Neutral Citation Number: [2023] UKIPTrib 3

Case No: **IPT/21/05/CH and ors**

IN THE INVESTIGATORY POWERS TRIBUNAL

Date: 11 May 2023

Before :

LORD JUSTICE EDIS
LADY CARMICHAEL
and
MR STEPHEN SHAW KC

- -

Between :

(1) SF
(2) DM
(3) PB
(4) CS
(5) KT
(6) KSS
(7) CP
(8) CC
(9) ME
(10) UB
(11) NA

Claimants

- and –

NATIONAL CRIME AGENCY **Respondent**

- -
- -

Abbas Lakha KC and Aneurin Brewer (instructed by Avisons Law) for the **1st, 2nd, 3rd, 4th and 5th Claimants**

Stephen Kamlish KC and Thomas Schofield (instructed by No5 Barristers Chambers) for the
6th Claimant
Matthew Ryder KC and Daniel Cashman (instructed by Carson Kaye Solicitors and Kenyon McAteer Solicitors) for the **7th, 8th and 9th Claimants**
Simon Csoka KC and Oliver Cook (instructed by Eldwick Law) for the **10th and 11th Claimants**

Sir James Eadie KC, David Perry KC, Victoria Ailes, Andrew Deakin, Richard O'Brien, and Natasha Barnes (instructed by **National Crime Agency**) for the **Respondent**
Jason Beer KC appeared as Counsel to the Tribunal

Hearing dates: 20-23 September 2022, 14-16 December 2022

- - - - - - - - - - - - - - - - - - - -

JUDGMENT

Lady Carmichael:

1. This is the judgment of the Tribunal to which all members have contributed. The Tribunal has conducted two closed hearings during the course of these proceedings. All of the conclusions in this judgment are based entirely on evidence and submissions presented in open proceedings. The Tribunal is issuing a separate written judgment in relation to the issues about legal professional privilege which were the subject of a ruling during the hearing on 14 December 2022.

Introduction

2. EncroChat was an encrypted communications platform. A joint investigative team ("JIT") of French and Dutch law enforcement agencies intercepted communications sent using EncroChat. It is common ground that this was "interception", as defined in UK law in section 4 of the Investigatory Powers Act 2016 ("IPA"). There is a dispute as to whether the communications intercepted were stored in or by a telecommunications system, or whether they were intercepted in the course of transmission. The distinction is important because of the different warrantry required for the interception of stored communications, and the different consequences for the admissibility of the product of that kind of interception in legal proceedings in the UK. The interception took place between 1 April and 11 June 2020.

3. On 22 January 2020 National Crime Agency ("NCA") and Crown Prosecution Service ("CPS") lawyers attended a Eurojust meeting in the Hague. They learned that French authorities had developed a capability to intercept communications on EncroChat. Between 19 and 21 February 2020 NCA officers attended a meeting at Europol relating to the interception of EncroChat communications.

4. The NCA wished to have access to the communications intercepted by the JIT. On 5 March 2020 a Judicial Commissioner approved a targeted equipment interference ("TEI") warrant under part 5 of the IPA. On 11 March 2020 the CPS served a European Investigation Order ("EIO") on French authorities asking for the product of the EncroChat interceptions. The Director General of the NCA sought revocation of the TEI warrant. This was because the warrant did not contain certain explanations as to the intended effect of the interceptions. A second TEI warrant was approved by Sir Brian Leveson, the Investigatory Powers Commissioner, on 26 March 2020. These proceedings are concerned with that warrant.

5. The Crown has sought to rely on material harvested from the EncroChat communication system in a number of prosecutions. A number of defendants have challenged the admissibility of that material on a number of bases, one of which was that it had been intercepted in the course of transmission. Material of that sort is not admissible by virtue of section 56(1) IPA. Those challenges have resulted in a number of preparatory hearings, some involving the hearing of evidence, and two decisions of the Criminal Division of the Court of Appeal: *ABD&C* v *R* [2021] EWCA Crim 128, reported as *R* v *A* [2021] QB 791; *R* v *A and others* [2021]

EWCA Crim 1447. Some of the criminal proceedings are subject to reporting restrictions. Although not all of the Claimants are defendants in cases in which there have been preparatory hearings, we have anonymised all of the Claimants in the interests of consistency and so that there is no need to restrict reporting of our conclusions.

6. This judgment is concerned with the following matters:

   (a) whether NCA failed in their duty of candour when they sought approval from the Judicial Commissioner, with the result that the warrant should be set aside;
   (b) whether the NCA required to obtain a mutual assistance warrant by reason of section 10, and whether the absence of such a warrant rendered the making of the EIO unlawful;
   (c) whether the NCA required to obtain a targeted interference warrant in order lawfully to acquire the EncroChat data, because of section 9;
   (d) whether the NCA required to obtain a bulk equipment interference warrant in order lawfully to obtain the EncroChat data.

7. In relation to (b), there is a preliminary issue as to the Tribunal's jurisdiction in so far as the Claimants allege a failure to comply with the requirements of section 10 of the IPA.

8. A number of other issues were raised before the Tribunal. Our approach is that we will determine the issues which require a decision from the Tribunal now. These are the issues identified at 6 above. Other issues have been canvassed where the Crown Court has concurrent jurisdiction with the Tribunal. Proceedings in relation to those issues are far advanced in the Crown Court, and it is not in the interests of justice for proceedings about the same matters to proceed in these different jurisdictions at the same time. We will address outstanding issues at the conclusion of the proceedings in the Crown Court. At that stage, we will be able to take into account the findings of the Crown Court, and the evidence adduced before it, in determining, among other things, whether any of the human rights claims advanced before the Tribunal succeed and, if so, what remedies are appropriate. Accordingly, we will give our decisions on the points identified in paragraph 6 above, and stay the rest of the proceedings with liberty to the parties to restore them once the Crown Court proceedings (including any further appeals) have resolved all issues concerning the admissibility of the product of the interception in this case.

9. At an earlier stage of these proceedings, the Tribunal made a case management decision to proceed without a trial of expert evidence, and to assume that the admissible expert evidence in reports by Professor Anderson as to the nature of the conduct involved in obtaining the material was correct. For the reasons that we give more fully below, we have relied on that assumption only in relation to one of the arguments presented to us.

10. For the reasons given at paragraphs 8, and 140-144 of this judgment, we have not made decisions about certain of the contentions that parties advanced at the hearing, namely whether the activity undertaken by the NCA was in accordance with the warrant granted, and an issue relating only to CP's case.

Summary of decision

11. For the reasons given below, we have reached the following conclusions.

    (a) The NCA did not fail in any material respect in fulfilling the duty of candour on them when seeking approval of the TEI warrant from the Judicial Commissioner.
    (b) The Tribunal does not have jurisdiction in relation to the question of whether the EIO was made lawfully.
    (c) The NCA did not require to obtain a targeted interference warrant.
    (d) The NCA did not require to obtain a bulk equipment interference warrant.

The IPA

12. Interception of communications which is not rendered lawful by the IPA is unlawful. The IPA provides for a range of warrantry that may render interception lawful. For the purposes of this judgment the relevant parts of the IPA are Part 1 (General Privacy Protections), Part 2 Chapter 1 (Interception and Examination with a Warrant), Part 5 (Equipment Interference), and Part 6 (Bulk Warrants). An appendix setting out in full all the material provisions of the IPA not otherwise referred to in this judgment is attached.

Issue (a): The duty of candour

13. The Claimants say that the NCA failed in two distinct respects to fulfil the duty of candour on them. First, they submit that the NCA did not tell the Judicial Commissioner just how limited was the information available to them about the method by which the JIT were to carry out the interception. The essence of the complaint is that, whether by lack of candour or lack of reasonable inquiry, the NCA were not in a position to maintain that the interception was of communications stored in or by a telecommunication system. Second, they submit that had the NCA been candid as to the effect of the interception and the extent of the collateral intrusion involved in the operation, it would have been clear that a bulk equipment interference warrant was required. We deal with this second point in the context of the challenge relating to the need for a warrant of that sort, that is under issue (d).

The law

14. The NCA owed a duty of candour when applying for authorisation of the TEI warrant. That included drawing to the attention of the judicial Commissioner anything that militated against the grant of the warrant: *R (Energy Financing Team Ltd) v Bow Street Magistrates' Court and others* [2006] 1 WLR 1316, paragraph 24; *R (Terra Services) v National Crime Agency* [2020] EWHC 1640 (Admin); see

also *R v Lewes Crown Court ex p Hill* (1991) 93 Cr App R 60; *R (Haralambous) v Crown Court at St Albans* [2018] AC 236.

15. IPCO Advisory Notice 1/2018 *Approval of Warrants, Authorisations and Notices by Judicial Commissioner* reflects the requirement to provide information which militated against the grant of the application, including material which weakened the case for the warrant: paragraph 30. It indicates that the application must explain why the proposed activity was necessary and proportionate, and that where the law is unclear or the applicant is proposing a novel or contentious legal interpretation, a more detailed explanation of the relevant legal principles must be provided: paragraph 33. Those requesting a warrant must confirm that they have made all reasonable efforts to take account of information that might weaken the case for the warrant.

16. The reference to "reasonable efforts" in the advisory notice is consistent with the duty of inquiry incumbent on a public authority at common law: *Secretary of State for Education and Science v Tameside MBC* [1977] AC 1014, page 1065B. There are similar references to "all such inquiries as were reasonable and proper" in private law authorities relating to *ex parte* applications for injunctions (eg *Brink's Mat v Elcombe* [1988] 1WLR 1350, at page 1358C).

17. The significant difference between the parties was as to the consequence of presenting material to a decision maker where the material was erroneous in some respect which did not give rise to a *Tameside* challenge. The Claimants submitted that material mistake of fact giving rise to unfairness was an error of law which if established would result in the warrant's being set aside: *E v Secretary of State for the Home Department* [2004] QB 1044. On that analysis if it turned out on the basis of information not available to the NCA at the time of the warrant application, that what was in the warrant application was wrong, the warrant should be set aside, providing that the five conditions set out in *E* were satisfied. It was therefore relevant to consider evidence showing that the interception had in fact taken place in the course of transmission, even if NCA had genuinely believed that it would not take place in that way, and had done so on the basis of reasonable inquiry.

