

Every Internet user in the UK can be spied on without a warrant

Robert Stevens
23 June 2014

The UK government has acknowledged that every UK citizen who uses Google and accesses web site services Facebook, Twitter and YouTube, can be monitored, under existing legislation, by the security services.

In an ongoing court case, Charles Farr, the director general of the Office for Security and Counter-Terrorism, said that emails to or from non-British citizens abroad were also legally accessible because they are deemed to be “external communications.”

Farr issued the statement last week to defend the government, in response to a case brought by Privacy International, Liberty, Amnesty International and other civil rights groups.

Privacy International is demanding the UK government end its use of the data collected on hundreds of millions of people by Prism, the mass surveillance system operated by the United States’ National Security Agency (NSA). The group is calling for an injunction against the Tempora system, which according to documents made public by NSA whistleblower Edward Snowden, is used by the UK’s Government Communications Headquarters (GCHQ) programme to systematically spy on the entire British population.

Privacy International is forced to bring its case before the quasi-judicial Investigatory Powers Tribunal (IPT), supposedly tasked with investigating claims regarding the UK’s spy agencies. A thoroughly undemocratic body, it was created under the Regulation of Investigatory Powers Act (RIPA) 2000, meets in secret and is not required to make a determination on a complaint. Its decisions are not made public and cannot be appealed to any higher authority.

The IPT is to hold hearings in the case next month and will be open to the public.

In his statement, Farr said that UK citizens communicating through servers that are in other countries could be targeted for monitoring by the intelligence

services without the legal requirement of a warrant.

The RIPA legislation, passed in 2000 by a Labour government, allows virtually every governmental body, department and affiliated organisation including HMRC (Revenues & Customs) to seek powers of surveillance in the national interest, whether for security, economic or other purposes.

Section 8(1) of RIPA stipulates that “internal” communications between British residents within the UK may only be monitored pursuant to a specific warrant connected to a specific individual or address. Such warrants should, according to the law, only be granted where there is some reason to suspect the person in question of unlawful activity. However, there are no such limits in place for “external communications”, which can be monitored without any hindrance under a general warrant, according to section 8(4) of the Act.

Farr stated that a Google search “is a communication between the searcher’s computer and Google’s web server.” Google’s “largest centres are in the US, and its largest European centres are outside the British Islands” and so use of these were “external communications.” This was the case even when the individual doing the Google search was located in the UK, as the search was being facilitated by a server in another country.

Facebook and Twitter also fell under the remit of “external” communications. Farr did not say so, but this categorisation would also cover the private messaging systems within such social media. As these were communications with a “web-based platform” in another country, they did not “require a person or a set of premises to be named in the interception warrant”.

While acknowledging the existence of Prism, “because it has been expressly avowed by the executive branch of the US government”, Farr refused to do so for the British government’s own mass surveillance system, Tempora. Tempora operates on a similarly massive scale to that of

Prism and is able to record 600 million so-called telephone events per day. It sucks in vast amounts of information from data interceptors placed on more than 200 fibre-optic cables carrying Internet data in and out of the UK. These include the cables dealing with Internet traffic between the US and Europe. According to the Snowden documents, the data taken in by Tempora is so voluminous it requires 300 GCHQ and 250 NSA operatives to sift through it.

Farr's statement referred to the "alleged Tempora interception operation", adding, "All I am able to confirm is that *if* the Tempora interception operation existed, it would have been carried out under the authority of the section 8 (4) [RIPA] regime..." (emphasis in original).

Farr stated that, "the government has accepted that Mr. [David] Miranda [partner of former *Guardian* journalist Glenn Greenwald who broke the Snowden revelations] was in possession of 58,000 stolen classified GCHQ documents when he was stopped pursuant to a Schedule 7 of the Terrorism Act 2000 at Heathrow Airport on 18 August 2013". Miranda is currently appealing this blatant infringement of his democratic rights, sanctioned at the highest levels by London and Washington.

The government attempted to justify Miranda's detention on the basis that they understood he was carrying material from Snowden and was a risk to "national security". Yet Farr continues blithely, "However, the government has not accepted the provenance for the documents which formed the basis for the media articles on the alleged Tempora interception operation; nor has the government confirmed or denied the provenance of any particular document that is alleged to have been stolen by Mr. Snowden."

In his submission, Farr attempted to justify the mass collection of data by the UK on the basis that the way "an electronic message reaches its intended recipient can be infinitely varied" and that the "route will not necessarily be the route that is geographically the shortest."

On this basis he stated, "It will be apparent that the only practical way in which the Government can ensure that it is able to obtain at least a fraction of the type of communication in which it is interested is to provide for the interception of a large volume of communications..."

As a member of the "Five Eyes" alliance with other English-speaking countries, GCHQ has developed its methods for decades in close collaboration with intelligence counterparts in the US, Canada, New Zealand and Australia; all of which have access to almost unfathomable amounts of intercepted data as the result of

mass and systematic surveillance of the planet's population.

Farr states that the UK's connections with the US mass spying operations are the most valuable as the "US intelligence agencies are far larger and much better resourced than the [UK] Intelligence Services."

He notes that in the 2012 fiscal year the US Intelligence budget was \$34.5 billion, while the 2013-14 budget for the UK spies was £1.9 billion.

Reading Farr's statement one would conclude the spies in GCHQ consist of bumbling, largely amnesiac people who sit around all day with only the most casual and passing interest in the data they have intercepted—which they almost inevitably and instantly forget all about anyway!

Farr cites the Interception of Communications Commissioner's 2013 annual report, which stated that "material which is of no intelligence interest is very quickly passed over, as often as not without being read or listened to."

The commissioner continued, "Meanwhile the analyst, being only human and having a job to do, will have forgotten (if he or she ever took it in) what the irrelevant communication contained. I have sat next to analysts and heard or seen this happening; any assessment of the degree of real intrusion should appreciate that this is what inevitably happens on the ground. The active intrusion is insignificant."



To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact