GENERAL CRIME CASE COMMENT

Cracking the Enigma Code: A, B, D & C and Regina [2021] EWCA Crim 128

Date: 25th February 2021

Contacts at QEB: Roger Smart and Oliver Mosley

In 2016, a service was launched by a French company called EncroChat. The company provided modified phones with specialist software pre-loaded onto them, and for a monthly fee you'd receive the device plus a contract for their service. The company's claim was to offer its users privacy and encrypted messaging on the "*world's most secure handset*".

The devices were actually Android phones, but any feature that could be vulnerable to hacking, like the camera, microphone and GPS services, was disabled. When certain buttons were pressed, the device would allow the user to access a specialist messaging service. Not only would your messages be encrypted, but they could self-delete shortly after being sent. By pressing another combination of buttons, the device would be wiped entirely.

There was nothing about this service that was illegal. EncroChat was not the first to offer encrypted messaging or self-delete functions (bigger companies like WhatsApp and Snapchat had got there first) but the 'bundle' of a secure, easy-to-erase handset with pre-loaded encrypted services made it especially attractive to criminals.

The service was a quick success; the company had 60,000 users worldwide and around 10,000 users in the United Kingdom.[1] In the same year it launched, it found itself on the radar of the National Crime Agency ('NCA') in the UK, as well as the French and Dutch authorities. In the summer of 2020, a French and Dutch joint operation successfully "*infiltrated the platform*". Without users realising, the messages they were sending and receiving were being read by law enforcement.

In June 2020, EncroChat sent all users a message saying the platform had been hacked, and that handsets should be thrown away. EncroChat shut down permanently later that month. By July 2020, 746 suspects in the UK had been arrested and over £54m in alleged criminal proceeds had been seized. The NCA claimed to have prevented over 200 threats to life. "*My*

[1] https://www.nationalcrimeagency.gov.uk/news/operation-venetic

team described this as the equivalent to the cracking of the Enigma Code," said Nikki Holland, Director of the NCA.

* * *

The question for the courts was whether EncroChat material was admissible. *A, B, D & C* became the test case, first considered by Dove J sitting at the Crown Court at Liverpool and now by Burnett CJ, Edis LJ and Whipple LJ in the Court of Appeal.

The historic position was that intercepted material was lawfully obtainable but inadmissible in criminal proceedings. Other European jurisdictions like France and the Netherlands have no-such blanket prohibition. That position changed in the UK with the passage of the Investigatory Powers Act 2016 ('the Act'). Although "*interception-related content*" was still inadmissible in legal proceedings under Section 56 of the Act, there were now important exceptions.

Dove J directed a preparatory hearing given the importance and complexity of the issue. After a 15-day hearing in November/December 2020, a much-anticipated written ruling was handed down in January 2021. Dove J held the material was admissible, amongst other matters. It was that decision that fell to be examined by the Court of Appeal.

Understanding Dove J's ruling requires an understanding of how the material was obtained by the NCA. The French and Dutch authorities had found a way to load their software onto EncroChat's servers in Roubaix, which in turn sent that software on to all EncroChat devices. Users would have thought it was a standard software update from EncroChat, but the 'update' in fact caused the recipient device to send all message data on it to the authorities. EncroChat devices typically had 7-days' worth of messages stored in the memory. The update would then collect all messages that were created after this point and transmit them as well. The material was sent to the French police digital crime unit ('C3N') and then onto Europol. From there, the material was handed over to the NCA in the UK via a European Investigation Order.

The question under Section 4 of the Act, which defines 'interception', was whether the material was "*being transmitted*" at the time it was accessed or whether it was being "*stored in or by the telecommunication system*" (i.e. the EncroChat device). Both are types of interception, but a combination of Section 56 (1), Schedule 3 (2) (a) and Section 6 (1) (c) means that intercepted material that is being stored is admissible, whereas material being transmitted is not.

Dove J held the intercepted material was being stored, as it was being accessed from the device's memory and then copied to the Police:

"*The effect of the implant was to lead to exfiltration of the messages from the devices: the messages were not taken after they had left the device or the sender or before they had arrived on the device of the receiver*".

This was how the Police got round the issue of encryption; they were either copying a message before it left the device (pre-encryption) or after the message had arrived (post-encryption).

* * *

There were four decisions by Dove J that the appellants challenged, which are set out in-full at paragraph [33] of the judgment. To paraphrase them:

(1) The EncroChat communications were intercepted whilst being stored, not when being transmitted, making them admissible.