18. A Divisional Court applied the principle in *E* in quashing the decision of a magistrates' court to refuse an adjournment and dismiss a charge in *R (DPP) v Sunderland Magistrates' Court* [2018] 1 WLR 2195. The Divisional Court emphasised that the application of material mistake of fact leading to unfairness as a ground of judicial review of decisions in criminal proceedings was limited to applications concerned with applications to adjourn trials in magistrates' courts: paragraphs 116, 117. A different Divisional Court considered *Sunderland Magistrates' Court* in *R (Daly) v Commissioner of Police of the Metropolis* [2018] 1 WLR 2221. Police had obtained a search warrant under section 23 of the Misuse of Drugs Act 1971, relying on evidence which included thermal imaging of a property showing high heat emissions, which was said to indicate that it was likely that cannabis was being grown there. They did not find any cannabis when they

searched. The claimant sought judicial review of the warrant. The court decided that the principle in *E* had no application in relation to search warrants.

19. As Sir Brian Leveson P pointed out in *Daly*, at paragraph 28, to apply mistake of fact to decision-making about search warrants would be to deprive search warrants of their potency. If execution of the warrant did not reveal evidence justifying the reasonable grounds, it would be contended that the mistake of fact removed the protection of officers acting pursuant to the warrant. We agree with that analysis. It applies to with equal force to warrants under the IPA. In the absence of any error of law, no such error being alleged here, they are not to be undermined other than on the basis of a failure of candour or failure of reasonable inquiry. It follows that we regard information subsequent to the grant of the warrant tending to show that the material was intercepted as irrelevant to the question of whether the warrant should be set aside.

20. The Claimants also sought to characterise the matter as one of precedent fact. Section 99(6) provides:

    "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)."

    The Claimants noted, in support of this submission, that there is no qualification suggesting that the person seeking the warrant must only have reasonable grounds to believe that the information presented was accurate. We consider that this submission was misconceived. To treat the question of whether the communication was a stored communication as a precedent fact would have the same effect as would treating mistake of fact as an error of law in the context of applications for warrants. We have therefore disregarded Professor Anderson's evidence, even assuming it to be accurate and to demonstrate that interception took place in the course of transmission, for the purposes of this chapter of the case.

21. The Claimants' position that the warrant could not authorise anything other than the recovery of material at a time when the communication was stored in or by the system is, however, potentially relevant to their claim that the recovery of the material was not in accordance with the law.

22. The Claimants submitted that if there had been a failure of candour or reasonable inquiry, the question was whether the information in question might have made a difference to the outcome when Sir Brian Leveson considered the TEI warrant: *R (Mills)* v *Sussex Police* [2015] 1 WLR 2199. The NCA referred to *R (Rawlinson & Hunter Trustees)* v *Central Criminal Court* [2012] EWHC 2254 (Admin) ("*Tchenguiz*"), which was the subject of discussion in *Chatwani* v *National Crime Agency* [2015] UKIPTrib 15_84_88-CH. Sir John Thomas P, in *Tchenguiz*, at paragraphs 172 and 173 expressed the view that the test when determining whether

to quash a warrant in a criminal context was whether errors and non-disclosure would have made a difference to the grant of the warrant.

23. We have not found it necessary to determine which test is applicable in this case. As we explain below, applying, in the Claimants' favour, the lower of the two tests (that in *Mills*) we are not satisfied that the decision of the Judicial Commissioner might have been different had the NCA provided the information that the Claimants said they should have done.

The facts – candour and reasonable inquiry as to the method of interception

Witness evidence

24. We heard oral evidence from Wayne Johns, Luke Shrimpton, and Emma Sweeting. Each provided one or more written statements. Mr Johns adopted the oral evidence he gave in criminal proceedings in Liverpool in November 2020. Ms Sweeting adopted the oral evidence she gave in criminal proceedings in Liverpool in November 2020 and in Manchester in May 2021. Mr Shrimpton also adopted his oral evidence from the same proceedings in Liverpool and Manchester. It is predominantly the evidence of Ms Sweeting that is relevant to this chapter of the case.

25. Mr Johns is a Grade 3 Branch Commander in the NCA and is the Senior Investigating Officer in the operation with which these proceedings are concerned. Ms Sweeting is an Intelligence Operations Manager in the NCA. Mr Shrimpton was formerly a Senior Officer in the NCA, and worked on EncroChat capability development.

26. We refer more fully to the evidence of Mr Johns in relation to the argument about the need for a bulk equipment interference warrant.

The period before the Europol meeting

27. Communications between the French Gendarmerie and the NCA about the potential for cooperation in relation to EncroChat date back to September 2018. On 5 September 2019 Ms Sweeting, in an email to her colleague Ms Clare Meehan, described France as "pivotal to the response to EncroChat" as the EncroChat infrastructure was hosted in France.

28. In these proceedings, as in earlier criminal proceedings, the focus has been largely on activities and communications in the early part of 2020. There was a meeting of EuroJust in the Hague on 22 January 2020. Ms Sweeting and other NCA officers attended it, as did Riaz Jakhura, a CPS lawyer. Ms Sweeting's evidence was that it was at this meeting the French prosecutor explained that the French authorities had a means of exploiting EncroChat communications. The terminology used by the French prosecutor suggested that the activity might be interception in transmission. The meeting did not, however, deal with technical detail, and no technical officers were present. Ms Sweeting had not formed a view as to the nature of the activity when she left the meeting.

29. After that meeting, there was email correspondence between the CPS and the NCA. It is clear from the correspondence, and readily understandable, that there was concern as to what type of warrantry might be required in relation to the operation to obtain data from the EncroChat system. We do not reproduce all of the correspondence in this judgment. We accept that it demonstrates that the UK authorities did not know how the operation was to be carried out. For example, in an email dated 24 January 2020, Luke Shrimpton wrote the following:

> "It looks like the French are planning to utilise their access to the EncroChat servers. Suspect it is a CVE based exploit for deploying on devices via the update server. Allows them to use intercept on the server to decrypt any data that passes through it … though not sure. Meanwhile, we may re-design the implant to make it less persistent. This involves removing the real-time exfil component instead focusing on a single hit DB exfil. An OP against an EncroChat device would look a little something like this: Hook device up on X3 during update; Deploy implant; Wait for app restart to trigger implant; Implant grabs DB, Key and exfil's it via current UDP system; Implant tides up; Implant removes itself. This way we can exploit a device and leave it in a relatively 'clean' state so we don't interfere with any implant deployed by the French."

30. There were also emails exchanged between Ms Sweeting, and M Jeremy Décou. He was an officer working in the digital crime unit of the French Gendarmerie. He was the Director of Investigation in relation to the disruption of the EncroChat communication system. The following exchange took place on 29 January 2020:

> 15:17 (from Ms Sweeting): "… Regarding the potential activity, we have had some discussions since our return from EuroJust in relation to how we would handle this material in the UK. You have suggested a second EIO but we treat intercept differently to other European partners so we may want to have some UK authorities in place in order to be able to use the material. This will of course be discussed between prosecutors.
>
> In order to consider our options, we would need to understand more about how the app works. It may be more appropriate for us to direct some formal questions via the prosecutor, but our main question (if you are able to assist) is whether the messages are collected from the database stored in the devices or live time from the server. This will greatly assist us in deciding how we could use this in the UK."
>
> 18:58 (from M Décou): "I remember, at our meeting you said, in UK you can't have interception on phone in judicial case. I think it's the same problem today with data interception …I hope the magistrates will find a solution for you, because if our rogue app works well, you could have great informations.
> You want to know what our rogue app can collect, here are the main features:
> - extraction chat (text and medias) + aes key database
> - extraction of notes database
> - extraction cell ID to identify country the phone is

> I try to explain the process, as a reminder, I'm not a technician, just an investigator. The data phone are collected on our server and we can access them in live or if it's not in live, it'll be almost in real time. I hope answer to your question … If you need more information, I can ask to my technician colleagues, send me your specific questions.
>
> About the meeting to Europol: Today Patrice, my French colleague who was present at Eurojust (cryptocurrency specialist), has proposed a meeting the week between 17 and 21 February. My programmers think that 2 days are enough for this meeting if everyone prepare on his side before coming. We will send to all our partners example of data before the meeting."

31. On 30 January Ms Sweeting responded:

> "Apologies for not being clear at EuroJust, but yes we can intercept on a judicial case, we just cannot use it as evidence in court. We can use this as 'intelligence only' in the investigation. In practice this means we would try to parallel the intelligence we receive, for example, we could carry out surveillance at a specific time and place based on the intelligence received through intercept. In court, we would then present what happened during the surveillance as our evidence, not the intercept material itself. I see this is very different to how you use the material but yes we can intercept under our legislation so we are extremely keen to access the material, as you say there will likely be great information in there that we could use.
>
> However, we only view material collected in live time as intercept. If the material is collected from the database in the devices, we might consider this to be what we refer to as 'Equipment Interference' instead and may be able to use this in evidence.
>
> We can work out these details with our prosecutors but yes there is a way for us to use your intercept on our cases."

32. The Claimants pointed out that there was no follow up between prosecutors or technicians in relation to the matters ventilated in the emails between Ms Sweeting and M Décou.

33. The Claimants placed some emphasis on the content of emails and other communications reflecting a belief or understanding that the technique for obtaining was such that a TEI warrant would be required. They include emails dated 5, 10 and 17 February 2020.

34. On 5 February 2020 Brendan Moore sent a memo to Matt Horne which included the following:

> "Our current understanding is:
> We know:
> […]
> - The technique used will be based on TEI, not TI."

35. There is an undated document specifying Gold Commander Requirements as to what is to be clarified at Europol, including the following:

> "Confirm that the data collected falls within the UK's definition of Targeting Equipment Interference rather than Targeted Intercept. The current UK understanding is that this will be TEI and not TI but this needs to be established for the purpose of authorities."

36. On 6 February 2020 Ms Sweeting wrote to M Décou:

> *"*We understand that you have legal authority to carry out this activity. For the UK we would like to put some authorities in place as well so we can use the data. This is a domestic issue but we want to get ready. In order to make this application, we need a description of what will be happening to the devices in the UK. I am not technical as you know, so would it be possible for you to share a description so we can use it in our authorities please."

37. A meeting took place on 13 February 2020 involving a number of NCA and CPS personnel. The minute records a variety of matters. For present purposes paragraphs 8 to 11 are potentially relevant. "ES" refers to Ms Sweeting, "MH" to Matt Horne, "PR" to Paul Risby, and "LH" to Liz Holley.

