Governments undermining encryption will do more harm than good

January 13 2016, by Suelette Dreyfus, University Of Melbourne

Credit: Andrea Piacquadio from Pexels

Western governments, notably the UK and the US, are pushing the software industry to open "backdoors" into our encrypted

communications.

The argument touted by government agencies for nearly 20 years is that terrorists use strong encryption to hide their communications, therefore we should ban strong encryption.

British Prime Minister David Cameron has been outspoken in his desire for a such a ban.

And last week, US President Barak Obama's Chief of Staff and a team of national security officials flew to Silicon Valley to meet with top technology companies Twitter, Microsoft, YouTube, Facebook, LinkedIn, Apple and Dropbox. It's likely they discussed collaboration between the Silicon Valley and the US intelligence and law enforcement on backdooring encryption.

Next week, Prime Minister Malcolm Turnbull will be meet the US president in Washington DC and encryption may also be on their security agenda.

Australia is already a member of the "5-Eyes" alliance, and a user of the PRISM regime to spy on citizens, which was revealed by Edward Snowdon. It is also a signatory to the Trans Pacific Partnership. It seems likely Australia will try to follow the US and UK lead.

In response to this push to undermine encryption, an open letter to governments, called "Secure The Internet", was published this week. It is signed by more than 170 companies, organisations and individuals from around the world, including leading data security researchers.

The letter calls for all governments to reject backdooring or the weakening of encryption products.

Keys to the door

Encryption is used by most of us every day, typically with no conscious effort. If you log into your email or bank site with an address starting "https://", then you are using encryption.

It seems likely governments around the world are trying to either woo or cajole the tech industry and security researchers to "break" the software they build by installing backdoors or other holes for the government to access our communications effortlessly.

The problem with installing backdoors is that bad actors – organised crime, fraudsters, hostile foreign governments and the like – may also focus their attention on these security holes. Any universal "passkey" built into such a system would be immensely valuable, and worth spending enormous resources to capture, thus making those who had them significant targets for espionage.

The push to emasculate the strong encryption we use every day is akin to the government telling every citizen we can't lock our front door, or maybe we can only use a weak little latch. It's like requiring everyone to send our passwords to a central government office.

The aim should be to improve security on the internet, not to break it. Governments colluding to break internet security introduces the risk of breaking our evolving digital economy as well by undermining trust in businesses and banks. Imagine logging into your online banking at National Australia Bank, ANZ, Westpac, Commonwealth Bank or your insurance company, and not knowing if the encryption was secure.

The argument that terrorists might use encryption so we should ban it is without nuance and probably even effect. Terrorists might also use steak knives to commit crimes, but we don't make steak knives illegal. Steak

knives have other useful purposes in society. And, like strong encryption, these benefits greatly outweigh the very small risks.

Will it even work?

The Secure the Internet letter references the research paper authored by a who's who of the world's top computer security researchers.

The paper highlights the numerous problems with implementing such policies in practice. Many of these researchers were around when the first major push came from government to impose weakened encryption on the masses in the form of Clipper Chip in 1997.

They concluded "the damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago." Such schemes kill innovation. Indeed the authors query whether Facebook and Twitter would even exist today if the previous scheme had been imposed.

Australian security agencies have significantly expanded their powers over the past few years. The agencies can break into computers remotely, plant software, copy data, access related metadata, install keyloggers to track a target's every keystroke.

These agencies' methods require some targeting, although some do not even require the oversight of judge. They already can force anyone to reveal a harddrive's encryption passphrase or face a prison term for failing to do so.

Agencies have also had a huge budget increase, with an extra A$1.2 billion added for national security in the 2015 budget. In short, they have a cornucopia of powers and resources to chase terrorists.

At some point, that chase has to be about the mundane gumshoe work of gathering "HUMINT" – intelligence from human contacts – not just about sitting at a desk of computers scanning communications.

Realistically, backdooring strong encryption software, which is what is being floated here, will not stop terrorists. They will simply find and use other channels, including secure software distributed via other countries that do not have such restrictive laws.

Making us more or less secure?

The desire to break the computer security of an entire population also hints at the more insidious aim of governments trawling all of our private communications. With Edward Snowden's revelations about exactly this, it is important to view this recent push to destroy the innocent citizen's right to use encryption securely through this lens.

The contradiction of this push is that governments are trying to force our communications to be less secure while claiming to make us more secure.

If we want to retain our freedoms, we will also need to take some responsibility by changing our own mindsets. We as citizens need to accept that there is some risk in an uncertain world. We cannot expect law enforcement nor intelligence agencies to provide 100% guarantees; it is both unrealistic and unreasonable.

The urge to "do something" after terrible attacks like those in Paris, should be spent fixing the underlying causes of terrorism, not creating legislative overreach designed to grab tomorrow's headline.

Keeping the keys to our own house requires a balanced approach in all things.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation