Kingdom authorities to carry out the interception. The request was the warrant with which the French authorities complied. They suggest that the judge erred in approaching the question of law under section 9 of the 2016 Act, namely whether the JIT had carried out the interceptions pursuant to a request from United Kingdom authorities, by giving particular weight to the suggestion that the JIT would have carried out the interceptions in the United Kingdom "in any event." His analysis is said to have misinterpreted the legal status of the Targeted Equipment Interference warrant. It is inherent in this submission that the 2016 Act created two different regulatory schemes for the same conduct, one by section 9 and the other by section 10. It is submitted that both schemes must be complied with. The section 9 scheme requires a warrant under Part 2, even in a case where section 10(2A) says that none is necessary.

The Prosecution

41. Mr. Kinnear took his submissions in a different order, and we will set them out in summary in the order he chose.

42. His first submission was that the prohibition on disclosure and the deployment of evidence in section 56(1) of the 2016 Act does not apply to equipment interference warrants at all. In advancing that submission he also set out his response to Grounds 2-4.

43. He submitted that even if the communications were taken by the French while they were "being transmitted", this did not amount to interception-related conduct as defined in section 56(2) of the 2016 Act. He supported this by a review of the 2016 Act and its Codes of Practice which, he said, showed that the Part 2 regime deals with "interception of communications" and Part 5 with "equipment interference". What was done in this case, whether it was interception or not, was done by equipment interference. He submitted that this involves a different regime under the legislation, which is outside the exclusionary rule in section 56, and which has no equivalent provision. He said that section 56 contains no reference to Part 5 or to section 99 and clearly relates to the warrants which may be issued under section 15 of the 2016 Act. He summarised the two different regimes by describing the section 15 regime as "old school" interception, which was to be contrasted with interception by equipment interference.

44. The Prosecution submitted that nothing done in this case by the National Crime Agency could amount to an offence under section 3(1) of the 2016 Act because the National Crime Agency neither perpetrated nor encouraged any conduct in the United Kingdom. The common law was varied by the clear terms of section 4(8) of the 2016 Act which require:

    i) a relevant act;

    ii) which is carried out by conduct within the United Kingdom; and

    iii) in the case of a public telecommunications system, that it is located in the United Kingdom, see section 261(8) and (9) at Appendix paragraph 9.

45. The "relevant act" is the modification of the system, including any wireless telegraphy apparatus used for making transmissions to or from apparatus that is part of the system. That may occur anywhere, as long as it involved a telecommunication system located in the United Kingdom, which provides a service to the public in any one or more parts of the United Kingdom. It only falls within the jurisdiction of the United Kingdom if it is carried out by conduct within the United Kingdom. If the location of "conduct" is determined in the way described by Lord Hope in *Cando Armas* then the requirement for it would add nothing to the definition of "relevant act".

46. It was further submitted that the National Crime Agency never sought any "intercept material" and could not be guilty of intentionally encouraging the JIT to procure and supply it. They believed at all times that the material was Targeted Equipment Interference material.

47. In relation to Ground 4, dealing with section 9 of the 2016 Act, Mr. Kinnear submitted that it clearly only applies to Part 2 warrants for "old school" intercept. The requirement for mutual assistance warrants appears only in section 15 of the 2016 Act (Part 2 warrants) and not in section 99 (Part 5 warrants). Section 9 is to be construed as limited to cases where a warrant under section 15 is required. The judge accepted this submission as his third reason for holding that section 9 did not apply to this case. If it is right as a matter of statutory construction it is not necessary to consider his first two reasons.

48. In relation to Ground 3, the operation of section 10 of the 2016 Act, the prosecution submitted that the judge was right. They seek to support paragraph 168 of the ruling which said:

> "The defendants contend that it is important to focus upon the use of the words "in connection with, or in the form of, the interception of communications" in section 10(1) of the 2016 Act. In their submission this formulation contemplates a breadth to the application of this section which would bring the EIO within the scope of the application of section 10, on the basis that the EIO was at the very least a request "in connection with" the interception of communications. I am not satisfied that this phrase is capable of interpretation so as to effectively include within the scope of the section what are in truth requests for the data obtained from an interception after it has occurred, and which the issuing authority has not requested and over which it has no control. A perusal of the nature of the questions contained within section H7 of the prescribed form, which call for details of the purpose, duration and technical data involved in a requested interception, provide some support for this approach. In my view there is force in the prosecution submissions that this phrase relates to the kinds of ancillary information where interception is being requested covered by article 30 of the Directive (the article of the Directive which deals with the interception of telecommunications with the technical assistance of another Member State) and in particular article 30(7) as follows:

> "30(7) When issuing an EIO referred to in paragraph 1 or during the interception, the issuing authority may, where it has a particular reason to do so, also request a transcription, decoding, or decrypting of the recording subject to the agreement of the executing authority.""