> "8. ES gave an overview of the project. Venetic is the overarching project and NCA are now realigning the operations under this project. Operation Emma is the linked French case. All the servers are in France. The French haven't had much interest previously as they don't believe they have a big user base but as the server is in their country there is an increased appetite for disruption. Initial conversations were had around the servers and getting images from them. The French believe they have found a vulnerability they can exploit in that "live time" they can send a modified app which will pull back data from the phone to the server. They have offered certain countries to have access. ES confirmed it is device access, not live intercept. ES described the timescales as terrifying as the French plan to deploy on 10/03/20. They are reluctant to push back because the action is based on a vulnerability that can be patched at any time.
>
> 9. ES discussed the approach to the data. Key word searches etc. may happen at Europol. The data is expected to include all the messages sent from the phone, metadata, encrypted data, not messages in transmission. It is the equivalent of downloading a phone at a point in time. NCA intend to work with ICPO (sic) in advance and NCA Legal advise that there is a need to put in place a UK lawful authority if we NCA intend to join this exploitation. ES confirmed that the French are calling the action 'intercept' but it is really exploitation.
>
> 10. ES will attend a 3-day workshop (19th to 21st Feb) with JW. This will determine how often the French intend to deploy the app but there is understood to be control over frequency which means it can be adjusted. Any subsequent grabs of data will be whatever is on the phone at the time and this will lead to duplication of data. MH confirmed that they wanted to put in place the

> capability to compare the grabs and eliminated duplication. PR highlighted that the NCA are not in control of the process. ES confirmed that it is unknown if the users or EncroChat themselves will see the exploitation. There is a risk that the deployment will be a one off because of that. Part of the workshop will be to assess whether or not the deployment will be detected. The French intention is to deploy for 2 months as their warrants are one month in duration, to be extended for one month and thereafter to 'kill' EncroChat by destroying their reputation. The French and the Dutch will go public to say they have brought the server down. It is intended that all the data will go to Europol, there will be triage at Europol, whether there is filter at Europol is unknown. ES believes that the UK can influence what we receive and the relationship with the French has improved and they want the UK to have the content as they realise the risk posed by 9,000 users. The French prosecutor has said he wants to have conversation with the UK prosecutor to shape the EIO and he has been positive about that. There is Dutch influence.
>
> 11. There was discussion about why the NCA need a domestic TEI warrant. LH outlined the concern that there could be a CMA [Computer Misuse Act] offence or conspiracy to commit the offence without a warrant. There are 9,000 UK devices and the concern is that the NCA would be complicit in the offence through sending the EIO and the involvement in the planning."

38. Ms Sweeting has been asked about this passage on a number of occasions. In *Coggins* she said that she would not have expressed herself categorically, as there was insufficient information available to allow for a firm conclusion as to the nature of the operation.

39. On 17 February 2020 Ms Sweeting wrote to a number of NCA colleagues, including Steve Bennett, Brendan Moore and Wayne Johns:

> "Further to the recent brief provided by Brendan on the planned exploitation under Project VENETIC, we are likely to need to seek a thematic TEI warrant. This will by its nature be deemed novel and contentious, although it has similarities with previous activity there are some distinct risks with this opportunity."

40. Ms Sweeting and M Décou exchanged a number of WhatsApp messages between 31 January and 6 April 2020. In a message on 31 January 2020, M Décou wrote, "I hope I understand; remember that my English is bad". He had made another reference to the quality of his English in the course of the messages.

41. The Claimants also relied on some parts of Mr Shrimpton's evidence as supporting the proposition that the NCA and its officers were reluctant to investigate or inquire for fear that they might discover information to which they had already closed their minds. Both Mr Shrimpton and Mr Johns gave evidence that the NCA had acquired EncroChat devices. Mr Shrimpton accepted that it would have been feasible to

allow those devices to become infected with the French implant by leaving them on during the period of the operation. The NCA might have been able to extract the implant and discover how it worked. They had not troubled to do so.

The Europol meeting – 19-21 February

42. Ms Sweeting's evidence was that Matt Horne gave the NCA delegation and the Police Scotland delegation the task of discovering the answer to ten questions, one of which is referred to above, regarding the nature of the activity (Gold Commander Requirements). She attended the meeting with NCA colleagues Luke Shrimpton, James Wilmott and Jonathan Belton. A number of round table meetings took place over the three days, and also informal discussions during breaks. In the course of the meetings she told the JIT partners that the UK authorities needed more information about the technique that would be used to carry out the proposed activity. She was told that the technique would not be shared with partners. She felt conscious of the need to maintain a relationship with the JIT, and so stopped asking questions during the round table sessions, and instead took the opportunity to speak with the JIT delegation during breaks. She understood that the technique was considered to be sensitive, and was to be protected.

43. On 20 February, after meetings had concluded for the day, the NCA delegation, including Ms Sweeting, placed a call to NCA legal. She could not remember the details of the call. During the course of the Europol meetings, Ms Sweeting had typed up a description of how she understood the French technique worked. It was based on information from meetings she attended, and with input from Luke Shrimpton regarding technical detail. He agreed her draft was accurate. She intended to ask M Décou to confirm if the description was accurate, as the NCA needed the information to decide what type of warrant was needed. She did this because it had been made clear that the JIT would not give a formal description of the technique. At the conclusion of the formal meeting on 21 February she showed M Décou the draft email on her laptop. It read as follows:

> "Stage 1 (historical data collection)
>
> An implant within an Application will be placed on all EncroChat devices worldwide. This will be placed on devices via an update from the update server in France.
>
> On deployment, this implant will collect data stored on the device and transmit this to French Authorities. This will include all data on the devices such as identifiers (eg IMEI and usernames), stored chat messages and notes (list not exhaustive).
>
> The implant will then remain installed on the device to enable stage 2.
>
> Stage 2 (forward facing collection)

> Communications (chat messages) on the EncrChat [sic] devices will then be collected on an ongoing basis.
>
> The messages are collected when they have been stored on the EncroChat devices.
>
> Simultaneously the messages are sent via the chat server but they will not be collected in transmission, they will be collected from the devices."

44. Ms Sweeting could not recall exactly what she said to M Décou after the meeting, but she explained to him why it was important that she obtain the information, so that the NCA could get the appropriate warrantry. She showed the text to him, he read it, and confirmed that it was an accurate reflection of the technique and how it worked. She was confident that he understood the definition and agreed it was a true and accurate. After confirming the description of the activity with M Décou, she was confident as to the explanation. Her view was that the activity was of the type that might be authorised by a TEI warrant. After the meeting she finalised the draft email and sent it to NCA colleagues just at 12:56. The description of the activity in the email was prefaced as follows:

> "I have drafted the below definition for the TEI application. The Gendarmerie has read and confirmed that the technical description is a true reflection of the activity:
>
> The French Authorities will be exploiting EncroChat devices globally to collect data from them. The French have domestic legal authorities in place which permits this activity. However, this activity would likely be deemed a Computer Misuse Act offence (more detail needed) in the UK. This application for Targeted Equipement Inteference [sic] under the IPA 2016 will make that activity lawful"

At the end of the email Ms Sweeting wrote:

> "I hope this helps clarify the activity as TEI but we would be grateful for confirmation."

45. Mr Shrimpton's evidence was that he remembered that Ms Sweeting showed him a document on her computer in which she had set out at a high level her understanding of how the French implant operated. He told her that it accorded with his general understanding of the operation of the implant. Ms Sweeting later told him she had shown the document to a French officer who had confirmed that her understanding was correct. Mr Shrimpton did not remember the name of the officer, or when, in the course of the Europol meetings, this had taken place. He could not remember whether the document was the text of the email referred to above.

46. After the meetings concluded, Ms Sweeting stayed in the café at Europol with her NCA colleagues, and possibly also Police Scotland colleagues, with a view to

agreeing the conclusions from the meeting. She took responsibility for finalising the meeting note. She had been compiling the note throughout the meetings at Europol. She produced a note with sections in black which she had written during the meetings, and sections in blue representing conclusions that she and her NCA colleagues had reached. The conclusions were finalised at the meeting in the café. The intention was to respond to the various requirements imposed by Matt Horne. The document included a section with Mr Horne's requirements in black, with the responses to them in blue. The document also included conclusions drafted by the JIT and Europol leads. These had been presented on large screens during the final session of the meetings, and Ms Sweeting had copy typed them into her laptop.

47. Mr Shrimpton's evidence was that he attended an informal meeting with the other members of the NCA team before returning to the United Kingdom. During the meeting they discussed Ms Sweeting's note of the meeting. Mr Shrimpton was satisfied that it was accurate so far as the technical elements were concerned, including the conclusion that the exploitation "amounted to TEI".

48. After returning to the UK, Ms Sweeting checked her note for spelling and grammar over the weekend. She sent the note ("the blue and black note") to the Gold Commander and other NCA colleagues on Sunday 23 February. After that there were "multiple meetings, including some with the Gold Commander, NCA legal as well as other key teams", after which there was agreement that a TEI warrant should be applied for.

49. Ms Sweeting gave evidence to us on 21 September 2022. It was not possible to conclude the hearing in the time available then, and three further days were therefore fixed for December 2022. After the September hearing she carried out a further disclosure review. In her offline files she found a note ("the offline files note") of the meeting other than the blue and black note. Offline files was a facility on her laptop's hard drive that permitted her to access and work on documents when her laptop was not connected to the NCA network. As a result, Ms Sweeting gave further evidence on 14 December 2022. Her evidence was that the offline files note was an earlier version of the document she had already produced. Its properties showed that it was last modified at 13:47 on 21 February 2021¸ a Sunday. She said that on the Sunday after the meeting, she worked at home. She sent the blue and black note to the Gold Commander that day. Her recollection was that she had gone through the conclusions in that note with her team at Europol on the Friday. She did not remember the sequence of events by which the content of the offline files note, or parts of it, had been incorporated in the blue and black note. She described the offline files note as a rolling note. The offline files note contained an entry, "*Need both TEI and TI*" under the heading "Day 1". Under the heading "Day 2", there appears a description of the activity that is almost identical to the one in Ms Sweeting's email of 21 February 2020. It also contained, near to the end of the document, an entry in blue reading:

> "We need to decide if the data is collected through TI or EI. The two techniques are described below:
>
> A) TI: The encrypted messages are collected while they pass through the chat server and are decrypted by French Law Enforcement.
> B) EI: Decrypted messages are sent from the device to a server owned by French Law Enforcement."

Ms Sweeting did not know at what point during the meeting she had written that passage. There were several other passages in the offline files note that were not reproduced in the blue and black note.

After the Europol meeting

50. After the meeting, the NCA entered into discussions with Paul Williams, Head of Legal at the Investigatory Powers Commissioner's Office ("IPCO"). An email from Simon Armstrong of NCA Legal to NCA colleagues at 17:13 on 21 February 2020 related that Mr Williams and Mr Armstrong had agreed that they felt that the warrantry for the operation was one that should be dealt with by Sir Brian Leveson, personally.

