Critics say there are no legitimate uses of encryption—they're wrong

May 19 2021, by Gernot Heiser, Lyria Bennett Moses and Vanessa Teague

Credit: CC0 Public Domain

Australia's parliament is considering legislation to give new powers to the Australian Criminal Intelligence Commission (ACIC) and the Australian Federal Police. These powers will allow them to modify online data, monitor network activity, and take over online accounts in

some circumstances.

Last week, in a submission to parliament regarding the proposed powers, ACIC made an inaccurate and concerning claim about privacy and information security. ACIC claimed "there is no legitimate reason for a law-abiding member of the community to own or use an encrypted communication platform."

Encrypted communication platforms, including WhatsApp, Signal, Facetime and iMessage, are in common use, allowing users to send messages that can only be read by the intended recipients. There are many legitimate reasons law-abiding people may use them. And surveillance systems, no matter how well-intentioned, may have negative effects and be used for different purposes or by different people than those they were designed for.

How surveillance can go wrong

Surveillance systems often produce unintended effects.

In 1849, the authorities at Tasmania's Port Arthur penal colony built the Separate Prison, intended as a humane and enlightened method of imprisonment. Based on the ideas of Jeremy Bentham's Panopticon, the design emphasized constant surveillance and psychological control rather than corporal punishment. However, many inmates suffered serious psychological problems resulting from the lack of normal communication with others.

From 2006 onwards, Facebook developed a privacy-invading apparatus intended to facilitate making money through targeted advertising. Facebook's system has since been abused by Cambridge Analytica and others for political manipulation, with disastrous consequences for some democracies.

In 2018, Australia's parliament passed the Telecommunications and Other Legislation Amendment (Assistance and Access) Act, with the ostensible purpose of helping police to catch terrorists, pedophiles and other serious criminals. The act gave the Australian Federal Police powers to "add, copy, delete or alter" material on computers. These powers were used the following year to raid the Australian Broadcasting Corporation in connection with a story on alleged war crimes in Afghanistan.

These examples demonstrate two facts about security and surveillance. First, surveillance may be used by people of any moral character. Second, a surveillance mechanism may be used by different people, or may achieve a completely different effect, from its original design.

We therefore need to consider what avoiding, undermining or even outlawing the use of encrypted platforms would mean for law-abiding members of the community.

Encryption limits the power of security agencies

There are already laws that decide who is allowed to listen to communications taking place over a telecommunications network. While such communications are generally protected, law enforcement and national security agencies can be authorized to intercept them.

However, where communications are encrypted, agencies will not automatically be able to retrieve the content of the conversations they intercept. The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 was passed to enable agencies to get assistance to try to maintain their ability to get access to the (unencrypted) content of communications. For example, they can ask that one or more forms of electronic protection be removed.

There are also federal, state and territory laws that can require people to assist law enforcement and national security agencies in accessing (unencrypted) data. There are also numerous proposals to clarify these laws, extend state powers and even to prevent the use of encryption in certain circumstances.

More surveillance power is not always better

While people may hold different views on particular proposals about state powers and encryption, there are some things on which we should all be able to agree.

First, facts matter. If the ACIC is wrong about lawful uses of encryption, its assertion should be withdrawn or discounted.

Second, people need both security and privacy. In fact, privacy can facilitate security (the more people know about you, the easier it is to trick you, track you and/or harm you).

Third, law enforcement and national security agencies need some surveillance powers to do their jobs. Most of the time, this contributes to the social good of public safety.

Fourth, more is not necessarily better when it comes to surveillance powers. We must ask what purpose the powers serve, whether they are reasonably necessary for achieving that purpose, whether they are likely to achieve the purpose, what negative consequences might result, and whether the powers are proportionate.

Lawful use of encrypted communication is common

We can only develop good policy in this area if we have the facts on

lawful uses of encryption.

There are many good reasons for law-abiding citizens to use end-to-end encrypted communication platforms. Parents may send photos or videos of their children to trusted friends or relatives, but prefer not to share them with third parties. The explosion of telehealth during the COVID-19 pandemic has led many patients to clarify that they do not want their consultation with their doctor to be shared with an intermediary such as Facebook or Google (or Huawei or WeChat).

Even the New South Wales iVote online voting system—hardly a standout example of excessive security given that it contained a defect that potentially allowed vote manipulation to take place—advertises the use of end-to-end encryption to protect the privacy of votes in transit. The necessity of privacy to protect a citizen's right to vote without coercion is one of the oldest examples of legal privacy requirements.

Undermining encryption will hurt legitimate users

As law-abiding citizens do have legitimate reasons to rely on end-to-end encryption, we should develop laws and policies around government surveillance accordingly. Any legislation that undermines information security across the board will have an impact on lawful users as well as criminals.

There will likely be significant disagreement in the community about where to go from there. But we have to get the facts right first.

We should not consider legislation to deliberately undermine the communications security of all individuals without acknowledging the potential harm this could cause to law-abiding citizens.

Commons license. Read the original article.

Provided by The Conversation