The ability of authorities to access encrypted messages must be balanced with the security risks. Ink Drop/Shutterstock

The Australian government plans to introduce new legislation forcing companies such as Google and Facebook to de-crypt messages in the name of fighting terrorism and other crimes. But the move will have serious implications for cybersecurity.

In a press conference on Friday, Prime Minister Malcolm Turnbull said the law would impose an obligation on technology companies to be able to provide Australian security agencies with access to encrypted user communications.

Both he and Attorney-General George Brandis have insisted they are not asking for " back doors " to be built into encryption software. Yet they have not detailed how their goal can be achieved otherwise.

Take an end-to-end encrypted messaging service like Signal. A server scrambles the original message, and the text can be de-scrambled only by a "key" that exists on the recipient's phone. The company never sees the plaintext.

The government's message is that it's only trying to keep the country safe, but this masks a great deal of complexity.

Cybersecurity is always a trade-off. Weakening security in one area to protect against terrorist attacks on the ground could increase the risk of cyberattacks by terrorists and hostile nations, and increase the likelihood of cybercrime.

Can Australia follow the UK's lead?

The attorney-general indicated that Australia would follow the UK's lead in the proposed law, and especially its Investigatory Powers Act , which became law in 2016.

Although the UK has been held up as an example to follow, it hasn't managed to actually get its version of the law working yet, nor has it decided how decryption would be achieved.

Also known as the " Snooper’s Charter ", the law gives UK intelligence agencies and law enforcement the ability to carry out both targeted and bulk surveillance of communications data.

Most importantly, the UK act requires that telecommunication operators "provide and maintain the capability to disclose, where practicable, the content of communications or secondary data in an intelligible form and to remove electronic protection".

Despite the UK having passed the law, there has been little public discussion about how technology companies would actually do this, nor what would happen if they failed to comply.

Could tech companies comply even if they wanted to?

In 2015, a group of cybersecurity experts debated how technology companies could comply with laws such as those proposed in both the UK and Australia.

The academics and industry researchers outlined the significant risks of a number of approaches that would allow specific agencies access to unencrypted information.

One approach, for example, involves using special keys provided by a government agency to encrypt a copy of all messages. This would allow users to continue to use end-to-end encryption of messages, but government agencies could always access their own versions of the messages when necessary.

The obvious risk with this is that if the “master key” was lost or stolen, everyone’s communications would be compromised.

Creating individual keys and putting them in a “key escrow”, effectively a large database, would also be insecure and technically impractical.

Another approach would be to weaken the encryption to such an extent that it would be feasible for someone with a large enough computer to break if necessary. Again, this would give foreign governments and well resourced criminals the same capability, rendering the communication unsecured.

Decreasing security increases risk in other areas

The Australian government, like other nations, has a Cyber Security Strategy that lays out how it aims to protect the country, its critical infrastructure and its population.

Strong encryption and the ability to communicate securely is a fundamental part of this strategy. Undermining this capability by making all communications open to a large number of people and organisations within the government significantly increases the risks of compromise by hostile actors like foreign nation states and organised criminals.

These risks are not being discussed as part of the fight against terrorism but are real nonetheless. The leaking of secrets from US agencies like the NSA and CIA demonstrates that even the most powerful organisations are not able to guarantee the security of sensitive information.

The only thing stopping hostile actors from getting access to encrypted information and communications on a large scale currently is the fact that the keys are not held centrally.

Terrorists will just shift the way they do things

While it is clear that being able to read encrypted messages would be an advantage for law enforcement and security in the short term, terrorists and criminals would quickly shift to other

non-regulated forms of encryption.

The open source Tor network, for example, is currently not controlled by a company or government and criminals and terrorists already use the dark web to communicate and trade illegal goods and services.

Nothing was said about the dark web on Friday, although this is arguably a bigger problem from a security perspective than the use of social media messaging apps.

But even if Tor was blocked in some way, there is a raft of encryption software that can be easily deployed by those who want to protect their communications from the government.

David Glance does not work for, consult, own shares in or receive funding from any company or organization that would benefit from this article, and has disclosed no relevant affiliations beyond the academic appointment above.

Authors: David Glance, Director of UWA Centre for Software Practice, University of Western Australia

Read more http://theconversation.com/australias-planned-decryption-law-would-weaken-cybersecurity-81028