51. An email from Mr Williams to Mr Armstrong on 25 February was in the following terms:

> "I've discussed with Ben and we think you can, in principle, get what you want authorised. Happy to discuss further if you want to give me a call … We think a [judicial Commissioner] briefing is probably not necessary."

52. On 2 March 2020 Mr Armstrong wrote to Mr Williams:

> "Thanks for discussions on Friday.
>
> My colleague Liz [Holley] will send the draft application over via the high side shortly, once we've impexed it over.
>
> As discussed, very happy for you to discuss with a [judicial Commissioner]. The app is still in draft and has not been reviewed by a DD here, nor seen by the DG. However, NCA Legal are content that covers all the matters necessary and there are no obvious omissions that we can see."
>
> We'd welcome any observations you may have."

53. The NCA sent the draft application to IPCO on the same day. Mr Williams responded with comments on the draft. These included a suggestion that the contention of exclusive criminal use of EncroChat was "expressed in surprisingly absolute terms", and invited an explanation as to why NCA considered that there were no legitimate users. They raised queries about possible collateral intrusion,

and emphasised the need for the identification of any specific targets of whose identity the NCA was aware.

54. There was also communication between the CPS and the NCA about obtaining the EIO. On 3 March 2020 Ian Lee of the CPS emailed Ms Sweeting, asking for the following:

> "1. A note of the meeting at Europol;
> 2. Any advice or note in relation to NCA Legal's position on TEI/TI;
> 3. Any material from the Information Commissioner (?) on their view of NCA Legal's position;
> 4. MOU with JIT partners;
> 5. Confirmation that the warrant is a warrant on behalf of the United Kingdom, rather than just Eng & Wales."

55. On 2 April 2020 M Décou provided a report to the French authorities in respect of the request in the EIO. The report includes a reference to "a data collection mechanism on the EncroChat telephones". It also includes the following:

> "Two types of data will be transmitted:
> 1) The ("earlier") data that is in the telephone at the time when the collection mechanism was installed on this telephone, with the condition that the telephone should receive the tool when they are on the British territory.
> 2) The data that is collected live (live) while the collection mechanism is taking place, with the condition that the telephones are on the British territory."

56. In a further report dated 3 April 2020 M Décou wrote, under the heading "Creation of the collection tool:

> "We requested the support of the only French Department that is authorized to create data collection tools. This Department and its productions are covered by the National Defence Secrecy Regulations. For this reason the details relating to the collection tool cannot be revealed."

57. M Décou again reported on 22 June 2020 in relation to the request in the EIO:

> "Pursuant to the request made by the British Authorities, we have explained the method that lead to the implementation of the data collection. Some elements could not be described as they are covered by the National Defence Secrecy Regulations."

58. On 23 September 2020 the CPS issued an EIO to the French authorities, requesting permission to allow an officer of the NCA to take a statement from M Décou. There followed a further request that M Décou provide oral evidence in proceedings in the United Kingdom. The French authorities responded that they did not consider that

this was a reasonable request and that it was unlikely that the French judicial authorities would accede to it. The history is more fully recorded at paragraph 115 in the judgment of Dove J in *R v A and others*. The outcome was that the French prosecutor and examining magistrate gave reasons why they would not permit M Décou to come to the United Kingdom to give evidence.

59. M Décou was interviewed by two NCA officers on 25 September 2020 at the Palais De Justice in Lille with the assistance of an interpreter and in the presence of a French prosecutor. His answers were compiled into a witness statement dated 25 September 2020. He declined to answer questions concerning the operation of the application that enabled the collection of data, on the grounds of defence secrecy. When asked what he meant by live data, he replied:

> "… live data is the data that the user enters on their phone and the data that appears on that phone. It is data that is sent and received, as provided for by French law."

and when clarifying the difference between stored and live data:

> "… the stored data are the data that were in the phone when the technical device was deployed on 1st April. The live data are the data that arrive after the technical device has been set up."

We do not narrate in further detail the content of the interview of the statement, as it is, for the reasons we give below, a portion of the evidence on which we place very little reliance.

Submissions

60. The Claimants' submission came to be that the NCA misled the judicial Commissioner by giving the false impression that there was formal approval by "the gendarmerie" of the methodology described in Ms Sweeting's email and to which she said M Décou had assented. The NCA had given the judicial Commissioner the impression that there had been formal communication and assent, when there had been none, and Ms Sweeting knew that there could be none. The legality of the operation was based on one reported conversation between Ms Sweeting and M Décou, to which no one spoke other than Ms Sweeting. The NCA could have asked M Décou to confirm the information. They had not done so, and the tribunal was entitled to draw the inference that they had not done so because they anticipated an answer that would be unfavourable to them. Ms Sweeting's account had emerged only in criminal proceedings in September 2020. It appeared neither in the rolling note nor in blue and black note. All of this called into question the credibility and reliability of Ms Sweeting's evidence.

61. The NCA had failed to disclose to the Commissioner also:

    (a) that NCA officers had had doubts during the Europol meeting as to nature of the warrantry that might be required; and

(b) that M Décou was not a technician and that he had expressed reservations about his proficiency in English;
(c) that there was no indication from M Décou that the conversation with Ms Sweeting occurred;
(d) that only Ms Sweeting spoke to the conversation's having occurred;
(e) that "the gendarmerie" had not confirmed the nature of the conduct;
(f) that that was the result of a deliberate decision;
(g) that the NCA had no intention of sharing the warrant with the JIT as a party from whom they were requiring assistance.

62. M Décou was questioned in September 2020. He refused to describe the application or technical device by which the EncroChat data were captured. Although the answers that he gave in September 2020 were not before the judicial Commissioner, they were instructive. The best that could be said was that he was prepared to give a "nod and wink" to the NCA in February 2020, and it must have been obvious to Ms Sweeting that he would never give any formal confirmation of the position. The content of his answers in 2020 indicated that he would not have assented to Ms Sweeting's draft description in the way that she said he had done.

63. The history of late disclosure of material deriving from Ms Sweeting called into question some aspects of her professional judgment, and that had a bearing on the assessment of her credibility and reliability. The content of the rolling note demonstrated that she had given inaccurate evidence before it was disclosed. She had previously asserted that the blue and black note was a note compiled during the course of the meeting, when it was not. She was capable as presenting as credible and assertive even when she was wrong.

64. Mr Johns had agreed in cross examination in the criminal proceedings, and in the present proceedings, that the judicial Commissioner might have wanted to know that information presented to them derived from a conversation at the end of the Europol meeting involving an individual looking at material on someone else's laptop in a language that was that individual's second language.

Conclusions

65. The Claimants asked us to conclude that the NCA had, before the Europol meeting, closed its mind to the possibility that anything other than a TEI warrant might be required. It is true that there were no communications between prosecutors or technical experts (as some of the emails had indicated there could be) to clarify matters before the Europol meeting. That needs, however, to be viewed in a context where the Europol meeting was imminent, and the purpose of the meeting was to provide further information about the operation. The various communications and records, looked at in the round, record an understanding, expressed with varying degrees of confidence, that a TEI warrant, rather than a TI warrant, would be required. Ms Sweeting's email of 30 January at paragraph 31 above is important in this context. It is couched in terms recognising the use to which material recovered under a TI warrant might be put. She was still, on 6 February 2020, making

inquiries of M Décou with a view to ascertaining what warrantry might be necessary. The minute of the meeting of 13 February, at paragraph 9 expresses an expectation that the data would not include messages in transmission. Ms Sweeting denied having had a closed mind before the Europol meeting. We accept that NCA officers would have had a preference that the data be material capable of being admitted in criminal proceedings, but are not satisfied that they, or any particular officers, had closed their minds on that matter before the Europol meeting.

66. We accept that the NCA did not instruct the deliberate infection of their EncroChat devices, and that that was a line of investigation or inquiry potentially open to them. We place little weight on this matter. We are not satisfied that there was a deliberate decision to avoid inquiry of this sort. The evidence of Mr Shrimpton and Mr Johns was to the contrary effect. Again, the context is relevant. It is common ground that the NCA was interested in EncroChat and was trying to find ways to infiltrate it. Mr Shrimpton was involved in those endeavours. In January 2020 at the Europol meeting the NCA learned that the French authorities actually had a means of exploiting EncroChat communications. It is unsurprising that the focus of attention should at that point have come to be on how to participate in the fruits of that exploitation, rather than on developing in parallel an independent means to carry it out.

67. The content of the offline files note does not undermine our view that the NCA officers had not closed their minds to the possibility that the operation would involve anything other than the recovery of material stored on the system. It is impossible to determine the order in which different parts of the note were written. The blue section at the end suggests that at some point during the three days the NCA were in some doubt about the matter, and actively considering it. The inclusion in the note of the description of the activity which also appears Ms Sweeting's email lends some limited support to her account of having put that description to Mr Décou in the way that she described in evidence. There are differences between the offline files note and the blue and black note. That is not surprising. The blue and black note was intended to convey the views that the NCA officers had formed after the full three days of meetings, and not to convey every part of their prior consideration of the material during those three days. The content of the offline file notes undermines the proposition that the NCA officers were attending the meetings with closed minds. The notes disclose that there was thought given to the possibility that a TI warrant might be required.

68. The history of disclosure in relation to this matter is not a happy one. We are aware that the WhatsApp messages between Ms Sweeting and M Décou were produced at a relatively late stage in the criminal proceedings in Liverpool in 2020. Ms Sweeting's own view of the relevancy of those messages in the context of a disclosure exercise differed from that taken by the CPS. That said however, the material actually put to her from them as potentially relevant is quite limited in scope and was said to cast light on M Décou's own view of his proficiency in the English language. As we have recorded, the disclosure of the rolling note came

very late in the proceedings before us. We cannot reach any firm conclusion on the basis of the evidence before us as to the order in which the rolling note was composed. We accept that it is more likely that the rolling note captured various pieces of information and discussions in the course of the three days of meetings, and that the blue and black note was a document created after the meetings were complete. We do not regard the history of the creation of the blue and black note as impacting in any material way on the credibility and reliability of the essential elements of Ms Sweeting's account of her conversation with M Décou.

69. The Claimants submitted that if the tribunal were not working on the premise, taking Professor Anderson's report as read, that the information provided by Ms Sweeting was factually wrong, they were impoverished in their ability to present their case. If the information was factually wrong, that in itself would tell against her credibility. For the purpose only of assessing her credibility and reliability we have assumed in the Claimants' favour that it will ultimately prove to be the case that exfiltration did not take place from the devices.