49. In the alternative, the judge correctly held that the National Crime Agency issued the European Investigation Order acting under regulation 7 of the 2017 Regulations and so section 10(2A) removed the requirement for any additional warrant which would otherwise have arisen by virtue of section 10(2).

50. Moving finally to Ground 1, Mr. Kinnear relied on paragraph 2 of Schedule 3 to the Act to permit the admissibility of the material because it had been lawfully obtained under section 6(1)(c) because a Targeted Equipment Interference warrant was in place and the JIT and the National Crime Agency acted in accordance with that warrant. He rejected the submission that a communication might be in the process of transmission forever if the recipient threw away the mobile phone (as Mr Ryder submitted), or lost the ability to access an email account. It could not depend upon whether the particular recipient had the ability to access the message once it had arrived. He submitted that the short answer to the appeal is that the messages were not intercepted after they had left the transmitting phone or before they arrived on the receiving phone. They had been extracted when they were stored on those phones.

Discussion and decision

51. The critical issue which falls for decision is the issue of the construction of section 4(4) of the 2016 Act. Given that our starting point is the agreement between the parties that the handsets are part of the public telecommunications system, the issue is whether the communications were intercepted while they were being transmitted or while they were stored in or by the system. Before embarking on that central issue, we must first deal with the Crown's first submission that there was no interception-related conduct at all, summarised at paragraphs [41]-[45] above. The judge agreed with this proposition, and dealt with it as a fallback position, in case he was wrong to find that the communications were stored in or by the system for the purposes of section 4(4)(b).

52. It is an important part of that submission that the events which occurred in this case did not involve, and could not have involved, an offence contrary to section 3(1) of the 2016 Act because the relevant act (modifying or interfering with the system) was not carried out by conduct within the United Kingdom, see section 4(2) and (8) of the 2016 Act. This is an argument which arises under Ground 2 but is also essential to the submission presently under consideration. That is because if no offence could be committed for this reason then admitting the evidence would not disclose that the origin of the intercepted communication was "interception-related conduct". It would not be conduct by a person within section 56(3) which was, "or in the absence of any lawful authority would be, an offence under section 3(1)", see section 56(2)(a). Equally, the Crown submitted, the EncroChat material does not disclose any breach of section 9 or 10 which otherwise would amount to interception-related conduct because of section 56(2)(b) and (c).

53. We do not need to determine whether the judge was right to uphold the Crown's submission that Targeted Equipment Interference warrants, when they relate to

communications, fall outside the exclusionary rule in section 56(1) of the 2016 Act. We see the force in the points which are made, but there is a directly relevant statutory provision which supports a contrary view, and in any event if the Crown succeeds on Ground 1 that provides an unassailable route to admissibility. Paragraph 2 of Schedule 3 sets out an exception to the exclusionary rule in section 56(1), and the two provisions have to be read together. The submission that that exception in relation to material which has been lawfully obtained under section 6(1)(c) is to be treated as a "belt and braces" provision is not without difficulty. That would mean that the exception is unnecessary because such material would be admissible without it. It is true that in very complex statutes such as the 2016 Act it is sometimes possible to find anomalous provisions which appear to be unnecessary, but the conclusion that they are should be a last resort when all attempts to give a meaning to the language chosen by Parliament have failed. In view of our conclusion in relation to Ground 1, to which we next turn, it is unnecessary to decide the issue concerning the scope of the section 56 exclusionary rule and further we consider that it would be far better for that potentially complex question to be decided in a case where it is truly necessary to the outcome.

Ground 1: s4(4)(b)

54. On this approach, the admissibility of the material depends upon whether it falls within section 4(4)(b), because it was intercepted at a time when it was stored in or by the system (whether before or after transmission).

55. We do not accept that this issue requires a minute examination of the inner workings of every system in every case. Parliament has not chosen to define the "relevant time" when interception takes place by reference to whether the communication is in the RAM of the device at the point of the extraction, or whether it is in its permanent storage database, or by any other technical definition. Given the speed at which technology changes, both concepts may become obsolete or be superseded. The statutory scheme must work whatever the technical features of the system in question. The words used are ordinary English words: "transmission" and "stored". The "system" is also defined in non-technical language. The task of the court, as the judge correctly said, is to understand the system and then to decide whether, as a matter of ordinary language, the communication was being transmitted or stored at the time of extraction. If the former, it is inadmissible. If the latter, it is admissible, provided the appropriate warrant was in place. On the findings of the judge the appropriate warrant was in place and the extraction was carried out in accordance with it.

