Admissibility of EncroChat evidence in criminal proceedings (R v A and others)

Corporate Crime analysis: In R v A and others, the Court of Appeal were asked to determine whether evidence obtained from the EncroChat application could be admitted in evidence in criminal proceedings, or whether it is excluded by the Investigatory Powers Act 2016 (IPA 2016). The Court of Appeal held that the EncroChat material was admissible as the material was being stored in or by the system at the relevant time (IPA 2016, s 4(4)(b)). They further held that the interception was carried out in accordance with a targeted equipment interference warrant under Part 5 and thus concluded that there was lawful authority for the interception. As the EncroChat material fell under the exception to IPA 2016, s 56(1)(a), the content of the communications were not prohibited from being disclosed. Alexandra Wilson, barrister at 5 St Andrew's Hill, explains the decision of the Court of Appeal.

R v A and others [2021] EWCA Crim 128, [2021] All ER (D) 83 (Feb)

The main question for the court to consider was:

- were the communications intercepted while they were being transmitted or while they were being stored in or by the system?

The court set out that if it was the latter, subject to some subsidiary arguments, the evidence would be admissible.

The law

IPA 2016, s 56(1) sets out 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.'

IPA 2016, s 56 is subject to exceptions set out in IPA 2016, Sch 3.

IPA 2016, Sch 3 para (2)(1)(a) sets out that IPA 2016, s 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'.

IPA 2016, s 6(1)(c)(i) sets out 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'.

IPA 2016, s 4(1) sets out that 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.'

IPA 2016, s 4(4) defines the 'relevant time' in relation to a communication transmitted by means of a telecommunications as:

> '(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).'

Thus the ultimate question for the judge to decide was whether the communication, at the relevant time of extraction, was 'being transmitted' (IPA 2016, s 4(4)(a)) or 'stored in or by the [telecommunication] system (whether before or after its transmission)' (IPA 2016, s 4(4)(b)).

If it was being stored (IPA 2016, s 4(4)(b)) and the interception was carried out in accordance with a targeted equipment interference warrant under Part 5 (IPA 2016, s 6(1)(c)(i)) then there would be lawful authority for the interception. If that was the case, then the interception would fall under the IPA 2016, Sch 3 para (2)(1)(a) exception to IPA 2016, s 56(1)(a), which means the content of the communication would not be prohibited from being disclosed.

The preparatory hearing

At this Crown Court hearing, the judge considered the question above and concluded that the communications were intercepted while they were being stored in or by the system. The judge decided that the EncroChat material obtained by the National Crime Agency is admissible as evidence against the appellants in their pending criminal proceedings.

While it is not relevant to this appeal, the judge also rejected the submission that he should exclude the EncroChat material under section 78 of the Police and Criminal Evidence Act 1984; and the submission that he should stay the criminal proceedings as an abuse of process of the court. These two decisions were not appealed.

Case history

A French and Dutch Joint Investigatory Team (JIT) obtained the EncroChat material. The JIT supplied the material obtained to the UK authorities. The EncroChat servers were in France and the French Gendarmerie sent an implant to all EncroChat devices under the cover of an 'update'. The implant caused the device to transmit to the French police all of the data held on it (stage one). It captured all data that had not been erased (eg the last seven days' worth of communications) and sent it to the C3N server, the French police digital crime unit server, and then on to the server at Europol. The implant continued to collect messages which were created after the 'update' (stage two).

'Stage two' is the main issue for this appeal. The court were asked to determine whether the intercept of messages in stage two occurred while the messages were being transmitted or while they were being stored in or by the system.

The task for the Crown Court judge was to firstly determine how the JIT obtained the EncroChat material and then secondly apply the UK domestic law on admissibility (IPA 2016).

The factual background is set out in detail in the decision refusing permission to pursue judicial review proceedings challenging the European Investigation Order (*R (C) v Director of Public Prosecutions* [2020] EWHC 2967 (Admin), [2020] 4 WLR 158).

The appellant's main argument: The EncroChat material is inadmissible in criminal proceedings because it is 'intercept material' (IPA 2016, s 56)—as it was being transmitted at the time it was taken.

The prosecution's main argument: The EncroChat messages were admissible and fell within the exception provided by IPA 2016, s 56(1) and IPA 2016, Sch 3 para (2)(1)(a) because the messages were 'stored in or by the system' at the time when they were intercepted; and, in any event.

Findings of fact

How EncroChat worked:

To use EncroChat the user would need to:

- send the message (the app ensured its encryption)
- compose a message for an identified contact (this would be held in RAM for the purposes of the app)
- open the app on the device (the app's program and some of its data would be drawn from Realm (a form of memory which holds an archive of apps and data for use on the device) into RAM (a form of memory which is a faster and temporary type of memory which holds apps and data while the app is running on the device and is used for the operation of the app in supporting the activity of the CPU) for use by the CPU to send/receive messages)
- the message would be sent from the user's device to the radio chip and antenna for it to be transmitted out of the device to the EncroChat server. The message would pass through

the EncroChat server via the receiver's message queue and arrive on the receiving device when it was switched on and running the app
- the message would be decrypted on the device, matched with other information on the receiving device (eg the sender's nickname) and held in RAM to be displayed on the device's screen or to be forwarded to other contacts
- the message would only be sent to Realm when the app was closed or the device was turned off. If the message was deleted prior to either of these, it would not be sent to Realm

How the implant worked:

- the implant took the messages from the devices, either before encryption (on sending) or after decryption (on receiving)
- the implant did not take the messages in the period of time from when the messages were sent from one device and received on another

With the stage one data, the implant copied data already on the device (from Realm) and sent it to C3N. With the stage two data, the implant copied data held in RAM and sent it to C3N. It worked like spyware on the devices. The 'received'-message evidence was married to user nicknames showing it had been combined with Realm data and not extracted during transmission. The 'received' data was not identical to the 'sent' data.

The court's decision

The judge had to decide whether the communication, at the relevant time of extraction, was 'being transmitted' (IPA 2016, s 4(4)(a)) or 'stored in or by the [telecommunication] system (whether before or after its transmission)' (IPA 2016, s 4(4)(b)).

The judge concluded that the EncroChat was stored in or by the system (IPA 2016, s 4(4)(b)), for the following reasons:

- there are only two alternatives—being transmitted or being stored
- the messages were not being transmitted when the data was taken
    - when taken from the sender's device—the message was stored on the device in RAM and copied from there by the implant before encryption
    - when taken from the receiver's device—the fact that there were nicknames for senders in the data from receiver's devices show that transmission had finished
- the communications were copied from data which was held on the device, the copy was sent to the C3N server

The Court of Appeal agreed with the Crown Court judge that the EncroChat material is admissible. They agreed that the material was being stored in or by the system at the relevant time (IPA 2016, s 4(4)(b)). They also agreed that the interception was carried out in accordance with a targeted equipment interference warrant under CPR 5 (IPA 2016, s 6(1)(c)(i)) and thus concluded that there was lawful authority for the interception. The interception of the EncroChat material has thus been found to fall under the IPA 2016, Sch 3 para (2)(1)(a) exception to IPA 2016, s 56(1)(a), which means the content of the communications are not prohibited from being disclosed.

Please note that there were other arguments advanced by the appellant, which have not been summarised here due to the length of the judgment.

Alexandra Wilson is a barrister specialising in criminal and family law. In her criminal law practice, she represents a variety of clients charged with serious matters and specialises in young and vulnerable clients. She has written a number of articles in relation to the EncroChat hack and has presented a webinar on the issues involved.

This article was first published by 5 St Andrew's Hill on 18 February 2021 and is republished with permission.