70. Having done so, we are of the view that the core of her account, namely the interaction between her and Jeremy Décou on 21 February 2020 is credible and reliable. We accept Ms Sweeting's account of her interaction with M Décou on 21 February 2020. She has been consistent in that account in earlier criminal proceedings and now in this tribunal. Her account is supported in some respects by the evidence of Mr Shrimpton. We give limited weight to the report provided by M Décou in the context of the EIO. The two stage process he describes has some similarities to the description that Ms Sweeting said he had approved, and which appeared in the offline files note, but it is not in identical terms.

71. We also place very little weight on the content of M Décou's interview and statement from September 2020. Both the Claimants and the NCA selected passages from them which they said supported their positions as to whether material was intercepted in the course of transmission, and by extension their position as to whether Ms Sweeting was credible and reliable in her account of her interaction with M Décou. We do not consider that M Décou's answers cast any additional light on those matters. Given his explanations as to his understanding of "live data", his answers provide little support for the Claimants' case.

72. In our view, it is correct to say that Ms Sweeting did not ask for formal confirmation because she knew she would not get it. She said as much in her evidence in the criminal proceedings in Liverpool on 19 November 2020. That was not, however, because she feared that the answer would be one that the NCA would not wish to have. Rather, it was because she had genuinely formed the impression that the French authorities were reluctant to provide details as to the method they proposed to use to obtain the EncroChat communications. She had formed that impression because of what had happened during the course of round table meetings. The content of M Décou's report of 3 April 2020 lends support to her account of a reluctance on the part of the French authorities to provide details.

73. We are not satisfied that candour required the Commissioner to be told that officers had at various stages entertained doubts before the end of the Europol meeting as to the nature of the warrantry that might be required. The complaints about a lack of disclosure that M Décou had not confirmed the conversation with him took place, or that only Ms Sweeting could speak to its occurrence are all elaborations of the central complaint, which is that the NCA misled the judicial Commissioner by giving the false impression that there was formal approval by "the gendarmerie" of the methodology described in Ms Sweeting's email and to which she said M Décou had assented.

74. This central complaint is, in our judgment, without substance. M Décou is an officer of the gendarmerie. He had, on our finding, confirmed the methodology as described in the application for the TEI warrant. Ms Sweeting said in evidence in the Liverpool proceedings on 19 November 2020, at Core Bundle page 840,

> "I was entirely confident that when I put that in front of Jeremy Decou he understood the definition and agreed it was a true and accurate reflection."

75. We accept that this was her state of mind at the time when the application was drafted, and that it informed the way in which it was drafted on this issue. If the application had contained a fuller account of how she had arrived at that state of confidence, the Commissioner might perhaps have wondered whether it was well-founded but he would have had no rational basis for rejecting what she said.

76. It is submitted that the Commissioner's decision might have been different had he known this additional detail:-

- that the source of the information as to the nature of the conduct derived from a conversation between Ms Sweeting, and M Décou, a single non-technician officer of the gendarmerie, whose first language was not English;
- that he had indicated his assent to text drafted by Ms Sweeting describing the conduct;
- and that she had deliberately approached matters in that way because it had become clear to her during the meetings that an attempt to obtain any more formal type of confirmation as to the nature of the conduct would be refused.

77. We are not satisfied that provision of that information to the judicial Commissioner might have resulted in a refusal to approve the warrant. The conduct he authorised was described in the warrant (so far as material to this issue) as follows:

> **Stage 1 (Historical Data Collection)**
> On deployment this implant will collect data stored on the device and transmit it to the French Authorities. This will include all data on the devices and is expected to include identifiers (e.g. IMEI and usernames), passwords, stored chat messages, geo-location data, images and notes. The implant will remain installed on the device to enable stage 2.

> **Stage 2 (Forward Facing Collection)**
> Communications (such as chat messages) stored on the EncroChat devices will then be collected throughout the duration that the tactic is deployed.
> Once stored on the handset, messages will be collected on an on-going basis. Messages will only be collected once they are stored on the device. As a result, this is considered as being conduct that is capable of being authorised under a Thematic Equipment Interference authority.

78. This conduct was so described because of Ms Sweeting's belief about the way in which the implant operated. At the end of this judgment we canvass a submission made to us that the warrant was not actually necessary at all, and also the jurisdiction of the Crown Court to investigate and determine whether the relevant material was collected "in accordance with the warrant". The purpose of the warrant was to render the conduct of the JIT lawful, when otherwise it might have been an offence under the Computer Misuse Act which the NCA might therefore commit as a secondary party by encouraging it. It therefore enabled the NCA to request the material from the JIT, which was going to acquire it in any event. From the point of view of the Commissioner, he was authorising conduct which was the collection and sharing of stored data from the devices. If anything else was to happen, which is the possibility which, it is said, should have been given greater prominence in the application, he was not being asked to authorise it, nor was he doing so. The necessity and proportionality of acquiring the data was clearly demonstrated to a high degree by the application. Therefore, even if he had entertained doubts about the methodology of the acquisition of the data, he would have inevitably granted the warrant. Any problems for the admissibility of the material which that methodology might cause would be for the criminal courts to resolve in due course.

Issues (b) and (c): Sections 9 and 10 of the IPA; the EIO

The statutory provisions

79. Sections 9 and 10 appear in Part 1 of the IPA, which is concerned with general privacy protections. They provided, at the material time:

> "9 (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 (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."

80. The EIO was made under the Criminal Justice (European Investigation Order) Regulations (SI 2017/730), which have subsequently been repealed. Regulations 7 and 11 provided:

> "7(1) If it appears to a designated public prosecutor—
>
> (a) that an offence has been committed or that there are reasonable grounds for suspecting that an offence has been committed, and
>
> (b) proceedings have been instituted in respect of the offence in question or it is being investigated,
>
> the prosecutor may make an order under this regulation.
>
> (2) …
>
> (3) An order under this regulation is an order specifying one or more investigative measures to be carried out in a participating State ("the executing State") for the purpose of obtaining evidence for use either in the investigation or the proceedings in question or both.

> (4) But an order under this regulation may only be made or validated if it appears to the designated public prosecutor that—
>
> (a) …
>
> (b) the investigative measures to be specified in the order could lawfully have been ordered or undertaken under the same conditions in a similar domestic case (see regulation 11), and
>
> (c) …
>
> 11(1) When deciding for the purposes of regulation 6(4)(b) or 7(4)(b) whether an investigative measure could lawfully have been ordered or undertaken under the same conditions in a similar domestic case, the judicial authority or designated public prosecutor ("the relevant authority") must consider in particular the following matters.
>
> (2) …
>
> (3) Where the investigative measure requested is one which would require authorisation under any enactment relating to the acquisition and disclosure of data relating to communications, or the carrying out of surveillance, before it could be lawfully carried out in the United Kingdom, the relevant authority must consider whether such authorisation—
>
> (a) has in fact been granted, or
>
> (b) could have been granted, taking into account in particular—
>
> (i) the matters specified in sub-paragraphs (a) to (d) of paragraph (2), and
>
> (ii) the provisions of the enactment applicable to the granting of such authorisation.
>
> (4) Where the investigative measure requested is in connection with, or in the form of, the interception of communications, the relevant authority must consider whether any additional requirements relating to the making of such a request, imposed by any enactment other than these Regulations, have been complied with.
>
> (5) …
>
> (6) …

81. The designated public prosecutor is defined, so far as England and Wales and Northern Ireland are concerned by regulation 2(1) and Part 1 of Schedule 1, and in the present context means the Director of Public Prosecutions and any Crown Prosecutor.

82. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters is designated as an EU mutual assistance instrument for the purposes of section 10 of the IPA: regulation 59. Paragraph 9 of Schedule 3 to the regulations amended the IPA by inserting section 10(2A).

Issue (b): The tribunal's jurisdiction in relation the claims that the EIO was unlawful, and the claim that the NCA breached section 10 of the IPA

Claimants' submissions

83. So far as section 10 was concerned, the conduct of the NCA was a request for assistance with the interception of communications by the JIT: *ABD&C*, paragraph 72. The conduct took place with the purported authority of a warrant under Part 5

of IPA, and was challengeable conduct. A request for mutual assistance in connection with, or in the form of, the interception of communications, required a mutual assistance warrant, unless one of the exceptions in section 10(2A) applied. Neither did. Even if the interception were of stored communications, the request for assistance was not made in accordance with a court order or in the exercise of a statutory power exercised for the purpose of obtaining information or taking possession of a document or other property.

84. The intention of section 10(2A) was to produce an exception to the need to obtain a mutual assistance warrant. If, however, requests fell outside the remit of section 10(2), they would not be subject to any need for domestic warrantry. The 2017 Regulations contained limitations to the exception, requiring either the order of a court, or the exercise of a statutory power exercised for the purpose of obtaining information or taking possession of a document or other property. The sort of power envisaged was, for example, a police constable's access to excluded material or special procedure material under section 9(1) of the Police and Criminal Evidence Act 1984: see *R(Ntl Group Ltd) v Crown Court at Ipswich* [2002] EWHC 1585 (Admin). The Claimants referred also to the examples of statutory powers listed in paragraph 12.14 of the Interception of Communications Code of Practice and the discussion at paragraphs 12.15 and 12.16. The requirement that a statutory power be exercised could not be satisfied by the mere making of the EIO itself: that would involve a circular process of reasoning.

85. The first five Claimants submitted that the public prosecutor had failed to consider, by reference to regulation 11 of the 2017 Regulations, whether the necessary authorities could have been obtained were the investigative measure to have been carried out domestically. The EIO fell foul of either regulation 11(3) or 11(4). The Claimants' analysis was that this argument was contingent on a finding that the Part 5 warrant was unlawful for at least one of the reasons advanced elsewhere in submissions.

NCA submissions

86. The making of an EIO was not conduct of a type mentioned in section 65(5), and in particular paragraphs (czd) (conduct of a kind which may be required or permitted by a warrant under Part 5 or Chapter 3 of Part 6 of that Act; (cze) (the issue, modification, renewal or service of a warrant under Part 5 or Chapter 3 of Part 6 of that Act); or (czm) (any conduct falling within paragraph (c), (czb), (czd) or (czi)). Conduct "in connection with" meant conduct properly ancillary to the authorised conduct.

87. Similar arguments to those presented by the Claimants as to the construction and significance of sections 10 were rejected by the Court of Appeal in *ABD&C*. The NCA submitted that the Tribunal was bound by the decision of the Court of Appeal. If it was not, the reasoning of the Court of Appeal was sound in law, highly persuasive, and the Tribunal ought to adopt and follow it.