56. We do not consider that any of the previous decisions of the court assist in this exercise. They were all decided under different statutory regimes. There are important differences between the provisions concerning stored material in section 2(7) of the Regulation of Investigatory Powers Act 2000 and in section 4 of the 2016 Act. The lack of any limitation on the exception created by section 4(4)(b) in relation to stored material is significant. That change, in our judgment, is relevant to the construction of section 4 of the 2016 Act. Perhaps unsurprisingly, the 1985 Act contained no reference to stored material, and no definition of "transmission" at all. In 1985 the legislature was not concerned with modern telecommunications systems and the principal focus was on telephone calls. Cases decided under that regime are of no assistance. The legislation has since had to address Council Directive 97/66/EC and Council Directive 2002/58/EC and technical developments both in the systems and in the means used to

intercept communications. The 2016 Act is a new statute, on which there is no relevant authority and its construction must be approached in that way.

57. Both parties cited *Coulson* in which the Court of Appeal said that section 2(7) of the 2000 Act was "at the heart of [that] appeal". This provided:

> "For the purposes of this section the times while a communication is being transmitted by means of a telecommunication system shall be taken to include any time when the system by means of which the communication is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it."

58. The 2016 Act, as we have said, adopted a framework in which some components are similar to those in the 2000 Act. Section 1 of the 2000 Act was the offence creating provision which criminalised the interception of communications in the course of their transmission by a telecommunications system. Section 17 was the provision which excluded the product of interception from disclosure or evidence. Like section 4 of the 2016 Act, section 2 of the 2000 Act dealt with the meaning and location of "interception". The language, so far as stored communications are concerned, is significantly different.

59. Section 2(7) of the 2000 Act makes it clear, among other things, that the storage which it describes can be occurring at the same time as the communication is "being transmitted". It also limits the concept of "storage" to storage "in a manner which enables the intended recipient to collect it or otherwise have access to it". Section 4(4) does not repeat this limitation, although Mr. Ryder suggested that transmission only ends when the recipient actually accesses the communication. In section 4(4), unlike section 2(7), all forms of storage are caught, whether or not they enable the intended recipient to access the communication. Further, section 2(7) of the 2000 Act is a "deeming provision". The time when a communication is being transmitted is taken to include times when that communication is also being stored in a relevant manner; by contrast, section 4(4) is not a deeming provision. Finally, the scheme of the 2000 Act so far as warrantry is concerned is entirely different and the word "stored" appears in the 2016 Act in various places which have no equivalent in the 2000 Act and is serving more purposes than it did in that Act.

60. The answer to this appeal is found in the construction of section 4(1) and (4)(4)(b) of the 2016 Act. Section 4(4)(b), read beside section 4(1)(b), means that a message which is, for example, monitored while it is stored in or by the system by means of which it is transmitted is intercepted while it is in the course of transmission. To hold that this only applies if the message is stored "in a manner that enables the intended recipient to collect it or otherwise to have access to it" would be to read words into the 2016 Act which had appeared in the 2000 Act but which Parliament deliberately omitted. That is a reading of section 4(4)(b) which is obviously quite unarguable. It is, however, essential to the appellants' argument on Ground 1. That became explicit when Mr. Ryder was dealing with storage on the handset of the recipient, in the context of the judge's approach to the "nickname" issue. It also explains why he was driven to submit that a communication would be in the course of transmission forever if, for example, it were sent to an email address to which the intended recipient no longer had access

because he or she had forgotten the password. That does unnecessary violence to the expression "being transmitted" which is not required by the 2016 Act.

61. Section 4(4)(b) extended the types of storage which amount to being in "the course of transmission" so as to catch communications which are "stored" for the purposes of the offence creating provision, to which the distinction between section 4(4)(a) and 4(4)(b) is immaterial. The importance of the distinction lies in the warrantry which is required, and in the admissibility of the product of lawfully obtained communications. The structure of section 4(4) is important here. The conjunction which connects section 4(4)(a) and 4(4)(b) is "and" not "or". The appellants' submission that the court must start with section 4(4)(a) and determine whether a message was intercepted while being transmitted and, if the answer to that is yes, cannot then go on to consider whether it was also, at the same time, being stored is simply wrong. The words in the parenthesis of section 4(4)(b) do not require that conclusion. They simply mean that it does not matter whether the storage began before or after the transmission. It is unnecessary to add any words there to catch storage while the communication is being transmitted because that is necessarily caught by the plain words of the provision.

