We're actually entering an era where censorship becomes harder and privacy easier, says Jamie Bartlett. At the same time, we need a strong, publicly supported intelligence architecture. But in a post-Snowden world, the intelligence agencies must become more rather than less open.

The argument over national security and individual privacy is certainly a pressing issue, but it’s not a new one. How any democratic society weighs up and trades liberty against safety gets re-examined each time a new technology or threat disrupts the established order. Governments have a tendency to see each new technology as a means to help them maintain order; radicals as a way to disrupt it. If governments overreach whatever finely balanced consensus that has been reached on the extent to which governments can monitor its people, there is always a counter-reaction.

To understand the current messy debate about encryption, privacy and terrorism, the best place to start is not with Edward Snowden. One of the first major spy scandals of the modern age took place in 1844 when the British Home Secretary, Sir James Graham, decided to secretly monitor the letters of Giuseppe Mazzini, the exiled leader of La Giovine Italia (Young Italy), a radical movement hoping to create a united Italy. The public and chattering classes of the day rallied against what was largely seen as an indecent breach of individual privacy. This “Post Office Espionage Scandal” more or less put an end to the political spying on letters for 50 years.

Fast forward to the early 1990s, when networked computing was just taking off. Millions logged on for the first time, and, predictably, brought nasty baggage with them. Although still tiny, “cyberspace” was a nuisance to the law. Untraceable paedophile networks were sharing illegal images of children via the net. Anonymous hackers were stealing intellectual property. Internet trolling was rife (although less mean than its modern incarnation).

This made the authorities worried. In the USA, the Federal Bureau of Investigation upped its monitoring of the online world. In 1990, it launched Operation Sun Devil, a nationwide – and over the top – crackdown on hackers. Most importantly, lawmakers tried to pass legislation to force telecommunications companies to hand over its customers’ details, and prevent the spread of powerful cryptography software. Their arguments were very similar to those of today: they greatly feared a degradation of capability, of the Internet going dark, of the terrorists being untraceable, of cyberspace becoming lawless.
But, just as in Mazzini’s day, the response was not exactly what the government hoped for. Crime continued, and net users reacted angrily to what they saw as a blatant infringement of civil liberties in this new space. Their space. Leading the counter-attack were the “cypherpunks”, a group of Californian libertarians determined to develop and share tools and techniques to keep activity online secret, and to keep the net free of state interference. They set up an email list and ended up predicting, inventing or refining almost every technique now employed by computer users to avoid government surveillance. (Julian Assange, posting as “Proff”, became a member in 1995.) It was around this time that a programmer named Phil Zimmerman (although not himself a cypherpunk), who felt alarmed at what to him was a concerted and disproportionate push by the law into citizens’ private space, decided to make the code of his “Pretty Good Privacy” software freely available to all. PGP is now an industry standard. Around the same time, the Electronics Frontier Foundation – a digital liberties group – was set up and remains an influential and fierce defender of online privacy. These struggles were known as the crypto-wars, and they’re back. We now share inordinate amounts of information about ourselves online: our bank details, our love life, our holiday snaps; our whole lives are online. More and more of us worry about the digital traces we leave behind: about governments who can monitor what we do; about big tech companies that collect all our data in large centralized servers and sell it; and about invisible US-based regulators exercising control over what happens on the net. The Snowden revelations have turbocharged this movement. But it’s about a lot more than intelligence agencies. It’s about privacy, freedom, and control. Just as in the 1990s, there has been a response – and, again, one which is starting to haunt the companies and intelligence agencies that are perceived to have overreached. Internet privacy and surveillance are now a major political preoccupation. Anonymous browsers, such as Tor, which are used to browse the net without giving away your location, are becoming ever-more popular. Facebook users, who used to be happy sharing everything with anyone, are inching towards more private settings. Phil Zimmermann’s PGP encryption is being downloaded by millions. New social media companies and messenger services are popping up with more security built-in. Motivated by an honourable desire to protect online freedom and privacy, hundreds of computer scientists and Internet specialists are working on ingenious ways of keeping online secrets, preventing censorship, and fighting back against centralized control. There will soon be a new generation of easy-to-use auto-encryption email services, such as Mailpile and Dark Mail. Then there are projects like Ethereum, which is building a new web out of the spare power and hard-drive space of millions of connected computers that its owners put on the network. Because it runs with strong encryption and the network is “distributed” across all those individual computers, it’s more or less impossible for anyone to censor or control what’s on it. Another is called MaidSafe, based in Scotland, which works to similar principles. Another is Twister. And on, and on. More and more of us – ordinary, typical users – will start using these sorts of systems, because of the obvious benefits. The upshot is precisely the opposite of what big companies and intelligence agencies want. We’re entering into an era where censorship becomes harder and privacy easier. That means more privacy from dictatorships, advertisers, spies, cookies, and hackers. A great development if you care about individual freedom and democracy. But it’s also good news if you want to browse child pornography or push out radical Islamist propaganda – both of which benefit from the use of encrypted systems, of course. The lesson of the 1990s (and the 1840s) is that, in the end, overreaching into the sphere...
of the individual tends to backfire. But the other lesson is, naturally enough, that spying will not, and cannot, stop (nor should it). The original crypto-war was won by the cypherpunks. Powerful encryption was then de-criminalized in the US, and the attempts to control Internet encryption were dropped. But, in response, the NSA and others simply changed tack – and developed ever more sophisticated systems of spying, some of which would eventually turn into the subject of Edward Snowden’s revelations.

So spying work will continue – and we desperately need a strong and publicly supported intelligence architecture to help keep us safe: from cyber espionage, terrorism, nuclear proliferation and dictatorial regimes unconstrained by democratic controls. But in a post-Snowden world, the intelligence agencies will have to change the way they work again – becoming more rather than less open. They will have to change their focus: far less mass surveillance, and far more gathering of detailed and careful human intelligence online, more targeted hacking attacks on individuals’ devices.

At some point they will overreach once more, and the whole thing will start again. In some ways this is quite a healthy tension for societies that wish to be free and safe. And if we stay vigilant, each time, the balance will tip slightly closer towards greater individual freedom and liberty.

Published 6 October 2015
Original in English
First published in Index on Censorship 3/2015
Downloaded from eurozine.com (https://www.eurozine.com/under-the-radar/)
© Jamie Bartlett / Index on Censorship / Eurozine