Decision

88. The claims in relation to the alleged unlawfulness of the EIO and the breach of section 10 are claims that the NCA breached the Claimants' human rights. The Tribunal is the only appropriate Tribunal for the purposes of section 7 of the Human Rights Act 1998 for actions incompatible with the Convention Rights which fall within section 65(3) RIPA. The relevant paragraph of section 65(3) is (d). The Tribunal will have jurisdiction only if the proceedings relate to the taking place in any challengeable circumstances of any conduct falling within subsection (5). Conduct takes place in challengeable circumstances if it is conduct that took place under, required the grant of, or at least required consideration of seeking, a warrant or other authority of the types listed in subsection (8): subsection (7).

89. The Claimants' characterisation of the conduct of which they complain in this chapter of the case is not consistent. They accept, under reference to *ABD&C* at paragraph 72, that the EIO was requesting assistance with the interception of communications. The Claimants' analysis is, however, that the conduct, namely "the interception" took place in challengeable circumstances because it took place under the purported authority of a warrant under Part 5 of the IPA. These competing characterisations involve a conflation of the respective roles of the DPP and the NCA. It was the former who made the request. So far as the lawfulness of the EIO and any breach of section 10 is concerned, we consider that the conduct in question is the making of the request. It is the making of a request that is, potentially, prohibited by section 10(2). The EIO was made for the purpose of obtaining the results of interception of communication and was therefore a request for assistance in connection with interception. Our approach to the nature of the conduct is consistent with that of the Court of Appeal in *ABD&C* at paragraphs 72-75.

90. As we note in paragraphs 102 and following, Sir James Eadie KC, leading counsel for the NCA, raised at a late stage in argument the possibility that the NCA might not have required a Part 5 warrant in order to benefit lawfully from the fruits of the JIT's endeavours. We accept, however, on the hypothesis that the NCA did require to obtain a Part 5 warrant, that the conduct of making a request for access to the data fell with section 65(5)(czm) of RIPA, because it was conduct in connection with conduct falling with paragraph (czd) of section 65(5).

91. We do not, however, consider that the conduct took place in challengeable circumstances. As we have explained, the conduct for the purposes of this part of the argument is the making of the request for access to the data obtained by the French authorities. The making of the request did not take place with the purported authority of a Part 5 warrant. There is no warrant under Part 5 that is required, or apt, to authorise the making of a request of this sort. The existence of the TEI warrant was not a necessary precondition for the lawfulness of the request.

92. We have considered whether anything in regulation 11 of the 2017 Regulations suggests otherwise, and have concluded that it does not. Where an investigative measure, if carried out in the United Kingdom, would require authorisation under

an enactment, the maker of the request must consider whether such authorisation has in fact been granted or could have been granted: regulation 11(3). The investigative measure specified in the EIO was a request for access to data obtained by the French authorities in respect of all EncroChat devices identified as located in the UK. The maker of the request was not requesting that an investigative measure be pursued, but was requesting the fruits of an investigation.

93. We have also considered whether the conduct could be regarded as having taken place in challengeable circumstances because it required the authority of a mutual assistance warrant. No mutual assistance warrant was required. We accept and agree with the reasoning of the Court of Appeal in *ABD&C* on this point. We do not consider that we are bound to follow a decision of the Criminal Division of the Court of Appeal, but such a decision is highly persuasive so far as the Tribunal is concerned. As we have decided to follow the approach taken by the Court of Appeal we have not engaged a detailed analysis of the competing submissions as to whether or not we are bound to do so.

94. The Court of Appeal found that the EIO was a request for assistance under an EU mutual assistance instrument which was in connection with the interception of communications. Subsection (2A) applied, because the request was made in the exercise of a statutory power, namely the power of a designated prosecutor to make or validate a EIO under regulation 7 of the 2017 Regulations. The purpose of those regulations and of section 10(2A) was to incorporate the EIO system into domestic law. That was reflected in the Explanatory Memorandum to the 2017 Regulations. It was inconsistent with that purpose to construe section 10(1) and (2A) so as to remove from its scope a EIO. The Court of Appeal rejected the contention that a mutual assistance warrant was required in order for a lawful request for assistance in connection with the interception of communications.

95. It follows that that had we been satisfied that we had jurisdiction, we would have found the substance of this challenge lacking in merit for the same reasons as those recorded by the Court of Appeal in *ABD&C.*

Issue (c): Was a TI warrant required?

96. The Claimants maintain that a targeted interception ("TI") or targeted examination warrant under section 15 was required. The NCA made a request of authorities of countries outside the United Kingdom to carry out the interception of communications sent by, or intended for, an individual who the person making the request believed would be in the British Islands at the time of the interception. Section 9 of IPA was engaged. The NCA was not permitted to make that request of the JIT unless a TI warrant had been issued under Chapter 1 of Part 2 of the IPA. By relying on a Part 5 warrant the NCA and the judicial Commissioner had erred in law. Section 9 was not simply concerned with Part 2 conduct, as the Court of Appeal had held in *ABD&C*. There was no distinction between live and stored communications in section 9, because foreign authorities would not be prepared to

disclose their methods of working. A TI warrant permitted interception in the course of transmission, but also permitted interception of stored material.

97. The NCA's analysis at the time of applying for the warrant was that they were "requiring" the JIT to provide assistance by conducting interference on UK EncroChat handsets. That analysis appears in the warrant application under the heading "Description of conduct authorised to take". The same passage includes reference to section 126.

98. This is again a ground of challenge litigated in *ABD&C*. We agree with the reasoning of the Court of Appeal on this point also (*ABD&C*, paragraphs 76-79). The court found that section 9 was applicable to requests for the interception of targeted interception material, and was of no application. The intention of section 9 was to prevent the circumvention of the regulation of Part 2 activity by the commissioning of overseas authorities to carry it out in the UK on behalf of the UK authorities, and it should be construed accordingly. The position which applied if the request were made under an EU mutual assistance instrument or an international mutual assistance agreement was governed by section 10 so far as the assistance was in connection with or in the form of interception of communications. That provision by necessary implication required section 9 to be construed so that it did not apply to cases within section 10. Section 9 governed only a request made by means other than an EU mutual assistance instrument or an international mutual assistance agreement.

99. We agree with the Criminal Division of the Court of Appeal that the intention of section 9 was to prevent the circumvention of the regulation of Part 2 activity by the commissioning of overseas authorities to carry it out in the UK on behalf of the UK authorities. Like the Court of Appeal, we consider that the conduct was rendered lawful by section 6(1)(c) and section 10(2A).

100. We add these further observations, which support that construction. As a matter of purposive interpretation, it is difficult to see why Parliament would have chosen to render inadmissible all material obtained emanating from requests for assistance from foreign agencies. That would be the consequence of the Claimants' construction of section 9. Section 9 requires a TI warrant. Material obtained under a TI warrant is inadmissible: section 56, and Schedule 3, paragraph 2. Even communications stored in or by a telecommunication system would be inadmissible if recovered under a TI warrant.

101. The refusal to admit evidence obtained by interception in the course of transmission is a policy choice to preserve the value of the use of the technique for intelligence purposes. It is not rooted in any concept that to admit evidence of that sort would be unfair, or that it would be inconsistent with Convention rights to do so. It is not designed for the protection of the individual, though it coincidentally provides a windfall benefit to defendants against whom the Crown cannot use evidence secured by those means. It is, as the Tribunal noted in *Hill* v *Metropolitan Police*

Service and Independent Officer for Police Conduct [2022] UKIP Trib 6, at paragraph 34b, an exception to the general rule that relevant evidence is admissible. There is no obvious reason why Parliament would have chosen to extend that windfall benefit to defendants where material was a communication stored in or by a telecommunication system, simply because a foreign agency, rather than a domestic one, had intercepted the material.

102. We record that in the course of the hearing in December, Sir James Eadie KC, leading counsel for the NCA, submitted that the exercise of obtaining a Part 5 warrant may have been unnecessary. The submission came at a very late stage and after the Claimants had presented their arguments. It was not prefigured in the NCA's written case, and was not fully argued before us. The Claimants and the NCA prepared and presented their respective cases on the basis that the NCA did require to obtain a warrant. We have not, therefore, come to any conclusions about the submission. We observe that in making the submission counsel recognised that there may be difficulties with the analysis promoted by the NCA at the time of seeking the warrant, so far as that analysis relied on the notion that the NCA was "requiring" the JIT to provide assistance. The notion that an agency of one state can "require" the agency of another state to do something by virtue of a domestic statute is an odd one. The provisions for the implementation of warrants are in terms that militate against their application to the agencies of foreign states. Both Chapter 1 of Part 2 and Part 5 of IPA contain provisions relating to the implementation of warrants: respectively sections 41-43, and sections 126-128. For predecessor provisions see section 11 of RIPA as amended by section 4 of the Data Retention and Investigatory Powers Act 2014.

103. Both sets of provisions in the IPA empower the authority to which a warrant is addressed to require other persons to render them assistance. Both say how service of the warrant on the person being required to provide assistance may be effected. That includes service on persons outside the United Kingdom. Both section 42 and section 127 allow for service on a person outside the United Kingdom by various means. Those include making it available for inspection at a place in the United Kingdom, but only where it is not practicable for it to be served by any other means.

104. Section 43 deals with sanctions for non-compliance with a requirement imposed under section 41. It applies to postal operators and telecommunications operators: section 43(2). A failure to comply with the steps notified by the intercepting authority is an offence: section 43(7).

105. In part 5 of the Act, the enforcement provisions are in section 128, and relate to telecommunications operators. The duty to assist imposed on telecommunications operators regarding warrants issued under section 106 is limited to steps for giving effect to the warrant which were approved by the Secretary of State/Scottish Ministers before the warrant was served: section 128(2). The duty imposed by section 128(2) is enforceable against a person in the UK by civil proceedings by the

Secretary of State for an injunction of for specific performance of a statutory duty under s45 of the Court of Session Act 1998 or other appropriate relief.

106. Every person required for the purposes of section 41 or section 126 of IPA to provide assistance with giving effect to a warrant is a person who is obliged to disclose documents and information to the Tribunal with a view to the Tribunal's exercising its jurisdiction under section 65 of RIPA: section 68(7)(e) of RIPA. That again militates against the notion that the agencies of foreign states are persons on whom requirements can be imposed in order to give effect to warrants.

107. None of these features suggests that a foreign agency can be required to provide assistance. The potential for difficulty associated with enforcing extraterritoriality unilaterally in respect of telecommunications operators was highlighted in the Joint Committee on the Draft Investigatory Powers Bill Report of Session 2015-16, 11 February 2016, HL Paper 93 - HC 651, at paragraphs 513 and following: Draft Investigatory Powers Bill - Joint Committee on the Draft Investigatory Powers Bill (parliament.uk).

