The government wants additional powers to access encrypted messages. Luis/Flickr , CC BY-NC

The Australian government wants the ability to read messages kept secret by encryption in the name of aiding criminal investigations. But just how it proposes to do this is unclear.

As Australian Attorney-General George Brandis recently told Fairfax :

At one point or more of that process, access to the encrypted communication is essential for intelligence and law enforcement.

In an interview with Sky News, he spoke favourably of controversial UK legal powers that seek to impose on device makers and social media companies “a greater obligation to work with authorities where a notice is given to them to assist in ‘breaking’ a communication”.

Brandis has insisted the government doesn’t want a “backdoor” in secure messaging apps. How, then, he expects companies to “break” them is unclear.

As many have pointed out , it’s hard to see any tool that gives law enforcement privileged access to otherwise encrypted messages as anything else but a “backdoor”.

How end-to-end encryption works

Backdoor or not, it’s worth being sceptical of any mechanism aimed at accessing encrypted messages on platforms like WhatsApp. To explain why, you need to understand how end-to-end encrypted messaging services work.

Encrypted messaging servers scramble the original message, the “plaintext”, into something that looks like random gibberish, the “cyphertext”.

Translating it back to plaintext on the receiver’s phone depends on a “key” – a short string of text or numbers. Without access to the key, it isn’t feasible to get the plaintext back.

How end-to-end encryption works. Elya/joshbressers/The Noun Project composite, CC BY

Keys are generated in pairs, a public key and a private key, of which only the private key must be kept secure. The sender of the secure message has the receiver’s public key, which is used to encrypt the plaintext. The public key cannot be used to unscramble the cyphertext, nor does possessing the public key help in obtaining the private key.

End-to-end encryption simply keeps the private key securely stored on the phones themselves, and converts the cyphertext to plaintext directly on the phone. Neither the private keys nor the plaintext are ever available to the operator of the messaging service.

Compromising security

An encrypted messaging app could hypothetically be modified in a number of ways to make it easier for authorities to access.

One would be to restrict the range of keys that the app can generate. That would make it possible for the government to check all possibilities.

The US government, which imposed regulations to this effect for a brief period in the 1990s, may have once had computing resources far in excess of any other entity, but this is no longer the case. In fact, these old rules are themselves still causing security problems, as some applications can be tricked into reverting to the insecure “export mode” encryption that is trivially crackable today.

Other national governments and well-funded private bodies would find “brute force” checking of

all the possible keys well within their capabilities, compromising the security of legitimate users.

And while governments might believe they can keep their “backdoor” secure, such secrets have a nasty habit of leaking out, as did hacking techniques used by the CIA and NSA .

Nor can governments simply make possessing encryption software a criminal offence.

Take the application Pretty Good Privacy (PGP) – or, more precisely, its open-source equivalent GNU Privacy Guard (GPG).

Once used for securing email messages, it’s now more often used to ensure software updates on Linux systems are from the original authors and have not been tampered with. For instance, the system update tool in Ubuntu Linux uses the GPG machinery for this. Without it, the Linux servers that run much of the internet would become much more vulnerable to hackers.

Similar mechanisms are used in Windows, iOS and Android to prevent tampered applications from being installed. As such, banning or undermining end-to-end encryption would seriously affect internet security.

Endless workarounds

In any case, creating backdoors in end-to-end encrypted messaging services would not achieve its goals. Once messaging app backdoors became known, savvy users would simply switch to another service, or make their own.

Most popular secure messaging apps, such as WhatsApp and Facebook’s secure messaging mode, use a system originally developed by Open Whisper Systems for the Signal secure messaging app. Anyone can download the source code and set up their own version.

But let us assume for a moment that the Australian government somehow forces users to use messaging apps that give the government access. While this would impose a minor inconvenience on those wishing to communicate securely, it would do little more.

It would be possible to develop a separate encryption app that encrypts the message. Using digital steganography, the encrypted message could be hidden within a photo or video file; this could then be sent as an attachment. The government's access to the messaging app would then be moot.

While they may – with some effort – be able to discover the existence of the hidden messages in media file attachments, they would still be unable to decrypt the message.

To date, the ideas floated by the Australian and British governments on end-to-end encryption could most charitably be described as vague.

They would be wise to consult experts to come up with proposals grounded in technical reality if they wish to be taken seriously by the technology industry.

Robert Merkel is a member of the Australian Greens.

Authors: Robert Merkel, Lecturer in Software Engineering, Monash University

Read more http://theconversation.com/when-is-not-a-backdoor-just-a-backdoor-australias-struggle-with-encryption-79421