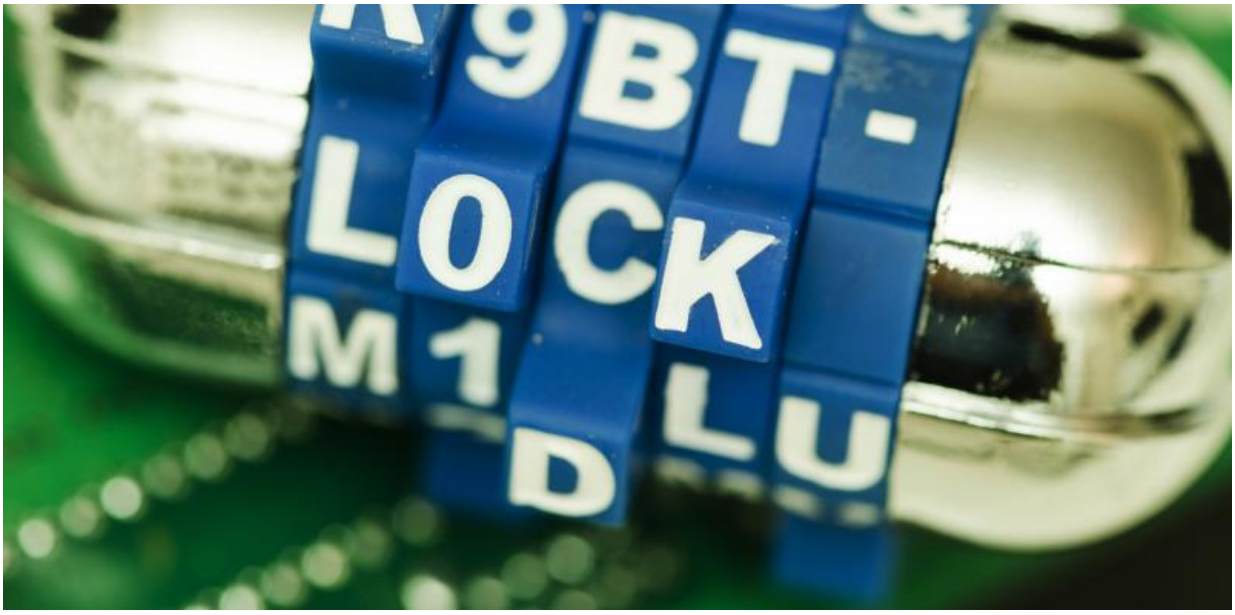
# The genie is out of the bottle – it's foolish to think encryption can now be banned

January 5 2016, by Adam Fish




Credit: Perspecsys Photos, CC BY-SA

Politicians have turned their sights on encryption once more following terrorist outrages in Paris and San Bernardino, California.

A country that once welcomed encryption, France is now considering outlawing it in the wake of the massacre in its capital. In the US, politicians and law enforcement have made similar demands, as has the British prime minister, David Cameron.

Encryption creates trust. It is the underpinning of the internet, ensuring the privacy of mail, commerce, and transactions of all kinds. End-to-end encryption, where data such as texts, emails, or other messages are encrypted in transit and in storage, and where no third party other than those communicating have the keys to decrypt it, has come under particular criticism.

Certainly it is difficult if not impossible to crack, and poses a serious problem for investigators. But the Paris attacks were not aided by encryption – the attacker's unencrypted mobile phone, which was found in a bin, led police to their safe house. Abdelhamid Abaaoud, the Belgian-Moroccan ringleader, communicated without encryption.

When in San Bernardino police claimed to have found that the terrorists used "levels of built-in encryption", Christopher Soghoian, principal technologist at the American Civil Liberties Union, dismissed this as nothing more than the standard encryption built into the 2G/3G/4G communications protocols that carry data between the phone handset and network transmitter masts. In other words, an unremarkable part of how mobile phones work.

Wanting to keep out prying eyes is only natural. Credit: yusamoilov, CC BY

It is clear that the Islamic State is aware of and uses encrypted communications, however. The US Army claims IS uses up to 120 different online platforms for communication, including messaging services such as WhatsApp or the encrypted Telegram service to organise, socialise, recruit, and for use as a press outlet. Telegram was used by IS to claim responsibility for the Paris attacks and the bombing of a Russian airliner over Egypt.

## No safety in backdoors

So with this in mind, Western leaders want powers to decrypt

communications. Particular ire has been directed at tech companies such as Apple, Google and Facebook which, by providing encryption in their popular products, have made investigators' work harder. FBI director Jim Comey urged them to prevent terrorist communications from "going dark". Even just using encryption makes you a suspect in the eyes of the law.

Governments want "backdoors" written into encryption schemes to provide privileged access to law enforcement and secret services. But tech companies are generally moving in the opposite direction, with Apple CEO Tim Cook calling backdoors "incredibly dangerous". Other smaller companies like Signal, Silent Circle, Wickr, Protonmail and Mega also offer encrypted communication platforms.

## The principles of privacy

On the other hand, Germany promotes the use of encryption by its citizens. However, the EU has no overarching policy on encryption. While the forthcoming General Data Protection Regulation specifies that data must be encrypted when in storage, it doesn't address end-to-end encryption and data in transit.

The UN, in both principle and practice, rejects efforts to criminalise or restrict encryption. Article 12 of the UN Universal Declaration of Human Rights argues that "no citizen should be subjected to arbitrary interference of their privacy, family, home or correspondence." UN special rapporteur on freedom of expression David Kaye has argued:

*States should avoid all measures that weaken the security individuals may enjoy online, such as through backdoors, weak encryption standards and key escrows [where encryption keys are held by third parties to be handed over to police on demand].*

If civil society groups had their way encryption would be protected. Rainey Reitman of the Electronic Frontier Foundation has argued that weakening encryption makes us all less secure, and that any backdoor can and will be exploited by malicious hackers or foreign powers.

## The powers they need already exist

Are laws banning strong encryption even necessary when the NSA, GCHQ or police can just hack our communications? Developers of Tor, software used for anonymous online communication, claim the FBI paid Carnegie Mellon University researchers to hack Tor, something both parties have denied. Controversial Italian security firm Hacking Team were found to have monitored Tor for the FBI, and Edward Snowden's leaked files revealed NSA efforts to monitor millions of computers by infecting them with malware.

Considering how widely used and important encryption is, and how little it is employed by terrorists, it's arguable that government hacking is preferable to enforcing backdoors that make us all less safe.

In truth, encryption is so pervasive and so easy to build into new software that it's practically impossible to ban. Phil Zimmermann, who invented free encryption software PGP, said any proposal to ban encryption was "absurd":

*End-to-end encryption is everywhere now. If you have strong encryption between your web browser and your bank, you can't have a man in the middle from the government wiretapping that.*

Melvin Kranzberg, a professor in the history of technology at Georgia Tech, famously said: "Technology is neither good nor bad; nor is it neutral." Proponents of banning encryption fail to recognise how encryption helps journalists, whistleblowers, and those who face

oppression under authoritarian regimes, while civil rights activists must recognise that encryption could be a powerful tool for those who would do society harm (government or otherwise). But while expectations of privacy fluctuate around the world and over the years, the value of privacy is constant.

We will make no progress by blaming the technology – whatever technology of the day that may be – instead of addressing the root causes of the antagonism that drives people to use it.

*This story is published courtesy of* The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation