Intercepted communications as evidence: The admissibility of material obtained from the encrypted messaging service EncroChat.

R v A, B, D & C [2021] EWCA Crim 128

Keywords: EncroChat; intercept; equipment Interference; admissibility; evidence

The infiltration by police investigators of the EncroChat messaging service, dubbed the "Crime Chat Network" by major media outlets, has so far led to over 800 arrests and multiple prosecutions across Europe. This has included members of Organised Crime Groups (OCGs) engaged in serious and significant criminal offending. Encrypted digital data platforms are legal and there can be genuine and legitimate motivations for their use however, the potential benefits of encrypted platforms for organised crime have not gone unnoticed by OCGs and criminal enforcement agencies. One such platform was EncroChat. The EncroChat system utilised software on Android handsets allowing users to engage directly in encrypted communication with other EncroChat users through a unique identifier or "handle". According to Europol, by "early 2020, EncroChat was one of the largest providers of encrypted digital communication with a very high share of users presumably engaged in criminal activity." (https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe, accessed 22.05.2022).

The present case arose from the infiltration of the EncroChat system, and the subsequent gathering of material on the platform by French and Dutch law enforcement agencies. At some point in 2019 French authorities developed the capability to infiltrate the EncroChat system under 'Operation Emma', described in the judgment as follows:

> …the EncroChat servers were in France and the French Gendarmerie had discovered a way to send an implant to all EncroChat devices in the world under cover of an apparent update. That implant caused the device to transmit to the French police all the data held on it. This was called the Stage 1 process…. Thereafter, in the Stage 2 process, the implant collected messages which were created after Stage 1. The Stage 2 collections occurred after what was called "the infection", which was the point at which the implant first arrived on the device and executed Stage 1. (at [12]).

EncroChat became aware of the existence of this implant on 13th June 2020 and advised its users to throw away their handsets as "Today we had our domain seized illegally by government entities(s) [sic]". Contrary to EncroChat's protestations of illegality, it was accepted in the present case that "all of the necessary legal instruments [were] in place" (at [13]) to ensure that the extraction of material from compromised devices was lawful under French law. A Joint Investigation Team (JIT), coordinated by Europol and involving French and Dutch investigators gathered data from the EncroChat system ('EncroChat material') from the 1st April 2020 until the 13th June 2020.

Based on the material shared with them, the National Crime Agency (NCA) launched Operation Venetic, an extensive criminal investigation into multiple organised OCGs and serious criminal offending. (https://www.nationalcrimeagency.gov.uk/news/operation-venetic, accessed 22.05.2022). By March 2022 more than 2,600 people had been arrested and 1,384 charged in connection with Operation Venetic (https://www.theguardian.com/world/2022/mar/14/two-guilty-of-james-bond-gun-plot-in-encrochat-conviction). A, B, D & C were amongst those arrested and charged. As part of the case against them, the Crown sought to adduce in evidence EncroChat

material which, following a 15-day preparatory hearing, Dove J ruled to be admissible. It is the appeal against Mr Justice Dove's judgment that the present case concerns.

A, B, D & C appealed four of Mr Justice Dove's rulings in the preparatory hearing [33]:

> (1) The EncroChat communications were intercepted whilst being stored, not when being transmitted, thereby making them admissible.
>
> (2) In the alternative, no offence was committed under s.3 Investigatory Powers Act 2016 (IPA) as the interception was not done in the UK so could not be excluded by s.56 of the Act.
>
> (3) The prohibition on requesting mutual assistance under s.10 IPA did not apply, because the European Investigation Order (EIO) made no request that fell under s.10. In the alternative, the request was in exercise of a statutory power, making it permissible under s.10 (2A).
>
> (4) The prohibition under s.9 on an overseas authority carrying out interception without a Part 2 warrant did not apply because the activities of the French and Dutch authorities were not pursuant to a request by the UK authorities.

Of these four rulings, the central question for the court in this appeal was "whether the communications were intercepted at the time they were being transmitted [in which case they would be inadmissible] or, as the judge found, were recovered (intercepted) from storage. If the judge was right, subject to a number of subsidiary arguments, the evidence would be admissible." (at [1]).

HELD, rejecting all four grounds and dismissing the appeal, at the time that the EncroChat material was obtained it was being stored in rather than transmitted by the system and was therefore *prima facie* admissible in evidence (at [79]).