(2) In the alternative, the interception was not done in the UK so could not be excluded by Section 56 of the Act regardless.

(3) The prohibition on requesting mutual assistance under Section 10 of the Act did not apply, because the European Investigation Order made no request that fell under Section 10 or, in the alternative, the request was in exercise of a statutory power and so was permissible under Section 10 (2A) regardless.

(4) The prohibition under Section 9 on an overseas authority carrying out interception without a Part 2 warrant did not apply because the activities of the French/Dutch authorities were not pursuant to a request by the UK authorities.

The first decision was the main part of the appeal. The Court firstly rejected the need to examine how the system worked in minute detail: Parliament intended 'transmission' and 'stored' to carry their ordinary meanings. Attempts to read more context-specific interpretations into the Act ran against the statutory wording and, given the pace of technological change, would render it less effective. Instead, the Court held the wording of Section 4 (4)(b) was clear and unambiguous: it applied to all communications stored on the system.

A Court therefore need only consider one question, "*was the communication stored by or in the system at the time when it was intercepted*". The answer to that question was 'yes'. The judgment also rejects a key appellant submission, that a message is transmitted as soon as the person presses 'send'. This would suggest anything that happened after pressing send would be intercepting a transmission. The Court disagreed, agreeing with Dove J that transmission takes place "*after the communication has been put into its final form*" [64] by the device. The

material that "*remains on the device is not what has been transmitted, but a copy of it*" [68]. It was acknowledged that the experts thought differently, they argued the communication appearing in the memory was an essential part of the process of transmission, but ultimately what counts as 'transmission' is a question of statutory interpretation, not technical evidence, and therefore one for the Court to determine.

Given the ruling on interception, there was consequentially no need to consider if Section 56 even applied to interceptions not done in the UK.

The Court went on to consider Section 10 of the Act, namely the prohibition on using mutual assistance to request interception without a mutual assistance warrant under Section 10 (2). Dove J concluded that the interception was going to happen anyway, so the UK were not 'requesting' interception, but alternatively held Section 10 (2) didn't apply because the request was in exercise of a statutory power, namely the power to make a European Investigation Order, and therefore came under the allowance under Section 10 (2A). The Court of Appeal agreed with the alternative position. The UK was clearly making a request "*in connection with*" interception which therefore triggered Section 10 (2), but given they were exercising a statutory power, Section 10 (2A) allowed them to do so. They noted that Section 10 (2A) was enacted specifically to include European Investigation Orders.

On the Section 9 issue, the final ground of appeal, Dove J had found there was no request to carry out interception, and that Section 9 didn't apply to material stored in or by the system anyway. The Court of Appeal agreed; the proper construction of Section 9 was a restriction on asking a foreign state to carry out interception that, if done in the UK, would require a Part 2 warrant. Material requiring a Part 2 warrant was that intercepted during transmission. By virtue of the ruling on Ground 1, Section 9 couldn't apply.

Ultimately, although Grounds 2 to 4 of the appeal may be of interest to those who enjoy the complexities of the Act, the crux of the appeal was decided on Ground 1. The Court of Appeal has upheld Dove J's approach: the EncroChat material was not being transmitted when it was intercepted and was therefore admissible.

* * *

The implications for this judgment are clear, the Court of Appeal have given their firm view that EncroChat material is admissible. It will likely form the basis of hundreds of prosecutions over the next few years. The Court have also closed the door for future appeals on these grounds:

"*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*".

An unresolved question from the appeal is whether mobile phone handsets are actually covered by the 2016 Act at all. The parties agreed that handsets were part of the "*public telecommunications system*". The Act only applies if you accept this premise. Notwithstanding the parties' agreement, the Court of Appeal expressed reservations about this given the vast number of things a smartphone can do, but the Court hasn't resolved the issue.

The implications here are potentially vast. Given the variety of ways we can now exchange data with smartphone apps, it remains to be seen if the 2016 Act protects this data from interception and use in criminal proceedings.

* * *

Please note that the judgment of A, B, D & C and Regina [2021] EWCA Crim 128 is currently subject to reporting restrictions. Reporting is permitted of the Court of Appeal judgment only. All the information in this article is therefore taken from the Court of Appeal judgment and material from public sources, and not the judgment of Dove J sitting at the Crown Court at Liverpool.

QEB Hollis Whiteman
1-2 Laurence Pountney Hill, London EC4R 0EU
DX: 858 London City Telephone 020 7933 8855 Fax 020 7929 3732
barristers@qebhw.co.uk www.qebholliswhiteman.co.uk