108. We consider that section 99(5)(b), which provides that a TEI warrant authorises any conduct 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, has no application in relation to the assistance that a foreign state may provide. We note that Dove J reasoned, in construing section 9, that to read that section as applying to conduct covered by a TEI would cut across the breadth of the authority given under section 99(5). For the reasons given we do not adopt that part of his reasoning. We note that it was not the subject of specific approval by the Court of Appeal.

Issue (d): Was a bulk equipment interference warrant required?

Facts

109. It is common ground that if a bulk interference warrant was required, it was not a warrant of a type that could have been granted to the NCA. Such warrants can only be issued on an application by or on behalf of the head of an intelligence service. The NCA is not an intelligence service for this purpose, see sections 178(1) and 263(1) IPA.

110. The NCA's National Strategic Assessment of Serious and Organised Crime in 2019 included the following under the heading "Use of Encryption in SOC [Serious Organised Crime]":

> "EncroChat is predicted to remain the most prominent criminally dedicated secure communications provider in the UK, with the greatest market share. Used exclusively by criminals, this bespoke encrypted communications platform is exploited to commit SOC, whilst thwarting information gathering."

111. Mr Johns gave evidence that the NCA continued, as at the dates of the hearings, to assess that EncroChat devices were used exclusively by people involved in criminal activity. It carried out a review in October 2020 and considered that it had not received sufficient data to "determine the criminality of 390 users". It considered that those users did not use EncroChat primarily for innocent purposes. No material had been found linking users to academia, journalism or privacy enthusiasts, although that had been looked for in the triage process.

112. In cross examination he was referred to an Operation Venetic Briefing which indicated that data had been obtained from 7407 UK-based EncroChat devices since 1 April 2020. 294 phones had not demonstrated a clear link to criminality. Of these 173 had no content, and the others contained limited data. A more detailed account of the examination of devices appeared in a disclosure schedule. Mr Johns conceded that that material did not entirely support the contention of exclusive criminal use.

113. He was extensively challenged in cross examination as to why no consideration had been given to the possibility that a bulk equipment interference warrant might be required. The lines put to him reflect the Claimants' submissions, set out below. His oral evidence provided relatively little assistance in our consideration of those submissions, which are essentially propositions of law made by reference to documents before the tribunal.

Claimants' submissions

114. The Claimants submitted that the TEI warrant purported to authorise the bulk interception of communications. TEI warrants were thematic warrants; they required to relate to equipment with a common theme. That was reflected in the *Code of Practice* at paragraphs 5.7 to 5.12. Part 3 of the IPA related to bulk interference warrants. Such warrants were available only when necessary in the interests of national security, and applications must be made only on behalf of the head of an intelligence service: section 178(1), (4). The main purpose of such a warrant must be to obtain overseas-related communications, overseas-related information, or overseas-related equipment data: section 176(1).

115. In seeking the TEI warrant, the NCA had relied on section 101(1)(c), which referred to:

> "equipment belonging to, used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation."

Under section 115, the warrant required to include a description of the nature of the investigation or operation and the name of, or a description of, as many of the persons or organisations as it reasonably practicable to name or describe. Neither of the warrant applications contained an analysis of how or whether the warrant properly related to a single operation or single investigation. Rather, there was a

description of evidence of EncroChat devices in earlier NCA operations, concluding:

> "Usage is reported across the majority of high priority commodity and organised immigration crime investigations. It is assessed to be likely that EncroChat features across all of these operations."

The NCA had mischaracterised Project Venetic as an investigation and/or operation in order to try to bring it within the terms of section 101(1)(c).

116. The Claimants advanced five propositions.

117. First, interception was not in respect of a single investigation or operation. "Operation" and "investigation", in the law enforcement community, meant the detection or pursuit of a specific criminal enterprise or conspiracy. The CPS received advice to that effect in an opinion by Lord Anderson. The use of the terms "single" in the section 101(1)(e) and "particular" in section 101(1)(c) and (f) supported that construction. The Claimants referred also to paragraph 298 of the Explanatory Notes to the IPA:

> "A targeted equipment interference warrant may relate to equipment where there is a common link between multiple people, locations or organisations where the interference is for the purpose of the same investigation or operation (so, for example, computers believed to being used by Terrorist Plot Group X), or equipment that is being used for a particular activity. These latter warrants have sometimes been described as 'thematic'."

The Claimants' construction was supported also by the examples of thematic TEI warrants in the *Code of Practice* at paragraphs 5.10, 5.16, 5.30 and 5.33. By contrast, the example in the *Code of Practice* of when a bulk equipment interference warrant was needed was where data was to be obtained from devices using a "particular software package commonly, but not exclusively, used by some terrorist groups." The Tribunal should decline to follow the obiter comments in ***R*** v ***A*** at paragraphs 118 and 120 in which the court characterised the data from EncroChat devices as likely to yield information about a large but defined group of people. Such a construction was not compatible with the requirements of the ECHR or EU law: *C-623/17 Privacy International* v *Secretary of State for Foreign & Commonwealth Affairs & ors*, paragraph 81.

118. Second, interception was intended to, and did, support multiple operations. It had been used for a range of conventional operations and investigations by the NCA and regional police units.

119. Third, the safeguards surrounding thematic warrants were less stringent than those for bulk warrants, because the breadth and reach of the former was less extensive. The key determinant of which type of warrant was required was the extent to which

all the interferences could be foreseeable so that necessity and proportionality might properly be assessed: *Code of Practice* paragraph 6.5. The NCA anticipated targeting 9,000 individuals, of whom none was named in the warrant application. The NCA had asserted that EncroChat was used exclusively by criminals. Use of the platform did not of itself, however, involve committing any offence. The evidence did not support the NCA's assertion as to exclusively criminal use of the facility. Even where particular measures were valuable in preventing or detecting crime, it did not follow that they were justified: cf *S and Marper v United Kingdom* (2008) 48 EHRR 50, paragraph 125. If the IPA did not permit meaningful distinctions between thematic and bulk warrants, then the scheme of the Act was contrary to Article 8 ECHR.

120. The Claimants submitted that law enforcement agencies inevitably encounter criminal activity, and will therefore have a biased or unbalanced sample of users of the technology. They relied on conference notes from 7 October 2019 in which the users of EncroChat were described as "mainly" criminals. The expression "the majority if not all" had appeared in documents at the stage of drafting the TEI and the EIO applications. Mr Johns had acknowledged in evidence that innocent use could not be excluded as a possibility at that time, but that that had not been disclosed to the judicial Commissioner.

121. Fourth, the first TEI warrant was revoked because the French exploit had been amended to enable the EncroChat handset to identify Wi-Fi access points in the vicinity of the handset and the unique number and readable name of the access point. The NCA understood that the acquisition of such data might be regarded as bulk personal data. The collateral collection by virtue of a TEI of a bulk personal dataset as defined by section 199 would require a compelling case that such collateral intrusion was necessary and proportionate. In any event the collection was not collateral, but part of the design of the interception. That feature was not disclosed in the warrant application. If the NCA had acted with appropriate candour the TEI warrant could not have been approved.

122. Fifth, the Claimants made the following additional points by reference to the duty of candour. Mr Johns' evidence was that the question of bulk interference never arose for discussion. He said that the 2019 National Strategic Assessment concluded that the user base of EncroChat was exclusively criminal. The only explanation for the failure to consider the need for bulk warrantry was that the NCA had closed its mind to questions over whether any form of targeted warrant could ever suffice.

123. The judicial Commissioner were not provided with information as to

(a) the suitability of the operation as a target for a TEI warrant;
(b) whether the true purpose of the interception as for the purpose of a single operation; and
(c) the reliability of the NCA's asserted assessment of exclusive criminal use.

NCA submissions

124. The TEI warrant described the investigation, accurately, in this way:

> "[t]his investigation relates to the criminal use of technology in the form of the EncroChat service which is provided to the criminal fraternity."

125. It was not necessary to identify the users of the devices, their device identifiers or organised crime groups in order to be able to assess the necessity and proportionality of the TEI warrant. It was clear from paragraph 5.16 of the Code of Practice that the practicability of doing so fell to be assessed on a case by case basis. The TEI warrant explained why it was not possible to do so:

> "The EncroChat service is a highly encrypted secure communication service provided to the global criminal fraternity. The NCA Strategic Threat Assessment 2019 concluded that the platform is used exclusively by criminal users via a bespoke encrypted platform that is exploited to commit serious and organised crime whilst thwarting intelligence gathering. There is an estimated UK user base of 9000 (nine thousand) and a worldwide user base in excess of 50,000 (fifty thousand).
> Users access the EncroChat service via EncroChat handsets. These are mobile devices solely used to access the encrypted EncroChat service. The registered users of this service are unknown. The inability to attribute devices to a specific individual means that the service is popular with those involved in serious and organised crime as it prevents law enforcement accessing their communications. The registered users are provided with a randomly generated "username" which does not identify them. As a result, it is not possible to list or name all users of the EncroChat service. The NCA is aware of specific individuals using these devices who are targets of NCA operations (further details provided below under the heading "Necessity"). The NCA has been unable to attribute all EncroChat usernames to specific targets.
> It is the intention of UK law enforcement to use the information obtained by this activity to conduct other investigative tactics to identify the end users of these EncroChat devices. This will maximise any disruption opportunities to the individuals and the associated Organised Crime Groups (OCGs)."

126. The necessity and proportionality case presented to the Director General of the NCA and to the Judicial Commissioner included the following:

> "Project Venetic is the NCA's response to the UK support of a global strategic response to EncroChat devices, assessed to be used exclusively by serious and organised crime…Encrochat…is being utilised by criminals across the UK and internationally to facilitate criminality. This includes money laundering, class A drug trafficking and firearms trafficking. Encrochat is assessed by the NCA to be the most prolific 'criminally dedicated secure communications' platform in the UK with an estimated UK user base of 9000…and a worldwide use base in excess of 50,000…"
> "It is assessed by the case team that there will be minimal collateral intrusion to innocent members of the public as a result of this activity. This is because this is a dedicated criminal platform."

> "It is recognised that the proposed activity is an invasive tactic, likely to engage individuals (as yet unidentified) rights to privacy…However, such intrusion is considered justified, proportionate and necessary when balanced against the seriousness of the offences assisted by the use of these devices. It is anticipated that the data obtained by this covert activity will be used to identify those involved and maximise the disruption to their criminal enterprise."

