Protection from crime or covert erosion of rights?

On 2 July 2020 the National Crime Agency confirmed that it had dismantled "entire organised crime groups" through Operation Venetic, part of an EU-wide investigation, which resulted in 746 arrests and the seizure of £54m in cash, 77 firearms and over two tonnes of narcotics. The operation concerned the infiltration of EncroChat, a communications network and service provider, utilised by criminals worldwide.

On first blush, it's a win for both law enforcement agencies and the public. Criminals will go to prison and the streets will be safer; but is there a more sinister side to this? What if a UK network was hacked by our Government, where every iota of information contained on each of our phones was scanned in order to discover criminality. Farfetched? Perhaps, however, the EncroChat case shows that our governments now have the capability to do just that.

What was EncroChat?

EncroChat was more than a messaging service. The company sold modified Android mobile handsets, known as carbon units, with the cameras, microphones and GPS receivers removed or disabled. The carbon units came with pre-installed apps including the encrypted messaging service, EncroChat. The units had various features, including versions of a 'kill switch', whereby the contents of a unit could be erased upon the entry of a 15-digit passcode. Units also came with a feature where a user could remotely erase messages held on another device.

Easy to see why EncroChat was favoured by criminal enterprises. It enabled immense volumes of illicit trade to be conducted apparently without detection. That said, there were others within EncroChat's target market - bone fide customers with no connection to criminality. EncroChat was founded in the wake of the phone hacking scandal and in an era of an ever increasing number of security breaches involving malware and ransomware, from both criminals and government run agencies alike. In 2009, for instance, there were reports that GCHQ had compromised devices to spy on world leaders at the G20 summit. In 2015 a security tribunal heard that GCHQ had carried out persistent, illegal hacking of phones, computers and networks worldwide under broad thematic warrants that ignore privacy safeguards.

The EncroChat devices therefore offered privacy to politicians, celebrities and royals, and security to high net worth individuals and C-suite executives. It offered a solution to those who felt that governments had unfairly and unilaterally eroded their right to privacy through the controversial legislation, such as the Snoopers' Charter.

Many argue that the number of legitimate users of EncroChat paled into insignificance. Indeed, the NCA claim there wasn't a single legitimate user: "*the sole use was for coordinating and planning the distribution of illicit commodities, money laundering and plotting to kill rival criminals*". The French came up with a different rhetoric, stating that over 6000 users were legitimate.

Either way, it's worth remembering that a high proportion of law abiding members of the public favour encrypted messaging not dissimilar to the EncroChat messaging system. To take one example, WhatsApp also enables deletion of messages after they are sent and read – yet there is no accusations that the reason for this relates to evading crime.

Encrypted messaging is appealing because it enables our private messages to be secure from hacks and it ensures that law enforcement agencies respect our right to privacy (whether the agencies like it or not). Legitimate corporations strive to maximise security. In 2016, for instance, the 'PGP' devices made by BlackBerry (a company favoured by global corporations) were marketed as offering "military grade security". Security and privacy are therefore not intrinsically murky features; rather, they enable our rights and freedoms to be protected.

What did the hack involve?

It's not clear. The reports from agency to agency are somewhat confusing, with some reports composed by the same agencies differing quite dramatically. We do not know exactly when the investigation started, who initiated the investigation, or what the hack involved. The NCA states that the infiltration was by the French and Dutch authorities sometime in March 2020: "*two months ago this collaboration resulted in partners in France and the Netherlands infiltrating the platform*." It is said that the harvested data was then supplied to Europol, who then passed to the NCA.

Having said this, it appears that French authorities were working on the hack back in 2017. Furthermore, in 2016 there were reports from a whistle-blower that EncroChat was working with the NSA and FBI, due to warrants being issued demanding access to their Canadian & Amsterdam based servers. If this is correct, law enforcement might have had a way from close to the time of the company's inception.

The details of the hack are not clear. There is a big difference between decrypting encoded messages and successfully installing malware to view communications, where no decryption is required. In one statement the Gendarmerie said, "*Gendarmes from the centre for combating organised crime have achieved a technological feat: decrypting a substantial quantity of communications encoded by EncroChat.*". In another by the same agency, it is said that they were able to access *unencrypted* communication by hacking EncroChat servers based in France.

