Could encryption 'backdoors' safeguard privacy and fight terror online?

January 27 2016, by Keith Martin, Royal Holloway

Hack attack. Wikipedia, CC BY-SA

Since so much of life has moved online, a clash has emerged between the opposing values of internet freedom, and internet control. Should the internet be a public arena free of all interference and influence from the

authorities? Or does too much freedom result in anarchy, turning the internet into a safe haven for criminals and terrorists?

The tension between these two opposing extremes, the "crypto wars", is a battle that has been raging for 30 years – an approach that would reconcile these two attitudes would offer a way forward. Long-term privacy advocate and cryptographer David Chaum recently put forward one such idea that involves building a special "backdoor" that could only be accessed on agreement by multiple parties across different countries and cultures – an idea that combines the protections of encryption while meeting the need for transparency that law enforcement wants. But will it work?

Freedom vs control

The internet is built as an open system, with unique IP addresses that identify computers online and logs of connections from one to another. So for supporters of a free internet the big challenge is maintaining anonymity, so that the web can be used and sites visited without leaving behind a digital trace that could identify users.

Anonymising software such as Tor has been developed in response, and hides the link between a browser and the website it visits. But while Tor makes it harder to determine who has been visiting websites, it is not infallible. The fact remains that guaranteeing absolute anonymity on the internet is very difficult.

Opponents of a free internet face a different conundrum. Internet users have a genuine need for cyber-security controls that are strong enough to protect their data from cyber-criminals. This is provided by cryptography, mathematically-based encryption tools that prevent unauthorised eyes from seeing data, whether en route through the internet or at rest on a hard disk or phone. Cryptography protects our

banking systems, our mobile phone calls, and is the core of anonymity technologies such as Tor.

The problem with cryptography is that it works too well. In the light of terrorist attacks some voices from law enforcement and government security agencies have criticised cryptography's power to prevent them from accessing communications others would rather they didn't. They claim that encryption and Tor hide information that they need. Some officials have even suggested that cryptography should be outlawed.

Bringing the two together

The history of the crypto wars includes several attempts at compromise, all unfit for today. In the 1980s governments used export controls to restrict movement of cryptographic hardware. In the 1990s the US and UK infamously attempted to impose "key escrow", which handed the ability to reverse encryption to government agencies.

Supporters of cryptography subsequently believed that attempts to control cryptography had failed. But the documents revealed by Edward Snowden since 2013 have shown that governments have been developing a barrage of techniques to circumvent cryptography behind a cloak of secrecy. In response companies such as Apple promised stronger cryptography on user devices.

The heart of the problem is simply this. How can we offer secure and, if required, anonymous communication technologies to "good" people, while allowing this protection to be removed if "bad" people also use them? One idea that keeps resurfacing is to deploy some sort of "backdoor" which, under exceptional circumstances, creates a hole in the encryption's protection. This is Chaum's suggestion, only with a twist.

The problem with backdoors is not how to build them, but how to govern

them. Who do we trust with our keys? And if someone – the police, say – has the ability to use a backdoor then how can we prevent that knowledge from being discovered by someone undesirable – perhaps the very criminals the police are pursuing?

Chaum's proposal is his new anonymity software, PrivaTegrity, whose cryptographic protections are built with a deliberate backdoor. PrivaTegrity's backdoor can only be activated by co-operation between nine different server administrators located in nine different countries. By distributing the governance of the keys across countries, cultures and continents, the argument is that there would be less chance for misuse. Only if all of them agree can the anonymity protection be removed to allow investigators to access details of the communication.

It's a nice idea, but hard to imagine it working in practice. In particular it's unlikely national security agencies in the UK and US will be keen to rely on the judgement of others about what information can be accessed, and when.

However, we should welcome all ideas on balancing data privacy and control and the UK parliament is currently debating the draft Investigatory Powers bill, known as the snooper's charter. Ultimately, it is likely to propose some sort of new trade-off between privacy and legal access. Whatever the final terms of this bill are, it's inevitable that it won't keep everyone happy. Despite Chaum's interesting ideas, the fact remains that the two opposing views on internet freedom would seem to be fundamentally irreconcilable. In whichever state of compromise we proceed, the crypto wars will inevitably rage on.

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

Source: The Conversation