Encryption

This article is more than **9 years old**

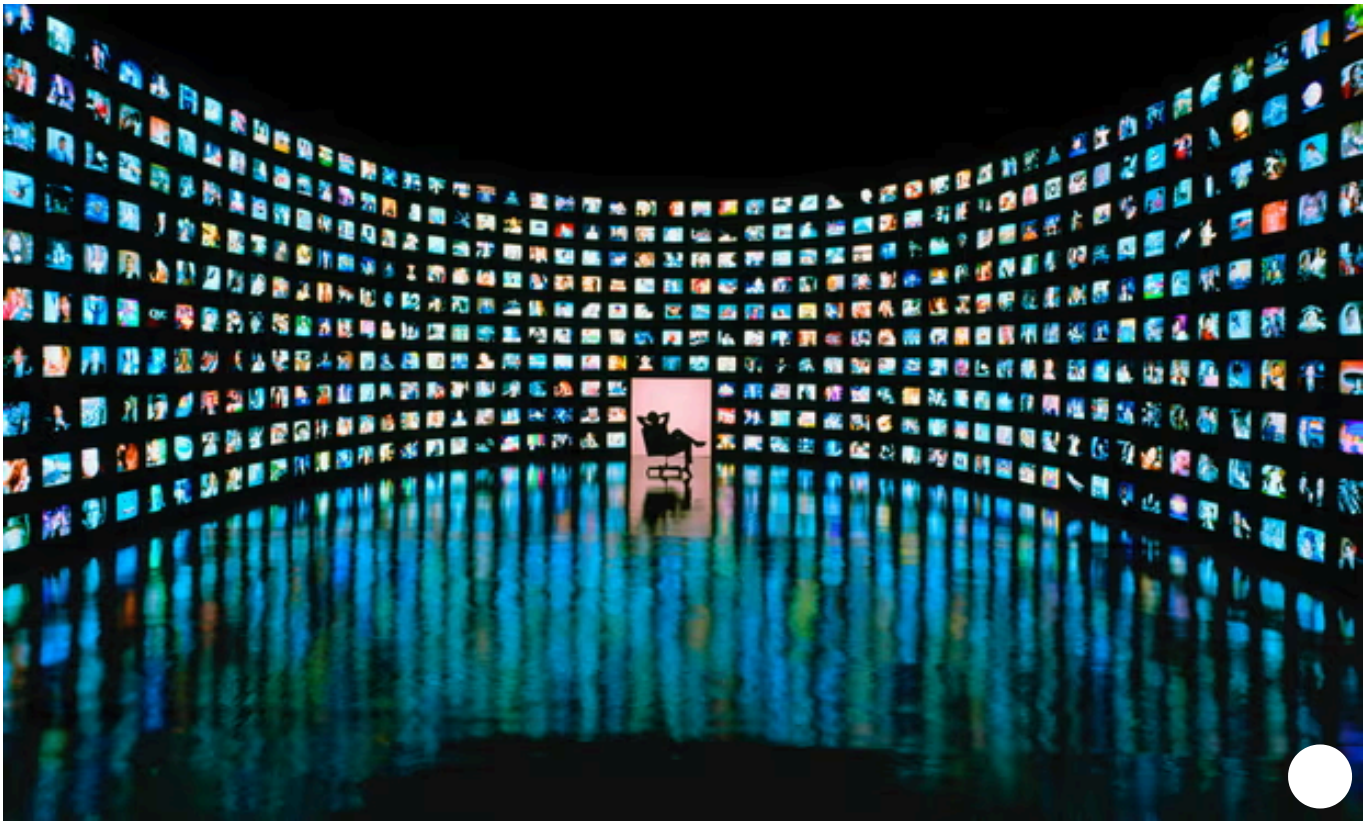
Crypto wars redux: why the FBI's desire to unlock your private life must be resisted

Cory Doctorow

In 1995, the US government tried – and failed – to categorise encryption as a weapon. Today, the same lines are being drawn and the same tactics repeated as the FBI wants to do the same. Here's why they are wrong, and why they must fail again

Your iPhone is now encrypted. The FBI says it'll help kidnappers. Who do you believe?

Thu 9 Oct 2014 16.37 BST



Eric Holder, the outgoing US attorney general, has joined the FBI and other law enforcement agencies in calling for the security of all computer systems to be fatally weakened. This isn't a new project - the idea has been around since the early 1990s, when the NSA classed all strong cryptography as a "munition" and regulated civilian use of it to ensure that they had the keys to unlock any technological countermeasures you put around your data.