Regardless of what occurred, it's not the first time that law enforcement agencies have claimed to be able to decrypt messages. In 2016 the Netherlands Forensic Institute and the Royal Canadian Mounted Police claimed that they could decrypt coded messages on the BlackBerry PGP devices (although neither law enforcement agency would explain how decryption was achieved).

Questions remain, but the battle between tech companies and law enforcement agencies, concerning disclosing over private data without the subject's consent, rages on. Agencies

frequently request that tech companies hand over encrypted messages which directly or indirectly relate to actual or suspected criminal activities. Providers such as Apple, Facebook and Google argue that they would have to change the way the messages are encrypted in order to allow entry via a 'back door', which they are not willing to do.

That said, if the EncroChat hack was via malware (which seems likely), this issue does not concern a back door, nor does it concern encryption per se. With this case, agencies were able to circumvent requesting permission from tech providers by infiltrating the devices rather than intercepting messages already sent. With EncroChat, the SIM or network was likely hacked, a trojan then installed, which enabled the agency to have eyes and ears, not just in relation to the specific messaging platform, but in relation to the entire device. The hacker would then have a window into all the activity on the device.

Is hacking by law enforcement agencies legal?

Yes, subject to some exceptions. Had the case involved the UK authorities obtaining the data directly, the Investigatory Powers Act 2016 (nicknamed the Snoopers' Charter) would have applied. The Act allows investigators to obtain private information in a variety of ways, including hacking, and in some cases without the need for a warrant. There are protections, however. Regard must be had to points such as: whether the outcome could be achieved by other less intrusive means; whether the subject should be afforded increased protections due to the particular sensitivity of the information (for example communications between a lawyer and their client); and the public interest in the integrity and security of telecommunication systems. On the flip side, there are wide-ranging blanket justifications to obtaining the private data, including where the investigation is in interests of national security or of the economic wellbeing of the UK, and where it is in the public interest to prevent or detect serious crime.

Even if the act of obtaining private data by overseas authorities would have been illegal had it had occurred in the UK, it is unclear whether there are any restrictions on UK law enforcement utilising the data.

It is yet to be seen whether there will be any challenge brought by defence teams of those arrested, either on the basis that the information was illegally obtained or on the basis that the evidence lacks integrity.

Why does any of this matter?

It matters because there may have been legitimate users of EncroChat, whose privacy was infringed. It also matters because criminals use various other messaging systems which law abiding citizens use, such as iMessage and WhatsApp.

If law enforcement agencies are able to hack EncroChat, what safeguards are there in place to prevent them utilising their new found hacking skills to hack, for instance, the Vodafone network and gain access to all Vodafone phones, with the overarching goal of preventing or

detecting serious crime? One might argue that such a large-scale hack wouldn't happen because the goal of tracking and arresting the few criminals using the systems would not justify grossly invading the privacy of the innocent users. The rebuttal is that it may have already happened. In 2015 there was an unprecedented breach of Belgium's telecommunications infrastructure, which was blamed on UK authorities and which is still unresolved.

Moreover, who makes the decisions on who is hacked and for what reason? Where is the line drawn? Does that public have a say? In many cases warrants are required, but what is preventing agencies asking from assistance from ally jurisdictions in order to circumvent the warrant requirement? There's a worry that if security breaches go unchallenged, law enforcement will have the ability to read everyone's emails, their messages, monitor their mobile banking transactions, view photos, view internet history, record and listen to conversations, monitor locations and movement, at home and abroad, record passwords and passcodes etc.

There is an argument that even if this is done, as it is done by a government agency, nothing untoward will happen to personal private information. There is also the, 'I've got nothing to hide' argument. Both valid points but what happens in the event of a rogue employees? Is there anything preventing agencies from sub-contracting with private institutions to perform the hacking or monitor and scan the hacked information? If not, then the net of the potential number of people able to access private information has been cast far wider. What are the limits to this net? Who determines the limits on access? What happens if someone oversteps the mark? Will we be informed? What about information belonging to or concerning minors? What happens if a criminal organisation hacks the information obtained by the agencies? The list goes on.

The real issue is that law enforcement agencies are now exercising significant powers, secretive by their very nature, with potential for no accountability to those whose rights may be infringed.