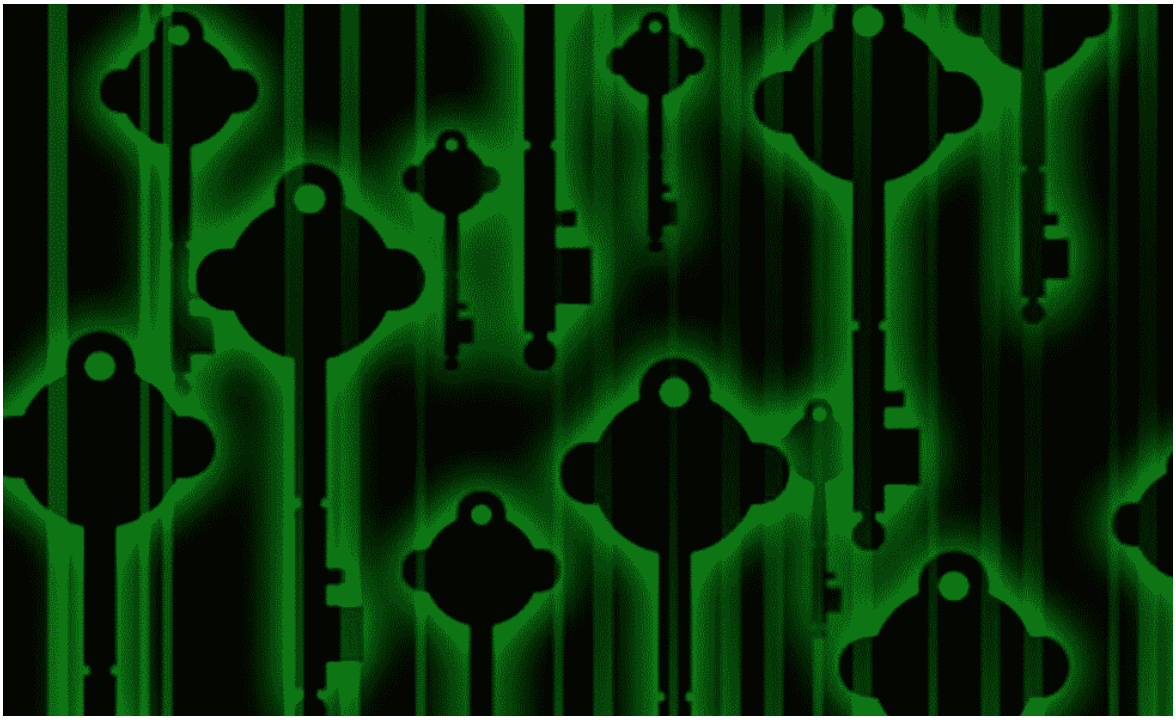

Battleground: Without Encryption, Technocracy Rules

Governments are being prompted to destroy encryption, permanently destroying privacy and handing all data in the world over to Technocrat social engineers. If successful, this will catapult the world into Scientific Dictatorship, aka Technocracy. TN Editor

In every country of the world, the security of computers keeps the lights on, the shelves stocked, the dams closed, and transportation running. For more than half a decade, the vulnerability of our computers and computer networks has been ranked the number one risk in the US Intelligence Community's Worldwide Threat Assessment – that's higher than terrorism, higher than war. Your bank balance, the local hospital's equipment, and the 2020 US presidential election, among many, many other things, all depend on computer safety.

And yet, in the midst of the greatest computer security crisis in history, the US government, along with the governments of the UK and Australia, is attempting to undermine the only method that currently exists for reliably protecting the world's information: encryption. Should they succeed in their quest to undermine encryption, our public

infrastructure and private lives will be rendered permanently unsafe.

In the simplest terms, encryption is a method of protecting information, the primary way to keep digital communications safe. Every email you write, every keyword you type into a search box – every embarrassing thing you do online – is transmitted across an increasingly hostile internet. Earlier this month the US, alongside the UK and Australia, called on Facebook to create a "backdoor", or fatal flaw, into its encrypted messaging apps, which would allow anyone with the key to that backdoor unlimited access to private communications. So far, Facebook has resisted this.

If internet traffic is unencrypted, any government, company, or criminal that happens to notice it can – and, in fact, does – steal a copy of it, secretly recording your information for ever. If, however, you encrypt this traffic, your information cannot be read: only those who have a special decryption key can unlock it.

I know a little about this, because for a time I operated part of the US National Security Agency's global system of mass surveillance. In June 2013 I worked with journalists to reveal that system to a scandalised world. Without encryption I could not have written the story of how it all happened – my book Permanent Record – and got the manuscript safely across borders that I myself can't cross. More importantly, encryption helps everyone from reporters, dissidents, activists, NGO workers and whistleblowers, to doctors, lawyers and politicians, to do their work – not just in the world's most dangerous and repressive countries, but in every single country.

When I came forward in 2013, the US government wasn't just passively surveilling internet traffic as it crossed the network, but had also found ways to co-opt and, at times, infiltrate the internal networks of major American tech companies. At the time, only a small fraction of web traffic was encrypted: six years later, Facebook, Google and Apple have made encryption-by-default a central part of their products, with the result that today close to 80% of web traffic is encrypted. Even the former director of US national intelligence, James Clapper, credits the revelation of mass surveillance with significantly advancing the

commercial adoption of encryption. The internet is more secure as a result. Too secure, in the opinion of some governments.

Donald Trump's attorney general, William Barr, who authorised one of the earliest mass surveillance programmes without reviewing whether it was legal, is now signalling an intention to halt – or even roll back – the progress of the last six years. WhatsApp, the messaging service owned by Facebook, already uses end-to-end encryption (E2EE): in March the company announced its intention to incorporate E2EE into its other messaging apps – Facebook Messenger and Instagram – as well. Now Barr is launching a public campaign to prevent Facebook from climbing this next rung on the ladder of digital security. This began with an open letter co-signed by Barr, UK home secretary Priti Patel, Australia's minister for home affairs and the US secretary of homeland security, demanding Facebook abandon its encryption proposals.

Read full story here...