62. As a matter of ordinary language, section 4(4)(b) is clear and unambiguous in its meaning. It extends to all communications which are stored on the system, whenever that might occur. That broad meaning coheres with the structure of the 2016 Act considered in overview, and importantly with the different types of warrantry for which the Act provides. Part 5 warrants are required for the interception of stored material, and Part 2 warrants for material which is to be intercepted while being transmitted. It also advances the overall purpose of the legislation in preserving the legislative framework – and the distinction between the different types of intercept – to which we have referred. The statutory question for any court in determining if section 4(4)(b) applies is this: was the communication stored in or by the system at the time when it was intercepted?

63. The judge's findings of fact are set out above. He found that the communications were extracted directly from the handset of the user and not while they were travelling to, through or from any other part of the system. This is a process which is like any other means of downloading the content of a mobile phone handset. It is done remotely, but it is done by interrogating the RAM of the phone, not by intercepting the communication after it has left the phone. In the case of the sender the material was recovered in the form of unencrypted messages stored in the RAM of the device in a form in which they existed before they were transmitted from the device to the servers in Roubaix, via the telecommunications system. This provides the answer to the statutory question. The material was stored when it was intercepted. It was within section 4(4)(b).

64. Given this conclusion on the meaning of "stored" it is not necessary to define exactly when transmission starts and ends. We do not accept that transmission of the communication started when the user pressed "Send". That was an action which caused the device to prepare the message in its final form and then to initiate the process of transmission. A mobile phone is a computer and a transmitter. Transmission takes place after the communication has been put into its final form by the computer. In the present case that includes the encryption. That takes place after the user presses "Send", but before the message is transmitted by the device. On receipt by the recipient's device it is decrypted in the RAM and it may be that in some cases a nickname is added to that

which has been transmitted which is stored in the Realm database on that device. We consider that the transmission is complete when the communication arrives on the receiving device so that the device can begin work decrypting it and making it legible. Even in this unusual type of system, the transmission occurs, in relation to each communication, when a device is in contact with the rest of the system for the purpose of sending or receiving a communication, and when the communication is travelling through other parts of the system.

65. The judge's key finding of fact was set out in the passage of his ruling which we have underlined in our paragraph [14] above.

66. We agree with the judge. The communication is that which is transmitted. What remains on the device is not what has been transmitted, but a copy of it or what, in older forms of messaging, might be described as a "draft". That is so however quickly after transmission the obtaining of the copy takes place, or even if the copy is extracted while the original encrypted communication is being transmitted. The fact that what was obtained was an unencrypted message, means that what was on the phone, and what was intercepted, was not the same as what had been transmitted because what had been transmitted was encrypted. It cannot therefore have been "being transmitted" when it was intercepted: it can only have been "being stored".

67. That being so, the harvesting was interception but was rendered lawful by the Targeted Equipment Interference warrants issued under section 99 of the Act. That is the effect of section 6(1)(c) of the Act. The product of that harvesting was thus rendered admissible in these proceedings by paragraph 2 of Schedule 3. Our conclusion is that the extracted communications were stored on the handsets. On the agreed basis that these formed parts of the public telecommunications system, the communications were stored in or by that system.

68. We have not found it necessary to set out in this judgment the expert evidence with which this conclusion is said to be inconsistent. The 2016 Act does not use technical terms in this area. The experts have an important role in explaining how a system works, but no role whatever in construing an Act of Parliament. They appear to have assumed that because a communication appears in the RAM as an essential part of the process which results in the transmission it did so while "being transmitted". That is an obvious error of language and analysis. It can be illustrated by considering the posting of a letter. The process involves the letter being written, put in an envelope, a stamp being attached and then the letter being placed in the post box. Only the last act involves the letter being transmitted by a system, but all the acts are essential to that transmission.

69. That being so, the judge's conclusion on the Ground 1 issue was right. If the EncroChat material was caught by the section 56 exclusion, it was admissible in evidence by this route. The communications were lawfully intercepted while stored on the handsets and are admissible by virtue of paragraph 2 of Schedule 3 to the 2016 Act.

Ground 2: section 4(8)

70. It is unnecessary to consider Ground 2 because that only arises if Ground 1 succeeds. The prosecution does not need its fallback argument in view of our conclusion on Ground 1.

Grounds 3 and 4: sections 10 and 9

71. It is necessary to say something about Grounds 3 and 4. If sections 9 or 10, or both, were breached by the National Crime Agency, then that would not affect the path to admissibility in section 6(1)(c) and paragraph 2 of Schedule 3. Compliance with sections 9 and 10 is not a statutory condition of admissibility by that route. It might, however, give rise to an argument that the material should be excluded pursuant to section 78 of the Police and Criminal Evidence Act 1984. It would be a surprising exercise of that power to exclude evidence which Parliament has provided in clear terms should be admissible, but we should nevertheless consider these Grounds.

