THE ENCROCHAT STORY

PAUL GREANEY Q.C.

Introduction

1. Throughout history, those involved in crime have wanted to keep communications about their criminal activities secret. That much is entirely unsurprising. In the electronic age this has involved attempting to identify methods of encrypted communication that law enforcement authorities could not penetrate. At an early stage, that involved the use of PGP, but by 2016 this technology no longer provided any significant degree of protection from law enforcement. Out of the ashes of PGP, a number of other companies emerged, making high claims about the level of encryption offered by their services and their impenetrability. Chief among those companies was the Dutch outfit EncroChat, whose handsets became the industry standard among Organised Criminal Networks ("OCNs"). But, on the night of 12th to 13th June 2020, EncroChat sent a message to its users' handsets informing them that it feared it had been hacked, that it was no longer able to guarantee the security of its devices and advising users to dispose of their devices immediately. EncroChat's fears were well-founded. Its servers had been attacked by law enforcement authorities and, as a consequence, since June, many hundreds of arrests have been made across Europe, and drugs, cash and firearms in substantial quantities have been seized. It is said that major conspiracies, including conspiracies to murder have been disrupted. In England, the response to the EncroChat hack has been led by the National Crime Agency. Trials of those arrested in England are some way off, but the obvious question is what the courts will make of the hacked evidence.

History

2. PGP stands for "Pretty Good Privacy" and at its inception was intended for use as a human rights tool, designed to ensure complete privacy in electronic communications. Blackberry mobile telephone handsets were commonly used with PGP software because they offered resilience to attempts to access the device content. Quickly, criminals identified the benefits of PGP and PGP-enabled handsets began to be used across OCNs.

Companies such as GhostPGP, Phantom Secure, PGP Safe and Ennetcom were set up, offering a PGP-enabled device for between £1,000 and £2,000. The device would typically function for six months before a further payment was required. The devices were commonly able to communicate only with other handsets belonging to members of the particular OCN concerned and had functions save for instant messaging disabled; they also often had remote wipe settings (or "kill pills") enabled.

3. From 2016, law enforcement authorities launched an offensive against these PGP providers. In April 2016, Dutch police arrested the head of Ennetcom. They seized servers in both the Netherlands and Canada and the Canadian authorities were able to access message content. The following month, suspects linked to PGP Safe were arrested and in March 2018, Phantom Secure was dismantled. These actions, together with the increasing ability of law enforcement authorities to decrypt PGP-enabled devices led to a decrease in the use of this technology within the criminal community. In parallel with that decrease, the authorities saw a proliferation in the use of devices provided by companies marketing themselves as a replacement for and improvement on PGP encryption. EncroChat was one of the leaders in that new movement.

EncroChat

4. EncroChat was based in the Netherlands. Its handsets were not available in standard mobile phone shops, but instead were advertised via the Internet and distributed in the same way, or via small, privately-owned shops. The handsets that were used to install the software (often the Aquaris X) when bought without EncroChat commonly cost no more than £300. Once enabled with EncroChat, they are believed to have sold for about £1,500 for six months' use. Thus, EncroChat was an expensive and, inferentially, valuable tool for the criminal fraternity.

5. EncroChat allowed an enabled handset to be booted up in two different ways. If booted up by the power button being depressed, the handset would appear to be an ordinary Android device, but if booted up with a different combination of button presses, the EncroChat functionality was revealed. In that mode, encrypted emails could be sent and encrypted calls made (although for a small number of minutes over the entire six-month period) but the function mainly used was an instant messaging service. Generally, the devices could be used to contact only other members of the same OCN. Messages would commonly delete after a set period of time and kill pills could be sent. But in any event,

it was thought that law enforcement authorities could not break the encryption afforded by EncroChat. That was EncroChat's USP.

6. Although the authorities had been aware of EncroChat since 2015, the existence of the company only came to public attention during the trial of two Manchester criminals for the murders of Paul Massey and John Kinsella, two prominent figures in the gangland of the North West[1]. The two men charged were called Mark Fellows and Steven Boyle. The evidence revealed that they had communicated using EncroChat-enabled handsets in order to carry out the murder of John Kinsella, although at the time in 2018, decryption was unavailable. But the simple fact of their use of devices employed only by criminals was used against them at trial.