In 1995, the Electronic Frontier Foundation won a landmark case establishing that code was a form of protected expression under the First Amendment to the US constitution, and since then, the whole world has enjoyed relatively unfettered access to strong crypto.

How strong is strong crypto? Really, really strong. When properly implemented and secured by relatively long keys, cryptographic algorithms can protect your data so thoroughly that all the computers now in existence, along with all the computers likely to ever be created, could labour until the sun went nova without uncovering the keys by "brute force" - ie trying every possible permutation of password.

The "crypto wars" of the early 1990s were fuelled by this realisation - that computers were changing the global realpolitik in an historically unprecedented way. Computational crypto made keeping secrets exponentially easier than breaking secrets, meaning that, for the first time in human history, the ability for people without social or political power to keep their private lives truly private from governments, police, and corporations was in our grasp.

The arguments then are the arguments now. Governments invoke the Four Horsemen of the Infocalypse (software pirates, organised crime, child pornographers, and terrorists) and say that unless they can decrypt bad guys' hard drives and listen in on their conversations, law and order is a dead letter.

On the other side, virtually every security and cryptography expert tries patiently to explain that there's no such thing as "a back door that only the good guys can walk through" (hat tip to Bruce Schneier). Designing a computer that bad guys can't break into is impossible to reconcile with designing a computer that good guys *can* break into.

If you give the cops a secret key that opens the locks on your computerised storage and on your conversations, then one day, people who aren't cops will get hold of that key, too. The same forces that led to bent cops selling out the public's personal information to Glen Mulcaire and the tabloid press will cause those cops' successors to sell out access to the world's computer systems, too, only the numbers of people who are interested in these keys to the (United) Kingdom will be much larger, and they'll have more money, and they'll be able to do more damage.

That's really the argument in a nutshell. Oh, we can talk about whether the danger is as grave as the law enforcement people say it is, point out that only a tiny number of criminal investigations run up against cryptography, and when they do, these

investigations always find another way to proceed. We can talk about the fact that a ban in the US or UK wouldn't stop the "bad guys" from getting perfect crypto from one of the nations that would be able to profit (while US and UK business suffered) by selling these useful tools to all comers. But that's missing the point: even if every crook was using crypto with perfect operational security, the proposal to back-door everything would still be madness.

Because your phone isn't just a tool for having the odd conversation with your friends - nor is it merely a tool for plotting crime - though it does duty in both cases. Your phone, and all the other computers in your life, they are your digital nervous system. They know *everything* about you. They have cameras, microphones, location sensors. You articulate your social graph to them, telling them about all the people you know and how you know them. They are privy to every conversation you have. They hold your logins and passwords for your bank and your solicitor's website; they're used to chat to your therapist and the STI clinic and your rabbi, priest or imam.

That device - tracker, confessor, memoir and ledger - should be designed so that it is as hard as possible to gain unauthorised access to. Because plumbing leaks at the seams, and houses leak at the doorframes, and lie-lows lose air through their valves. Making something airtight is much easier if it doesn't have to also allow the air to all leak out under the right circumstances.

There is no such thing as a vulnerability in technology that can only be used by nice people doing the right thing in accord with the rule of law. The existing "back doors" in network switches, mandated under US laws such as CALEA, have become the go-to weak-spot for cyberwar and industrial espionage. It was Google's lawful interception backdoor that let the Chinese government raid the Gmail account of dissidents. It was the lawful interception backdoor in Greece's national telephone switches that let someone - identity still unknown - listen in on the Greek Parliament and prime minister during a sensitive part of the 2005 Olympic bid (someone did the same thing the next year in Italy).

The most shocking Snowden revelation wasn't the mass spying (we already knew about that, thanks to whistleblowers like Mark Klein, who spilled the beans in 2005). It was the fact that the UK and US spy agencies were dumping $250,000,000/year into sabotaging operating systems, hardware, and standards, to ensure that they could always get inside them if they wanted to. The reason this was so shocking was that these spies were notionally doing this in the name of "national security"- but they were dooming everyone in the nation (and in every other nation) to using products that had been deliberately left vulnerable to attack by anyone who independently discovered the sabotage.

There is only one way to make the citizens of the digital age secure, and that is to give them systems designed to lock out everyone except their owners. The police have never had the power to listen in on every conversation, to spy upon every

interaction. No system that can only sustain itself by arrogating these powers can possibly be called “just.”

Edward Snowden to speak at Observer Ideas festival

Most viewed