Encryption risks leading to ‘ethically worse’ behaviour by spies,…

6-8 minutes

Sir David Omand by Chatham House/Flickr

The increasing use of encryption technologies in everyday emails and messaging services risks “ethically worse” behaviour by the intelligence agencies, a former head of GCHQ has predicted.

Sir David Omand warned there would be greater intrusion on individuals’ privacy, not less, if agencies are unable to intercept communications – because they will be forced into more direct spying methods.

He explains that would risk inadvertent interception of third parties, which would be an ethically worse position than mass surveillance.

US companies such as Apple and Google are introducing more sophisticated encryption options to their customers while signalling their unwillingness to co-operate in full with government demands to obtain their users’ data.

One way of getting around problems of reading encrypted messages on services such as Whatsapp and iMessage is to hack directly into people’s computers, phones and other devices, and monitor the messages as they are written.

Speaking at a public discussion at the London School of Economics on the post-Snowden world on Tuesday night, Sir David called for a debate on “network exploitation” – the term used by GCHQ for hacking.

National Security Agency whistleblower Edward Snowden leaked documents in 2013 that revealed mass communications surveillance by US and UK intelligence agencies.

Sir David, who was director of GCHQ from 1996-97, said: “One of the results of Snowden is that companies are now heavily encrypting [communications] end to end.

“Intelligence agencies are not going to give up trying to get the bad guys. They will have to get closer to the bad guys. I predict we will see more close access work.”

“Close access” means surveillance techniques that require physical proximity to the target. It could mean physical observation, bugging their room, or directly hacking into their mobile phones or computers.

Sir David said: “You can say that will be more targeted but in terms of intrusion into personal privacy – collateral intrusion into privacy – we are likely to end up in an ethically worse position than we were before.”

Related story: Thatcher and Blair Cabinet Secretary: Intelligence committee has helped public by confirming GCHQ’s internet tap ‘Tempora’ powers

Sir David also tried to reassure the audience that GCHQ’s work was not all “offence”. His former employer’s remit also includes defensive work such as protecting the UK from cyber attacks.

However, another panel member at the debate, Gus Hosein, executive director at campaigning NGO, Privacy International, argued GCHQ was placing less emphasis on that role than in the past.

While GCHQ had previously been expected to inform companies such as Apple if it found flaws in its software – vulnerabilities- “they’re not going to do that any more”, Hosein said.

He added: “They’re going to harvest these vulnerabilities, treat them like arms, pull them out and use them in a widespread manner that will not necessarily be targeted.”

But Sir David urged the audience to visit Apple’s and Microsoft’s websites.

He said: “Look at the list of software defects that have been reported to them – zero day defects that have to be fixed.

“You’ll find that large numbers of these have been reported by GCHQ… GCHQ has found flaws in software that is essential for the running of society. Don’t run away with the idea that it’s all offence.”

The Bureau was unable to see any reference to GCHQ reports on the companies’ websites.

Apple and Microsoft declined to comment on the numbers of zero day vulnerabilities reported to them by GCHQ.

Zero day vulnerabilities

GCHQ and some of its contractors employ researchers to uncover previously unknown software defects, known as “zero day vulnerabilities”.

An advertisement posted on various websites in October 2014 for a security-cleared software vulnerability researcher in Cheltenham, where GCHQ is based, said the successful applicant "will be involved in challenging cyber software security problems, both defeating and developing new & advanced security techniques" to "support key defence & government programmes".

The agency could also purchase these flaws, in which there is a burgeoning market with hackers selling the rare vulnerabilities they uncover to criminals and governments, sometimes for huge sums.

The defects may then be used to improve cybersecurity or to access systems belonging to other individuals, organisations or nations.

New documents from US National Security Agency (NSA) whistleblower Edward Snowden, published by Der Spiegel last weekend, reveal that at a hacking workshop in 2010, GCHQ staff worked out they could access Apple's iPhone while the user was downloading PDFs via the Safari browser.

A GCHQ team then developed an "exploit" – a piece of software or data which exploits weakness in a computer system or programme – to access data stored on the phones.

"The WARRIORPRIDE exploit has result in extraction of the target's address book, sms, call logs, notes, WLAN [wireless local area network] logs, bookmarks, map query history, Safari browsing history and some images," the Snowden file says.

Revelations of these practices have angered some cybersecurity experts and civil liberties campaigners as well as Apple itself.

They argue that the security and privacy of everyone using an iPhone was put at risk by this hacking programme, because a defect was left open for potential abuse by criminals and authoritarian governments for several years before the company changed its systems.

In the UK, the body responsible for information security and assurance is CESG (Communications-Electronic Security Group), which is an arm of GCHQ. Its role includes ensuring that the public sector IT is secure, securing on-line communications between the government and citizens as part of the UK's "digital strategy" and working with industry to protect national infrastructure against cyber attacks.

* This article was updated on January 28 after Sir David Omand contacted us to clarify and explain his remarks. The headline has been amended to say

“Encryption risks leading to ‘ethically worse’ behaviour” instead of “Encryption will lead to ‘ethically worse’ behaviour”. We have also added a paragraph to explain Sir David’s belief that the security services would be put in an “ethically worse” position as a result of more encryption, not that they would set out to be “ethically worse” in their motives.