127. The suggestion that if information was obtained under a thematic warrant for one investigation or operation which was likely to be useful for other investigations or operations (including those not yet commenced) then the interference was not for the purpose of a single investigation or operation was misconceived. That construction of the IPA would render the warrantry regime unworkable. The Tribunal should not favour a construction that defeated the purpose of the legislation: *Test Claimants in the FII Group Litigation v Revenue and Customs Comr (formerly Inland Revenue Comrs)* [2020] 3 WLR 1369, paragraph 155. The powers created by sections 99 and 101 of the IPA were very broad: *R (Privacy International) v Investigatory Powers Tribunal* [2021] QB 336, paragraph 54. Even the narrower powers under section 5 of the Intelligence Services Act 1994 which related only to specified property had been capable of authorising very wide interferences: *Privacy International*, paragraphs 61, 62.

128. The TEI warrant made it clear that the NCA expected to obtain data relating to Wi-fi access points. It acknowledged that the result might be the collection of data belonging to innocent members of the public. It explained that the individual associated with an access point could not be identified only from the data relating to Wi-fi access points. There was no want of candour. The *Code of Practice* recognised that activities involving collateral intrusion might be authorised, provided that the intrusion was proportionate to what was sought to be achieved: paragraph 5.58.

129. The Claimants relied on provisions concerning the retention of bulk personal datasets. Those were irrelevant to whether a TEI warrant could be used to obtain data which included data of innocent members of the public.

130. As a matter of fact the implant had not functioned as anticipated and the NCA did not obtain the addresses of the Wi-fi access, but only the SSID addressed with which the devices had actually connected, usually after entry of a password, to use specific Wi-fi networks.

Decision

131. The first three arguments for the Claimants are closely related and we deal with them together. The points made about candour so far as those matters are concerned raise no separate issue.

132. The Claimants submitted that a single investigation or operation denoted targets with a common link beyond the fact that they were the subjects of the investigation

or that they used a common technology incidental to their suspected criminality. We are satisfied, however, that the operation here was one to obtain material from one source, namely the EncroChat system. It was material about a large group of people, who were all users of the system. The NCA's approach was based on its assessment that the use of EncroChat was exclusively for criminal purposes. As the Divisional Court pointed out in *Privacy International*, the powers in Part 5 of the IPA are very broadly drawn. It is clear from the language of section 101(1)(c) that a TEI warrant is not restricted to equipment used by a particular person or organisation, providing that the interference is for the purpose of a single investigation or operation. Similarly, it is not restricted to situations where a group of persons share a common purpose or carry on a particular activity.

133. The investigation was characterised, for the purposes of the warrant, as one relating to the criminal use of technology. Characterising that investigation as a single investigation did not involve an error of law. As the Court of Appeal explained in *R* v *A* at paragraph 120:

> "This was an investigation into those who used EncroChat which system was thought to be a conduit for messages being passed between criminals. It was properly characterised as a thematic warrant. The fact that once the material was obtained and analysed it was conveniently divided up so that different aspects of the illegal behaviour could be prosecuted does not diminish from the nature of the overarching investigation into the misuse of this particular system."

134. That passage expresses concisely the conclusions we have reached independently.

135. There was no want of candour. The information presented to the judicial Commissioner was based explicitly on the Strategic Threat Assessment from 2019. The NCA placed before the Commissioner information that there was an interference intended with the communications of 9,000 users in the United Kingdom. An analysis and explanation as to why it was not possible to list the users was also provided. So far as proportionality is concerned, the judicial Commissioner were presented with information as to the nature of the crimes that the NCA said were being facilitated by the use of the network, to permit them to assess the matter. We do not accept that the proportionality of approving the TEI warrant required identification of the users of organised crime groups given the way in which the NCA had assessed the use of the EncroChat system.

136. On that analysis, the Claimants can succeed in challenging the issue of a TEI warrant on the basis that a bulk equipment interference warrant should been sought only if they have a proper basis for undermining the NCA's assessment, at the time of the warrant application, as to the criminal use of EncroChat. No material has been provided to the tribunal that undermines that assessment. The assessment dates from 2019 and was still current at the time of the application. It had not been created for the purposes of the application. The material which has emerged subsequently is, on our analysis, irrelevant, but in any event does not show non-

criminal use of the system. It shows very extensive use of the system for criminal purposes, and a small number of cases where the information was insufficient to show why the user had chosen to use it. In these cases there was no evidence of criminal use, but neither was there any evidence of some non-criminal use which would explain its use, see the summary at paragraphs 111 and 112 above. The NCA's contention was placed before the judicial Commissioner. The correspondence with IPCO, to which we refer in part at paragraph 53 above, indicates that there was no attempt to disguise the contention, or to underplay its significance.

137. We turn to the challenge based on a lack of candour as to collateral intrusion. The *Code of Practice* recognises that activities involving collateral intrusion might be authorised, provided that the intrusion is proportionate to what was sought to be achieved: paragraph 5.58. The TEI warrant made it clear that the NCA expected to obtain data relating to Wi-fi access points. It acknowledged that the result might be the collection of data belonging to innocent members of the public. It explained that the individual associated with an access point could not be identified only from the data relating to Wi-fi access points. The section headed "Summary of what warrant is expected to produce", included this:

> "In addition the EncroChat handset will routinely scan for Wi-Fi access points in the vicinity of the device. The implant will instruct the EncroChat handset to provide a list of those Wi-Fi access points (such as a Wi-Fi router) in the vicinity of the device. The command from the implant will result in the JIT receiving the MAC address which the unique number allocated to each Wi-Fi access point and the SSID which is the human readable name given to that access point."

138. The following information was provided under the heading "Collateral intrusion assessment":

> "It is assessed by the case team that there will be minimal collateral intrusion to innocent members of the public as a result of this activity. This is because this is a dedicated criminal platform. This operation is concerned with the illegal activities of criminal networks using these devices that impact across the entire UK and broader communities. However, due to the fact that the Wi-Fi scan will reveal data in respect of Wi-Fi access points in the vicinity of the handset it is possible that the implant will collect data in respect of those points belonging to a member of the public. However, the data that the implant receives as a result of this scan is minimal and the individual associated with that access point cannot be identified by that data alone. In addition, if the EncroChat handset device is located in the home address of the user the collateral intrusion would be minimal as the user would be assessed to be using EncroChat as a criminal platform. Any material that is obtained and does not relate directly to criminality or criminal intelligence will be dealt with in accordance with Investigatory

> Powers Act 2016 (IPA), Criminal Procedure and Investigations Act 1996, and NCA guidelines.
>
> The development of this intelligence and the disruption of this communications network are anticipated to support successful prosecutions, resulting in the expectant lengthy custodial sentences and the confiscation of the assets of those involved in the exposed criminality. Any individuals identified as not being criminally connected will be excluded from any anticipated pro-active investigations. When balanced against what the NCA seeks to achieve, in the prevention of serious and organised crime within the UK, it is assessed that this level of intrusion is justified.
>
> The following steps will also be taken in order to minimise collateral intrusion:
>
> - Activity will remain focussed on the subjects wherever possible.
> - All activity will be appropriately supervised."

139. We are satisfied on the basis of that material that there was no want of candour as to the potential for collateral intrusion.

Issues not determined, or not fully determined, in this judgment

CP's claim

140. The issue in CP's case is a discrete one which will be addressed, if necessary, at a separate hearing. It raises issues about what is said to be the recovery of messages in Dubai. We did not hear fully developed argument on this at the hearings in September and December 2022.

Whether the conduct of the NCA was authorised by the TEI warrant

141. The question of whether the conduct was authorised by the TEI warrant turns, on the Claimants' analysis, on whether the interception was interception of communications in the course of their transmission. In a case management decision on 3 March 2022 we indicated that we would assume that the admissible expert evidence contained in Professor Anderson's report was right. We indicated that if there were parts of the reports said to be inadmissible, or not properly expert evidence, we would require to deal with those arguments. We took that course with a view to determining whether or not it would be necessary to have a trial of expert evidence at a later stage.

142. As we have already recorded, the Claimants submitted that the question of whether the interception was interception of communications in the course of transmission was relevant not only to whether the conduct was authorised by the TEI warrant, but that it went to the lawfulness of the warrant itself (the Claimants' precedent fact argument), and that it was relevant to our assessment of the credibility and reliability of Ms Sweeting's evidence. For the reasons we have already given, we rejected that contention in relation to the lawfulness of the warrant. As we have recorded

above, for the purposes only of assessing Ms Sweeting's evidence, we have assumed, in the Claimants' favour, that that their contention that the interception was interception in the course of transmission.

143. The NCA submitted that there could never be a need for a trial of expert evidence in this case, and that Professor Anderson's opinions were irrelevant. They submitted that section 99(11) of the IPA obviated the need for such an inquiry. It provides that any conduct which is carried out in accordance with a warrant under Part 5 of the Act is lawful for all purposes. The NCA's contention was that later inquiry as to the nature of the exercise undertaken would, like the Claimants' precedent fact argument, undermine the protection that Parliament had intended to confer on those executing warrants. We reject that contention. The protection is conferred only when the conduct is in accordance with the warrant. It is clear that a TEI warrant cannot authorise conduct in relation to communications other than stored communications. Subsections 99(6) and (7) put that beyond doubt. Section 99(11) confers no protection against a claim that conduct was not in accordance with the law where there is interception of communications other than stored communications in purported reliance on a TEI warrant. It follows that we are satisfied that it will be necessary to determine whether the interception was of communications in the course of their transmission.

144. By the time of the hearing in September, it was clear that matters had moved on to some extent in relation to communications and co-operation between Professor Anderson and the NCA in proceedings in the Crown Court. Some of the Claimants submitted that it was likely in those proceedings that there would be clear evidence as to the means by which the French authorities obtained the EncroChat data. The NCA had a technique that they believed would extract the French applications from an EncroChat device, although there was some concern that the technique might result in the destruction of the device. At the December hearing counsel told us that two weeks earlier the NCA had extracted the relevant material from infected devices. It is likely that the Crown Court will determine what conclusions can properly be drawn from Professor Anderson's evidence. The Crown Court has jurisdiction to do so. There is no merit in a parallel trial of expert evidence before this tribunal. It would be inappropriate for us to grant a remedy on the basis of evidence "taken as read" in the knowledge that that evidence will be tested in other proceedings in early course. We defer further consideration of this chapter of the case until the outcome of the criminal proceedings is known, as explained at paragraph 8 above.

Relevant appellate court

145. The Tribunal specifies the Court of Appeal in England and Wales as the relevant appellate court for the purposes of section 67A of RIPA.

Appendix

Investigatory Powers Act 2016

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.

…….

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.

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) …….

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.

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.

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.

261Telecommunications 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.

…….

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.