Ground 3: section 10

72. Ground 3 relies on the prohibition in section 10 of the 2016 Act which is said to have been breached. It is said that the United Kingdom authorities made a request for assistance under an EU mutual assistance instrument in connection with the interception of communications when there was no mutual assistance warrant in being under Chapter 1 of Part 2 authorising the making of that request. That would be a breach of section 10(2) of the Act. The judge rejected that submission, holding that since the JIT was intending to proceed whatever the United Kingdom authorities did, there was no request for any interception, only for the product of it. We prefer not to base our conclusion on that finding. It appears to us that the European Investigation Order in this case was a request for assistance under an EU mutual assistance instrument which was "in connection with" the interception of communications. This is because of the statutory context of section 10(2A) which we describe below. Therefore, unless section 10(2A) applies what was done was done unlawfully because no Part 2 mutual assistance warrant was in place. If that were so, then the rule in section 56(1) and 56(2)(c) would apply and the evidence could not be adduced, unless it was admissible under paragraph 2 of Schedule 3 to the 2016 Act as we have held it was. The issue of unlawfulness turns on section 10(2A). The judge held under section 10(2A) of the Act that section 10(2) did not apply because the request which was made was made in the exercise of a statutory power. The judge concluded that the statutory power concerned was the power of a designated prosecutor to make or validate a European Investigation Order under regulation 7 of the 2017 Regulations.

73. The 2017 Regulations amended the 2016 Act by the addition of section 10(2A), see paragraph 9 of Schedule 3 to the 2017 Regulations. Regulation 59 designated the Directive relating to the European Investigation Order as an EU mutual instrument for the purposes of section 10 of the 2016 Act. It appears that the purpose of the 2017 Regulations and of section 10(2A) (described as a "consequential amendment") was precisely to incorporate the European Investigation Order system into United Kingdom domestic law. The Explanatory Memorandum to the 2017 Regulations says this:

> "2.1 The purpose of the Criminal Justice (European Investigation Order) Regulations 2017 ("the Regulations") is to give effect to Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130, 1.5.2014, p. 1) ("the Directive")."

74. It would be inconsistent with that purpose to construe section 10(1) and 10(2A) so narrowly as to remove from its scope a European Investigation Order of the sort issued in this case. The words used are "a request for assistance in connection with, or in the form of, interception of a communication stored in or by a telecommunications system" which are broad in their meaning. In this case, the European Investigation Order was made for the purpose of obtaining the results of interception of communications and that appears to us to be a request for assistance in connection with interception.

75. Just as this statutory context makes it impossible for the Prosecution to argue that the European Investigation Order was not a "request" for the purposes of section 10, in exactly the same way it makes it impossible for the appellants to contend that it was not "the exercise of a statutory power" for the purposes of section 10(2A). Section 10(2A) was enacted specifically to include European Investigation Orders. Ground 3 is without merit.

Ground 4: section 9

76. Ground 4 relies on the prohibition in section 9 of the 2016 Act against requesting interception without a Part 2 targeted interception or examination warrant being in place. There was no warrant of this kind, and unlike section 10, section 9 contains no provision dealing with communications which are stored in or by the system. The appellants therefore contend that activity which was rendered lawful by the clear terms of section 6(1)(c) and 10(2A) of the Act was rendered unlawful by section 9, which does not refer to stored communications at all. That would be an extraordinary outcome.

77. The judge dealt with the section 9 issue on the basis that there was, in fact, no request to carry out the interception of communications for broadly the same reasons as applied in relation to the section 10 issue. We do not consider it necessary to review the judge's determination of the facts. Whether he was right or wrong about this conclusion, he also ruled against the appellants as a matter of law on the construction of section 9. He said at paragraph 165:

> "……it is clear that on its proper construction, section 9 of the 2016 Act is applicable 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. Firstly, the reference to interception of communications in section 9 of the 2016 Act is a cross-reference to interception of communications governed by Part 2 and section 15 of the 2016 Act. This is reinforced by the reference in section 9(2) to the need for targeted interception warrants under Part 2 of the Act: the clear intention of this section is to prevent the circumvention of the regulation of Part 2 activity by the commissioning of overseas authorities to carry it out in the UK on behalf of the UK authorities. As set out above, the powers created by section 99 of the 2016 Act in relation to Targeted Equipment Interference material include obtaining assistance in relation to giving effect to the Targeted Equipment Interference warrant, and that provision is not limited in its geographical reach. To read section 9 as applying to conduct covered by a

> Targeted Equipment Interference warrant would cut across the breadth of the authority given under section 99(5), and would require the obtaining of a Targeted Interception warrant in relation to conduct involving Targeted Equipment Interference material. This would not sit well with the structure of the legislation which clearly provides separate regimes for Targeted Interception and Targeted Equipment Interference material."