On Ground 1 the court found that the material was obtained by way of "a process which is like any other means of downloading the content of a mobile phone handset. It is done remotely, but it is done by interrogating the RAM of the phone, not by intercepting the communication after it has left the phone." (at [63]). Further the court determined that "What remains on the device is not what has been transmitted, but a copy of it or what, in older forms of messaging, might be described as a "draft"." (at [66]). Thus, as the handsets formed part of a telecommunications system, the material was being stored in or by the system and not being transmitted at the time of interception: "That being so, the harvesting was interception but was rendered lawful by the Targeted Equipment Interference warrants issued under section 99 of the [2016] Act." (at [67]). This decision on Ground 1 rendered consideration of Ground 2 unnecessary.

On Grounds 3 and 4 the court acknowledged the potential for a challenge to be brought under s.78 Police and Criminal Evidence Act (PACE) 1984 on the basis of non-compliance with ss.9 & 10 of the IPA despite the fact that "Compliance with sections 9 and 10 is not a statutory condition of admissibility" (at [71]) under s.61(1)(c) IPA. The court observed that "It would be a surprising exercise of that power to exclude evidence which Parliament has provided in clear terms should be admissible" (at [71]) but nevertheless deemed the Grounds worthy of consideration.

On Ground 3 the court held, contrary to the position of Dove J, that the EIO did constitute "a "request" for the purposes of section 10 [IPA]" (at [75]) however, consistent with the alternative

ruling of Dove J, that also meant that the EIO involved the exercise of a statutory power making it permissible under s.10(2A) IPA and as such Ground 3 was "without merit" (at [75]).

On Ground 4 the court upheld the decision of Dove J that s.9 IPA "governs only a "request" made by means other than an EU mutual assistance instrument or an international mutual assistance agreement." (at [78]). No such request was made by the UK with the request for access to the material falling under s.10 IPA (as per Ground 3, above).

Ultimately the court "concluded that the only substantial question which the judge was required to answer was whether the EncroChat material was stored by or in the telecommunications system when it was intercepted." (at [79]). As discussed above in the context of Ground 1, on that question the court agreed with the ruling of Dove J at the preliminary hearing and dismissed the appeal accordingly.

Commentary:

To understand the significance of the decision in the present case it is important to consider the broader context in which the appeal was brought. As a result of Operation Venetic, described by the NCA as the "biggest and most significant operation of its kind in the UK" (https://www.nationalcrimeagency.gov.uk/news/operation-venetic, accessed 22.05.2022), some 1,348 people were charged and at least 260 convicted of various offences as of March 2022 (https://www.theguardian.com/world/2022/mar/14/two-guilty-of-james-bond-gun-plot-in-encrochat-conviction, accessed 27.05.2022). Many of these prosecutions were ongoing at the time of the appeal in the present case and it is reasonable to assume that several them would have been placed in significant jeopardy had the court in the present case determined the EncroChat material to have been inadmissible.

The convictions of Paul Fontaine and Frankie Sinclair, the first defendants to be convicted of conspiracy to murder based on EncroChat material and the subject matter of the newspaper article cited above provide a cogent example. Both men were convicted of conspiracy to kill a rival drug dealer in retaliation for a previous shooting incident. In respect of Fontaine defence counsel highlighted that "there was no DNA, no fingerprints, no eyewitness, no actual drugs or guns. Nothing. All the evidence depends on EncroChat." (The Guardian, above). No such conviction would have been possible had the EncroChat material been ruled inadmissible.

Hearsay

Hearsay barely featured in this particular EncroChat judgment. Assumedly, the judges were satisfied the Encrochat messages aligned with Lord Hughes' logic surrounding text messages in *R v Twist and Others* [2011] EWCA Crim 1143, that Encrochat messages did not amount to hearsay as they were based in a 'common understanding'. When determining the admissibility of material contained in telecommunications involving a defendant it is important when applying the statute to distinguish between:

i) the speaker wishing the hearer to act upon his message; and

ii) the speaker wishing the hearer to act upon the basis that a matter stated in the message is as stated (i.e. true).

Only the second will bring into operation the hearsay rules (*Twist,* at [16]). Where a communication falls outside of the scope of the hearsay provisions the probative value of the evidence is then a matter for the jury [*Twist,* at [21]). It is submitted that the court was correct to proceed on this basis in respect of the EncroChat material.

Interception during transmission or from storage and the importance of the distinction.

Of much greater significance was the question of whether the EncroChat material was intercepted during transmission from, or whilst being stored by or in, the telecommunications system. Historically, intercept material could be lawfully obtained by the authorities for intelligence use but not for use as evidence in criminal proceedings (at [8]). Other European jurisdictions faced no such evidential hurdles as intercept evidence is permitted into trial within those jurisdictions. The blanket ban on "interception-related content" in the UK was removed by the IPA. Interception-related content remains inadmissible under Section 56 of the Act, but significant exceptions have been introduced.

Section 4 of the IPA defines 'interception' as being whether the material was "being transmitted" at the time it was accessed or whether it was being "stored in or by the telecommunication system". In both instances, there is interception, but under the IPA, stored intercepted material may be admissible. Section 56(1) of IPA states that: "*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."*

The exceptions in Schedule 3 are as follows:

Schedule 3(2)(1)(a) states that 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… sections 6(1)(c) and 44 to 52."*

Section 6(1)(c)(i) significantly clarifies that *"for the purposes of this Act, a person has lawful authority to carry out an interception if, and only if… in the case of a communication* ***stored in or by a telecommunication system,*** *the interception - 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."*

The NCA had obtained just such a Targeted Equipment Interference warrant under Part 5, approved by a Judicial Commissioner and the Investigatory Powers Commissioner.

Realm and RAM

The 15-day long preparatory hearing might be explained by the hearing of extensive expert evidence on the workings of the handsets and the broader EncroChat system. The relevance of this evidence was largely dismissed in this judgment: 'The 2016 Act does not use technical terms in this area. The

experts have an important role in explaining how a system works, but no role whatever in construing an Act of Parliament.' (at [68]).

The Court of Appeal focused primarily upon the legality and the route to admissibility for material "harvested" from the EncroChat system: "The issue is whether the communications were intercepted while they were being transmitted or while they were stored in or by the system." (at [51]).

The EncroChat messages were construed as essentially the same as any data downloaded from a mobile phone handset, albeit downloaded remotely. The material was "stored" when it was intercepted. The only technical issue before the court was in determining when transmission began and when it ended. The ultimate decision on a potentially technically complex point rested on whether the information obtained was encrypted or not: "The fact that what was obtained was an *unencrypted message*, means that what was on the phone, and what was intercepted, was *not the same as what had been transmitted* because what had been transmitted was encrypted. It cannot therefore have been "being transmitted" when it was intercepted: it can only have been "being stored" (at [66]).

The importance of the expert evidence

The Court was dealing with principle and admissibility rather than technical arguments about the EncroChat system. This was articulated by the court (at [55]):

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

Taken at face value this appears to be a sensible approach. The avoidance of an overly technical focus allows the court to lay down general principles, consistent with the intention of the statutory provisions and less likely to be rendered obsolete by ongoing technical changes. As identified in the extract from the judgment above, the job of the court is to **understand the system** and then make a determination about how the material was obtained. In order to achieve the first step, the court will often require the assistance of experts. As is well established, and now contained in Part 19A.1 of the Criminal Practice Direction (Crim PD), expert opinion evidence is admissible at common law if it is relevant to a material issue in the proceedings, the matter with which the court requires the assistance of the expert falls outside of the "knowledge and experience of the court" (*R v Turner* [1975] 1 All ER 70) and the expert is competent (or "peritus", see e.g. *R v Silverlock* [1894] 2 QB 766).

Relatively recent amendments to Part 19 of the Criminal Procedure Rules (Crim PR) and to the associated Crim PD, based in part on the decision of the Court of Appeal in *R v Dlugosz and others* [2013] EWCA Crim 2, require the court to consider whether the expert opinion evidence is founded on a "sufficiently reliable scientific basis for the evidence to be admitted." (*Dlugosz* [at 11]). Whether such amendments amount to the creation of a discreet admissibility criterion remains a moot point

(see e.g. Stockdale, M and Jackson, A, Expert Evidence in Criminal Proceedings: Current Challenges and Opportunities, (2016) *J. Crim. L*. 80(5)) but it certainly the case that where a court determines that expert opinion evidence lacks sufficient reliability it may be properly excluded on that basis.

The NCA were permitted access to the EncroChat material gathered by the JIT pursuant to an EIO issued by UK authorities (at [13]). The lawfulness of the EIO was separately challenged in *R (C) v DPP* [2020] EWHC 2967 (Admin) before Singh LJ and Dove J who refused an application seeking judicial review of the granting of the EIO and finding the Order to have been properly obtained. As discussed above, further challenges to the lawfulness of this process were brought and dismissed under grounds 3 and 4.

