How an app to decrypt criminal messages was born ‘over a few beers’ with the FBI

David Tuffley, *Griffith University*

Australian and US law enforcement officials on Tuesday announced they’d sprung a trap three years in the making, catching major international crime figures using an encrypted app.

More than 200 underworld figures in Australia have been charged in what Australian Federal Police (AFP) say is their biggest-ever organised crime bust.

The operation, led by the US Federal Bureau of Investigations (FBI), spanned Australia and 17 other countries. In Australia alone, more than 4,000 police officers were involved.

At the heart of the sting, dubbed Operation Ironside, was a type of “trojan horse” malware called AN0M, which was secretly incorporated into a messaging app. After criminals used the encrypted app, police decrypted their messages, which included plots to kill, mass drug trafficking and gun distribution.

Millions of messages unscrambled

AFP Commissioner Reece Kershaw said the idea for AN0M emerged from informal discussions “over a few beers” between the AFP and FBI in 2018.

Platform developers had worked on the AN0M app, along with modified mobile devices, before law enforcement acquired it legally and adapted it for their use. The AFP say the developers weren’t aware of the intended use.

Once appropriated by law enforcement, AN0M was reportedly programmed with a secret “back door”, enabling them to access and decrypt messages in real time.

A “back door” is a software agent that circumvents normal access authentication. It allows remote access to private information in an application, without the “owner” of the information being aware.

So the users — in this case the crime figures — believed communication conducted via the app and smartphones was secure. Meanwhile, law enforcement could reportedly unscramble up to 25 million encrypted messages simultaneously.

But without this back door, strongly encrypted messages would be almost impossible to decrypt. That’s because decryption generally requires a computer to run through trillions of possibilities before hitting on the right code to unscramble a message. Only the most powerful computers can do this within a reasonable time frame.

Providers resist pressure for ‘back-door’ access

In the mainstream world of encrypted communication, the installation of “back-door” access by law enforcement has been strenuously resisted by app providers, including Facebook who owns WhatsApp.

In January 2020, Apple refused law enforcement’s request to unlock the Pensacola shooting suspect’s iPhone, following a deadly 2019 Florida attack which killed three people.

Apple, like Facebook, has long refused to allow back-door access, claiming it would undermine customer confidence. Such incidents highlight the struggle of balancing competing demands for user privacy with

the imperative of preventing crime for the greater good.

Getting criminals to use AN0M

Once AN0M was developed and ready for use, law enforcement had to get it into the hands of criminal "underworld" figures.

To do so, undercover agents reportedly persuaded fugitive Australian drug trafficker Hakan Ayik to unwittingly champion the app to his associates. These associates were then be sold mobile devices pre-loaded with AN0M on the black market.

Purchase was only possible if referred through an existing user of the app, or by a distributor who could vouch for the potential customer as not working for law enforcement.

The AN0M-loaded mobiles — likely Android-powered smartphones — came with reduced functionality. They could do just three things: send and receive messages, make distorted voice calls and record videos — all of which was presumed to be encrypted by the users.

With time the AN0M phone increasingly became the device of choice for a significant number of criminal networks.

Building up a network picture

Since 2018, law enforcement agencies across 18 countries, including Australia, had been patiently listening to millions of conversations through their back-door control of the AN0M app.

Information was retrieved on all manner of illegal activities. This gradually enabled police to etch a detailed picture of various crime networks. Some of the footage and images retrieved have been cleared for public release.

One major challenge was for police to match overheard conversations with identities — as the AN0M phone could be purchased anonymously and paid for with Bitcoin (which allows secure transactions that can't be traced). This may help explain why it took three years before police openly identified alleged perpetrators.

It's likely the evidence obtained will be used in prosecutions now that a multitude of arrests have been made.

The future of encryption

Encryption technology is improving fast. It needs to — because computing power is also growing rapidly.

This means hackers are becoming increasingly capable of breaking encryption. Moreover, when quantum computers become available this problem will be further exacerbated, since they are massively more powerful than conventional computers today.

These developments will likely weaken the security of encrypted messaging apps used by law abiding people, including popular apps such as WhatsApp, LINE and Signal.

Strong encryption is an essential weapon in the cybersecurity arsenal and there are thousands of legitimate situations where it's needed. It's ironic then, that the technology intended by some to keep the public safe can also be leveraged by those with criminal intent.

Networks of organised crime have used these "legitmate" tools to conduct their business, secure in the

knowledge that law enforcement can’t access their communications. Until AN0M, that is.

And while Operation Ironside may have sent a shiver through criminal subcultures operating around the world, these syndicates will likely develop their own countermeasures in this ongoing game of cat and mouse.

David Tuffley, Senior Lecturer in Applied Ethics & CyberSecurity, *Griffith University*