78. We agree with the judge that 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. This was not such a case.

Conclusion

79. We have concluded that the only substantial question which the judge was required to answer was whether the EncroChat material was stored by or in the telecommunications system when it was intercepted. Like him, we consider that these communications were not being transmitted but stored at that time. That being so, the appeal is dismissed.

APPENDIX: STATUTORY PROVISIONS FROM INVESTIGATORY POWERS ACT 2016

1. The scheme is described in this Appendix so far as it relates to public telecommunications systems.

2. Section 3 makes it an offence to intercept a communication in the course of its transmission by a public telecommunications system, if the interception is carried out in the United Kingdom and it is done without lawful authority.

> **3 Offence of unlawful interception**
>
> (1) A person commits an offence if—
>
> (a) the person intentionally intercepts a communication in the course of its transmission by means of—
>
> (i) a public telecommunication system,
>
> (ii) a private telecommunication system, or
>
> (iii) a public postal service,
>
> (b) the interception is carried out in the United Kingdom, and
>
> (c) the person does not have lawful authority to carry out the interception.
>
> …….
>
> (3) Sections 4 and 5 contain provision about—
>
> (a) the meaning of "interception", and
>
> (b) when interception is to be regarded as carried out in the United Kingdom.
>
> (4) Section 6 contains provision about when a person has lawful authority to carry out an interception.
>
> (5) For the meaning of the terms used in subsection (1)(a)(i) to (iii), see sections 261 and 262.
>
> …….

3. Section 4 defines interception and some other terms. So far as relevant it provides:

> **4 Definition of "interception" etc.**
>
> Interception in relation to telecommunication systems

(1) For the purposes of this Act, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if—

(a) the person does a relevant act in relation to the system, and

(b) the effect of the relevant act is to make any content of the communication available, at a relevant time, to a person who is not the sender or intended recipient of the communication.

For the meaning of "content" in relation to a communication, see section 261(6).

(2) In this section "relevant act", in relation to a telecommunication system, means—

(a) modifying, or interfering with, the system or its operation;

(b) monitoring transmissions made by means of the system;

(c) monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system.

(3) For the purposes of this section references to modifying a telecommunication system include references to attaching any apparatus to, or otherwise modifying or interfering with—

(a) any part of the system, or

(b) any wireless telegraphy apparatus used for making transmissions to or from apparatus that is part of the system.

(4) In this section "relevant time", in relation to a communication transmitted by means of a telecommunication system, means—

(a) any time while the communication is being transmitted, and

(b) any time when the communication is stored in or by the system (whether before or after its transmission).

(5) For the purposes of this section, the cases in which any content of a communication is to be taken to be made available to a person at a relevant time include any case in which any of the communication is diverted or recorded at a relevant time so as to make any content of the communication available to a person after that time.

(6) In this section "wireless telegraphy" and "wireless telegraphy apparatus" have the same meaning as in the Wireless Telegraphy Act 2006 (see sections 116 and 117 of that Act).

Interception in relation to postal services

(7)…….

Interception carried out in the United Kingdom

(8) For the purposes of this Act the interception of a communication is carried out in the United Kingdom if, and only if—

(a) the relevant act or, in the case of a postal item, the interception is carried out by conduct within the United Kingdom, and

(b) the communication is intercepted—

(i) in the course of its transmission by means of a public telecommunication system or a public postal service, or

(ii) in the course of its transmission by means of a private telecommunication system in a case where the sender or intended recipient of the communication is in the United Kingdom.

4. Section 6 defines "lawful authority". The key provision for this case is 6(1)(c), which provides that interception of stored communications (to which s4(4)(b) applies) under a Part 5 warrant is lawful. Paragraph 2 of Schedule 3 below renders product within that category admissible by excluding it from section 56.

6. Definition of "lawful authority"

(1) For the purposes of this Act, a person has lawful authority to carry out an interception if, and only if—

(a) the interception is carried out in accordance with—

(i) a targeted interception warrant or mutual assistance warrant under Chapter 1 of Part 2, or

(ii) a bulk interception warrant under Chapter 1 of Part 6,

(b) the interception is authorised by any of sections 44 to 52, or

(c) in the case of a communication stored in or by a telecommunication system, the interception—

(i) is carried out in accordance with a targeted equipment interference warrant under Part 5 or a bulk equipment interference warrant under Chapter 3 of Part 6,

(ii) is in the exercise of any statutory power that is exercised for the purpose of obtaining information or taking possession of any document or other property, or

(iii) is carried out in accordance with a court order made for that purpose.