Recent Developments

7. In June 2020, the criminal community's confidence that EncroChat was incapable of being penetrated was burst open. EncroChat sent its members the message I have set out above and quickly thereafter shut down completely. Since then, many many arrests have occurred. It seems clear that law enforcement officials have penetrated the EncroChat servers. Quite how this was achieved remains to be seen. It appears from a press conference given on 2nd July 2020[2] by Europol (which supports the EU member states in their fight against, inter alia, serious and organised crime) and Eurojust (the EU agency for criminal justice co-operation) that the investigation was initially driven by the French, who swiftly brought in the Dutch. Later still, information was provided to other countries, including the UK. Still, we do not know exactly how the penetration of the servers was achieved. Speculation on the Internet refers to the French authorities having installed a *"technical tool"* that enabled them to record messages for months. Whether this was achieved lawfully remains to be seen.

8. It is beyond doubt that there will be trials in England based solely or largely on evidence deriving from the penetration of the EncroChat servers. Inevitably, there will be challenges at those trials. Some of those challenges will be based in and on the facts of the individual cases with defendants maintaining that a particular handset and/or messages are not correctly attributed to them. These are defences we have often seen for many years in prosecutions reliant upon telecommunications data and these defences will call for no

[1] https://www.liverpoolecho.co.uk/news/liverpool-news/sold-liverpool-3k-year-mobile-15652444
[2] https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe. The press conference can also be watched on-line.

special or different approach from that we have always adopted. But there will obviously also be challenges based upon the **circumstances in which the data was obtained**. These challenges will likely take the following forms:

a. First, consideration will be given to whether the circumstances in which the data was obtained offends *"the court's sense of justice and propriety"*. The courts have power to stay (or stop) cases where this is so[3], but it is right to say that this is a power that is rarely exercised.

b. Second, there will be investigation into whether the circumstances in which the data was obtained from the Encrochat servers render a fair trial of the defendant impossible. Again, the courts have power to stay cases where this is so. Challenges under this head will be likely to focus not just upon the legality of what was done by the French and English, but also upon the reliability of what has been obtained as a result and the ability of the defence to understand and challenge what has occurred. If it proves to be the case that shadowy techniques were used to obtain the data and that the defence cannot analyse the accuracy of what has resulted or trace attribution because the servers are no longer available, there may be real issues about whether defendants can fairly be tried.

c. Third, applications to exclude EncroChat data may be made pursuant to section 78 of the *Police and Criminal Evidence Act 1984* on the basis that the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it. This will engage similar issues in relation to legality and reliability.

9. Before practitioners are able to make informed decisions about whether any of these challenges is realistic in any particular case, much more will need to be known about the circumstances in which the data was hacked or harvested. However, I have little doubt that challenges will be available and will be made. A decision of the Court of Appeal Criminal Division is to be expected at an early stage, in order that the Crown Court approaches what will be many cases in a consistent way.

13th July 2020

[3] See, for example, *Warren v Attorney General of Jersey [2012] 1 A.C. 22*.

Paul Greaney Q.C. is a barrister at New Park Court Chambers. He was called in 1993 and took silk in 2010. He practices in the areas of crime, inquiries and inquests and regulatory law. He was leading counsel for the prosecution in the Fellows/Boyle trial at which EncroChat evidence was first considered. In Chambers & Partners 2020, he was recommended in four practice areas and was described as follows:

> *"Highly capable with inherent gravitas. He is, without doubt, one of the leading advocates in the country … He's a superb tactician and technically excellent."*
>
> [Crime]
>
> *"He's a superb advocate - he's got a lightness of touch and can make complex issues seem very straightforward … Paul is first class. He has a succinctness of words and will use one sentence where the rest will need three … He's an example of a criminal jury advocate who's transferred seamlessly and impressively to the inquiry field."*
>
> [Inquests and Inquiries]
>
> *"Comes highly recommended and his technical ability isn't in any doubt."*
>
> [Professional Discipline].
>
> *"An extremely accomplished, hard-working and effective barrister. He has the complete set of skills."*
>
> [Financial Crime]