What remains less clear from the judgment in the present case was the way in which the EncroChat system was initially infiltrated and the material gathered by the original investigators. Whilst the court engaged in a detailed consideration of the workings of the EncroChat system for the purposes of determining whether the material gathered was intercept material (Part 2, IPA) or, as determined, equipment interference material (Part 5, IPA) it does not appear to have applied the same level of scrutiny to the reliability of the technique(s) used to gather the material in the first place. The court satisfied itself (at [13]) that;

(i) The French has all of the necessary legal instruments in place to undertake the extraction of the material from the devices all over the world lawfully as a matter of French law.
(ii) The implant was loaded by the French Authorities on to the EncroChat servers in Roubaix and then via the servers uploaded on to all EncroChat devices worldwide.

The approach of the court in the present case therefore appears to have operated on the assumption that the technique(s) used to infiltrate and gather material from the EncroChat system were reliable *per se* without full details about how the material was gathered. The decision of the French authorities to withhold details about the exact manner in which the EncroChat system was infiltrated on the basis of "defence secrecy" was unsuccessfully challenged in the French Constitutional Court (Décision no 2022-987 QPC du 8 avril 2022). Ironically, the protection from scrutiny of the covert capabilities of the security services remains one of the long-standing justifications for the restrictions on the use of intercept material as evidence in the United Kingdom.

Crim PD 19.5 provides a non-exhaustive list of factors to be taken into account by a court seeking to determine the reliability of expert opinion evidence. This list includes *inter alia*; "the extent and quality of the data on which the expert's opinion is based, and the validity of the methods by which they were obtained" (Crim PD 19.5 (a)), "if the expert's opinion relies on the results of the use of any method (for instance, a test, measurement or survey), whether the opinion takes proper account of matters, such as the degree of precision or margin of uncertainty, affecting the accuracy or reliability of those results" (Crim PD 19.5 (c)) and "the completeness of the information which was available to the expert, and whether the expert took account of all relevant information in arriving at the opinion (including information as to the context of any facts to which the opinion relates)" (Crim PD 19.5 (f)). It is difficult to see how any of these questions can be answered with any degree of certainty, and therefore any proper determination of reliability be made, whilst the exact manner in which the material was obtained remains unclear. If the technique(s) utilised to infiltrate and gather the EncroChat material are in fact sound, then the issue is more of academic than practical concern. However, if the technique(s) are subsequently shown to be flawed it will cast serious doubt on the evidentiary reliability of the evidence subsequently gathered. Possibly of greater concern is how, in a process shrouded in secrecy, any such flaws might come to light.

Conclusions and the future of EncroChat cases

Following the present judgment, it is likely we will see further EncroChat-related prosecutions as appetite to prosecute can only increase. For those prosecuting or defending EncroChat-related cases in the future, there are two immediate conclusions to be considered. The first relates to any argument for exclusion of such material under s.78 PACE. The Court of Appeal has upheld Mr Justice Dove's judgment in *R v Coggins* (2020), Liverpool Crown Court, unreported that EncroChat messages ought not to be excluded under S.78 of PACE, or for any arguments of abuse of process. Defence teams should pay heed to the Court of Appeal's warning: "*If it is intended to repeat this kind of process in other pending cases involving EncroChat material, those involved should not be surprised if the trial judges deal with them rather more briskly*" (at [6]).

A further consideration for defence teams lies in recent judgments surrounding EncroChat and sentencing. In the case of *R v Nelson & Markham* [2020] EWCA Crim 718, confirmed in *R v English & Read* [2020] EWCA Crim 100, the Court of Appeal ruled the use of encrypted devices by drug dealers to be an aggravating factor, reflecting sophistication of the organisation.

Whilst questions may remain about whether the court may entertain further challenges based on the reliability of material obtained from the EncroChat system what is now clear is that, where the prosecution has lawfully obtained data which has been stored on handsets, whether as draft communications or otherwise, those messages are admissible. A broader question for consideration is whether we have now reached a point, notwithstanding the relatively recent introduction of the IPA, where Parliament should legislate to allow the more general admission of intercept evidence within an appropriate statutory framework.

The authors would like to thank Ian Whitehurst at Exchange Chambers for his insights.

Cerian Griffiths and Adam Jackson