(2) …….

(3) …….

5. Sections 9 and 10 impose restrictions on requesting interception by overseas authorities, and on requesting assistance under mutual legal assistance agreements. The principle is that such requests must be authorised by appropriate warrants in accordance with the scheme of the Act.

9 Restriction on requesting interception by overseas authorities

(1) This section applies to a request for any authorities of a country or territory 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.

(2) A request to which this section applies may not be made by or on behalf of a person in the United Kingdom unless—

(a) a targeted interception warrant has been issued under Chapter 1 of Part 2 authorising the person to whom it is addressed to secure the interception of communications sent by, or intended for, that individual, or

(b) a targeted examination warrant has been issued under that Chapter authorising the person to whom it is addressed to carry out the selection of the content of such communications for examination.

10 Restriction on requesting assistance under mutual assistance agreements etc.

(1) This section applies to—

(a) a request for assistance under an EU mutual assistance instrument, and

(b) a request for assistance in accordance with an international mutual assistance agreement

so far as the assistance is in connection with, or in the form of, the interception of communications.

(2) A request to which this section applies may not be made by or on behalf of a person in the United Kingdom to the competent authorities of a country or territory outside the United Kingdom unless a mutual assistance warrant has been issued under Chapter 1 of Part 2 authorising the making of the request.

(2A) Subsection (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 telecommunication system if the request is made—

(a) in the exercise of a statutory power that is exercised for the purpose of obtaining information or taking possession of any document or other property, or

(b) in accordance with a court order that is made for that purpose.

(3) In this section—

"EU mutual assistance instrument" means an EU instrument which—

(a) relates to the provision of mutual assistance in connection with, or in the form of, the interception of communications,

(b) requires the issue of a warrant, order or equivalent instrument in cases in which assistance is given, and

(c) is designated as an EU mutual assistance instrument by regulations made by the Secretary of State;

"international mutual assistance agreement" means an international agreement which—

(a) relates to the provision of mutual assistance in connection with, or in the form of, the interception of communications,

(b) requires the issue of a warrant, order or equivalent instrument in cases in which assistance is given, and

(c) is designated as an international mutual assistance agreement by regulations made by the Secretary of State.

6. The rule against admissibility in court proceedings is found in section 56 and schedule 3 to the Act.

> **56 Exclusion of matters from legal proceedings etc.**
>
> (1) No evidence may be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings or Inquiries Act proceedings which (in any manner)—
>
> (a) discloses, in circumstances from which its origin in interception-related conduct may be inferred—
>
> (i) any content of an intercepted communication, or
>
> (ii) any secondary data obtained from a communication, or
>
> (b) tends to suggest that any interception-related conduct has or may have occurred or may be going to occur.
>
> This is subject to Schedule 3 (exceptions).
>
> (2) " Interception-related conduct " means—
>
> (a) conduct by a person within subsection (3) that is, or in the absence of any lawful authority would be, an offence under section 3(1) (offence of unlawful interception);
>
> (b) a breach of the prohibition imposed by section 9 (restriction on requesting interception by overseas authorities);
>
> (c) a breach of the prohibition imposed by section 10 (restriction on requesting assistance under mutual assistance agreements etc.);
>
> (d) the making of an application by any person for a warrant, or the issue of a warrant, under Chapter 1 of this Part;
>
> (e) the imposition of any requirement on any person to provide assistance in giving effect to a targeted interception warrant or mutual assistance warrant.
>
> (3) The persons referred to in subsection (2)(a) are—
>
> (a) any person who is an intercepting authority (see section 18);
>
> (b) any person holding office under the Crown;

(c) any person deemed to be the proper officer of Revenue and Customs by virtue of section 8(2) of the Customs and Excise Management Act 1979;

(d) any person employed by, or for the purposes of, a police force;

(e) any postal operator or telecommunications operator;

(f) any person employed or engaged for the purposes of the business of a postal operator or telecommunications operator.

(4) Any reference in subsection (1) to interception-related conduct also includes any conduct taking place before the coming into force of this section and consisting of—

(a) conduct by a person within subsection (3) that—

(i) was an offence under section 1(1) or (2) of the Regulation of Investigatory Powers Act 2000 ("RIPA"), or

(ii) would have been such an offence in the absence of any lawful authority (within the meaning of section 1(5) of RIPA);

(b) conduct by a person within subsection (3) that—

(i) was an offence under section 1 of the Interception of Communications Act 1985, or

(ii) would have been such an offence in the absence of subsections (2) and (3) of that section;

(c) a breach by the Secretary of State of the duty under section 1(4) of RIPA (restriction on requesting assistance under mutual assistance agreements);

(d) the making of an application by any person for a warrant, or the issue of a warrant, under—

(i) Chapter 1 of Part 1 of RIPA, or

(ii) the Interception of Communications Act 1985;

(e) the imposition of any requirement on any person to provide assistance in giving effect to a warrant under Chapter 1 of Part 1 of RIPA.

