UK parliamentary committee justifies mass spying on e-communications

Paul Mitchell
14 March 2015

The UK Parliament's Intelligence and Security Committee (ISC) published its report "Privacy and Security" on March 12 into the activities of the Government Communications Headquarters (GCHQ). Since the inquiry began in 2013, the ISC has taken evidence, both in public and in secret, from a variety of senior figures, including the heads of Britain's security services, MI5, MI6 and GCHQ.

The report is a whitewash, aimed at legitimising the mass surveillance apparatus exposed by former National Security Agency (NSA) whistleblower Edward Snowden in 2013.

The inquiry was convened after Snowden disclosed that GCHQ and the NSA were collaborating through the Tempora and Prism programmes to tap fibre-optic cables that carry global communications and sharing vast amounts of harvested data. Telecom companies had been forced to install equipment that duplicates the cable data and diverts it to GCHQ. According to Snowden, the UK Tempora programme was the first "full take" system developed in the world, allowing the wholesale collection of Internet traffic.

Snowden was bitterly denounced for making public the documents confirming this nefarious activity by then-ISC chair Sir Malcolm Rifkind. Snowden not only revealed the mass surveillance taking place but exposed the ISC for its role as a mouthpiece for the security services.

The UK government has adamantly refused to acknowledge the existence of Tempora and the scale of its activities, insisting that all surveillance carried out in the UK takes place in accordance with the law. The ISC merely regurgitates the government's line. In its entire 149-page report, the words "Prism" and "Tempora" do not warrant a single mention.

Instead, the document is littered with redactions concealing exactly how much data is gathered, filtered and read. Even so, the ISC still acknowledges that agents read an unspecified "*** thousand items a day". This figure could range from 1,000 to 999,000 and is a substantial amount of detailed surveillance of private communications and, as the ISC admits, only a tiny percentage of the data intercepted.

The ISC declares the "bulk interception" of communications to be legal and clears GCHQ of breaking surveillance rules and invading privacy. It recommends a single new law be introduced, replacing the existing "piecemeal" legislation, because the current laws could be thought to provide the agencies with a "blank cheque to carry out whatever actives they deem necessary". The ISC calls for greater transparency but then declares it won't be possible to "specify the detail of certain arrangements in legislation."

The report claims bulk collection is necessary to find out the "what, when, where" of every e-mail so the intelligence agencies can use "thousands of filters" to "find patterns and associations, in order to generate initial leads." It continues, "This is an essential first step before the agencies can then investigate those leads through targeted interception."

The targeted interception of communications "with both ends known to be in the UK" requires a ministerial warrant specifying an individual or address. In a separate report published on Thursday, the Interception of Communications Commissioner, who oversees the warrant system, revealed that 2,795 warrants had been granted in the UK in 2014.

Communications having only one end within the UK, whether leaving or entering, can be collected based on a list of categories defined in "the Certificate" and do not have to be targeted for a named individual or address.

However, the report points out that it is very difficult to determine what constitutes internal and external e-mail and that many of the activities are undertaken without any explicit authorisations.

The report describes how the agencies are increasing the number of Bulk Personal Datasets, "large databases containing personal information about a wide range of people—to identify individuals in the course of investigations, to establish links, and as a means of verifying information obtained through other sources."

The ISC defends "bulk interception" and "large" Bulk Personal Datasets, and notes that the commissioner responsible for overseeing the activities of the agencies operates under an "unsatisfactory and inappropriate" non-statutory framework, that MI6 undertakes intrusive operations abroad but is not obliged to record them, and that agents have been disciplined or sacked for "inappropriately" accessing personal information gathered from bulk interception. Nonetheless, the ISC comes to the sinister conclusion that GCHQ's activity is legal and "does not equate to blanket surveillance, nor does it equate to indiscriminate surveillance."

The ISC also describes how GCHQ is particularly concerned to solve "the encryption problem" and has three main elements in a programme to that end. One is "developing decryption capabilities"—possibly the development of encryption-breaking software. The other two elements have been redacted, but according to journalist Glenn Greenwald, who worked closely with Snowden to make public his revelations, may involve attempts to pressure encryption companies to provide get-arounds.

The ISC claims that bulk interception has stopped specific threats to the UK, but "these examples cannot be published, even in redacted form, without significant risk to GCHQ's capabilities, and consequential damage to the national security of the UK."

Mass surveillance is offered up as the answer to terrorism, but it failed to prevent attacks such as those in London, Boston, Paris and Copenhagen. It has emerged that every recent terrorist attack in the UK or by British citizens abroad was carried out by individuals who were well known to the intelligence agencies.

Responding to the ISC report, human rights organisation Privacy International declared that it "provides a long-awaited official confirmation that the British government is engaging in mass surveillance of communications. Far from allaying the public's concerns, the ISC's report should trouble every single person who uses a computer or mobile phone: it describes in great detail how the security services are intercepting billions of communications each day and interrogating those communications against thousands of selection fields.

"The ISC has attempted to mask the reality of its admissions by describing GCHQ's actions as 'bulk interception'. However, no amount of technical and legal jargon can obscure the fact that this is a parliamentary committee, in a democratic country, telling its citizens that they are living in a surveillance state and that all is well."

The report, which comes one month after a similar whitewash of the intelligence services by the Investigatory Powers Tribunal, smooths the way for further repressive powers for Britain's security services.

Following January's terror assaults on the *Charlie Hebdo* office in Paris and a Jewish supermarket, in which 17 people were killed, the UK government and intelligence agencies demanded an intensification of their surveillance powers. Former MI-5 head Lord Evans claimed that existing anti-terror legislation was "no longer fit for purpose" and new laws were "vital" to enable the state to monitor e-mails and social media web sites such as Facebook and Twitter.

Prime Minister David Cameron pledged that if the Conservatives return to power after May's General Election, they will speed up plans for a "snoopers' charter" Communications Data Bil l,

giving the intelligence agencies the power to access all encrypted communications.

The author also recommends: US and UK intelligence agencies hacked cell phone encryption keys 21 February 2015 NSA strategy document envisions unrestrained global surveillance 26 November 2013