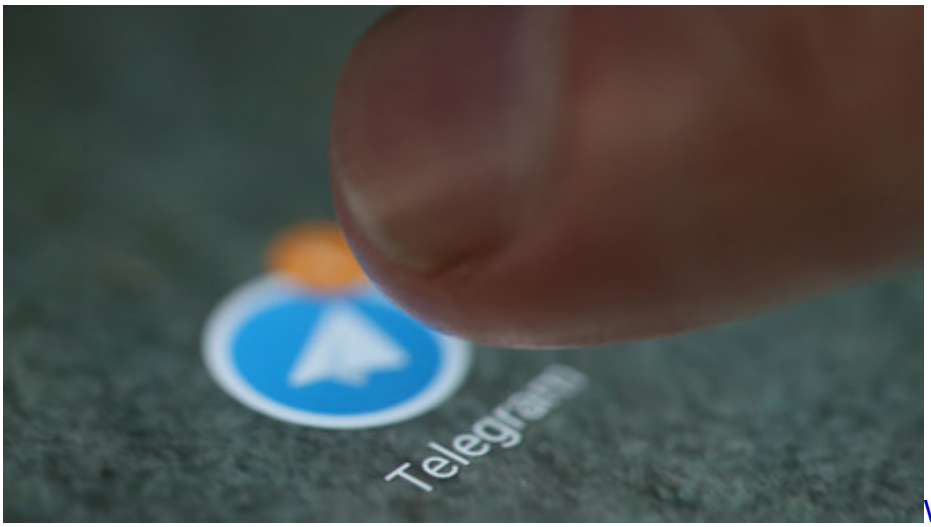
‘Five Eyes’ spying worldwide private correspondence

Description

A global network of intelligence agencies wants easier access to your private and encrypted messages. In a barely veiled warning to tech companies, it has promised to make things tough for those that don’t comply.

After a meeting on Australia’s Gold Coast last week, ministers for the intelligence agencies of the US, UK, Canada, Australia, and New Zealand – known as the ‘Five Eyes’ – have shared their vision for worldwide snooping in a joint statement.

In the official communique, the ministers outline the importance of reading private messages in the fight against terrorism and crime, citing “the urgent need for law enforcement to gain targeted access to



Watchdog to consider de-blocking Telegram in Russia if service provides encryption keys to FSB

The spy chiefs paid lip service to the importance of encryption for privacy purposes, but went on in another statement to call for increased powers to access private data. Cracking your files, they argue, is no more sinister than a patrol cop searching your vehicle or house.

“Privacy laws must prevent arbitrary or unlawful interference, but privacy is not absolute,” they said. Recognizing that some encrypted data can be nearly impossible to crack, the agency chiefs called on tech companies to turn over the keys voluntarily.

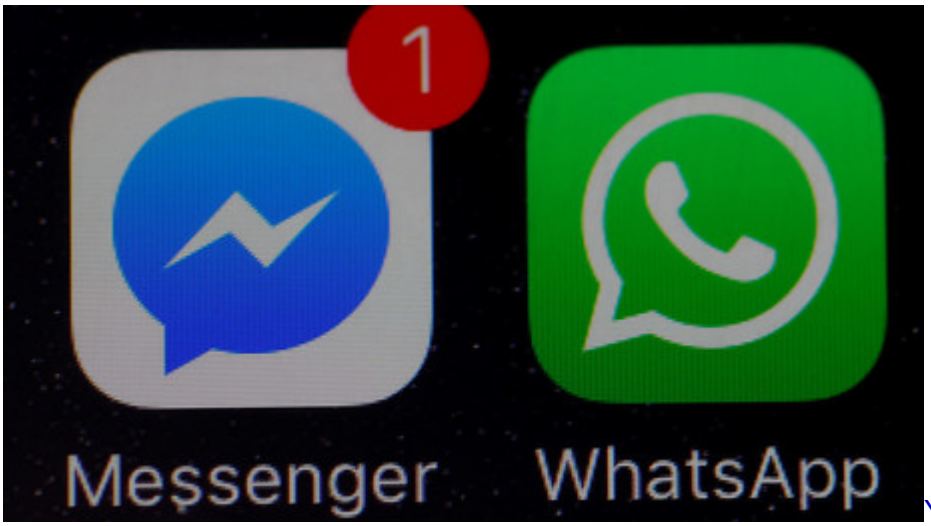
“The governments of the Five Eyes encourage information and communications technology service providers to voluntarily establish lawful access solutions to their products and services,”reads the statement.

And if the companies don’t cooperate voluntarily, the Five Eyes have ways of making them talk.

Stubborn companies may be hit with “technological, enforcement, legislative, or other measures,” the agencies warned, without elaborating on what those measures might be.

With encryption methods growing ever more sophisticated, securing the cooperation – voluntary or otherwise – of tech companies makes the job of law enforcement and spy agencies that much easier. To that end, the ministers present at last week’s meeting invited several “senior digital industry representatives” who did not accept the invitation.

Exactly what kind of access the spy chiefs want is also unclear. It could involve developers turning over access to an individual user’s messages when requested by law enforcement, or companies installing so-called ‘backdoors’ into their hardware which could be accessed at will by governments or law



You could soon spend 10 years in Australian jail if you don’t hand over your phone password to cops

Earlier this summer, US lawmakers proposed legislation that would block the latter approach. A bipartisan bill introduced in the House of Representatives said that “backdoors in otherwise secure products make Americans’ data less safe, and they compromise the desirability of American goods overseas.”

The bill was introduced two years after the FBI threatened to take Apple to court in order to attempt to force the tech giant to create software to unlock an iPhone belonging to one of the shooters responsible for a massacre in San Bernardino, California. One day before the court hearing was scheduled, the FBI backed off, as it had found an Israeli firm able and willing to crack the phone.

The tech industry was divided on the case. Apple fought tooth and nail against the FBI, and the company said that America’s founding fathers “would be appalled” by the invasion of privacy. Facebook CEO Mark Zuckerberg supported Apple, as did renegade cyber security developer John McAfee. Microsoft CEO Bill Gates threw his support behind the FBI, saying he supported unlocking the phone in this “specific case.”

With the Five Eyes set to put the squeeze on tech companies again, those in the industry will once again have to choose where they stand on the liberty versus security spectrum.