(5) In this section—

"Inquiries Act proceedings" means proceedings of an inquiry under the Inquiries Act 2005;

"intercepted communication" means any communication intercepted in the course of its transmission by means of a postal service or telecommunication system.

7. Schedule 3 to the Act contains a number of exceptions to the operation of the exclusionary rule in section 56(1) in certain classes of proceedings.

SCHEDULE 3

Exceptions to section 56

Introductory

1 This Schedule contains—

(a) exceptions to the exclusion by section 56(1) of certain matters from legal proceedings, and

(b) limitations on those exceptions where that exclusion will still apply.

Disclosures of lawfully intercepted communications

2 (1) Section 56(1)(a) does not prohibit the disclosure of any content of a communication, or any secondary data obtained from a communication, if the interception of that communication was lawful by virtue of any of the following provisions—

(a) sections 6(1)(c) and 44 to 52;

(b) sections 1(5)(c), 3 and 4 of the Regulation of Investigatory Powers Act 2000;

(c) section 1(2)(b) and (3) of the Interception of Communications Act 1985.

(2) Where any disclosure is proposed to be, or has been, made on the grounds that it is authorised by sub-paragraph (1), section 56(1) does not prohibit the doing of anything in, or for the purposes of, so much of any proceedings as relates to the question whether that disclosure is or was so authorised.

8. Section 99 in Part 5 of the Act deals with the kind of warrants which were granted in this case, a Targeted Equipment Interference warrant. It is as follows:-

> **99 Warrants under this Part: general**
>
> (1) There are two kinds of warrants which may be issued under this Part—
>
> (a) targeted equipment interference warrants (see subsection (2));
>
> (b) targeted examination warrants (see subsection (9)).
>
> (2) A targeted equipment interference warrant is a warrant which authorises or requires the person to whom it is addressed to secure interference with any equipment for the purpose of obtaining—
>
> (a) communications (see section 135);
>
> (b) equipment data (see section 100);
>
> (c) any other information.
>
> (3) A targeted equipment interference warrant—
>
> (a) must also authorise or require the person to whom it is addressed to secure the obtaining of the communications, equipment data or other information to which the warrant relates;
>
> (b) 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 paragraph (a).
>
> (4) The reference in subsections (2) and (3) to the obtaining of communications or other information includes doing so by—
>
> (a) monitoring, observing or listening to a person's communications or other activities;
>
> (b) recording anything which is monitored, observed or listened to.
>
> (5) A targeted equipment interference warrant also authorises the following conduct (in addition to the conduct described in the warrant)—
>
> (a) any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the warrant, including conduct for securing the obtaining of communications, equipment data or other information;

(b) 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.

(6) A targeted equipment interference warrant may not, by virtue of subsection (3), authorise or require a person to engage in 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).

(7) Subsection (5)(a) does not authorise a person to engage in conduct which could not be expressly authorised under the warrant because of the restriction imposed by subsection (6).

(8) In subsection (6), "stored communication" means a communication stored in or by a telecommunication system (whether before or after its transmission).

……..

(11) Any conduct which is carried out in accordance with a warrant under this Part is lawful for all purposes.

9. There are definition sections. In Part 5, section 135 defines, among other things "communications" for the purposes of that Part of the Act. Section 261 contains "telecommunications definitions". The definitions which may be relevant in this case are set out below.

261 Telecommunications definitions

(1) The definitions in this section have effect for the purposes of this Act.

Communication

(2) "Communication", in relation to a telecommunications operator, telecommunications service or telecommunication system, includes—

(a) anything comprising speech, music, sounds, visual images or data of any description, and

(b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus.

Entity data

……

Events data

……

Communications data

……

Content of a communication

(6) "Content", in relation to a communication and a telecommunications operator, telecommunications service or telecommunication system, means any element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but—

(a) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded, and

(b) anything which is systems data is not content.

Other definitions

……

(8) "Public telecommunications service" means any telecommunications service which is offered or provided to the public, or a substantial section of the public, in any one or more parts of the United Kingdom.

(9) "Public telecommunication system" means a telecommunication system located in the United Kingdom—

(a) by means of which any public telecommunications service is provided, or

(b) which consists of parts of any other telecommunication system by means of which any such service is provided.

……..

(13) "Telecommunication system" means a system (including the apparatus comprised in it) that exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy.

…….