UK spy agency admits hacking phones and computers without warrants

Trevor Johnson
15 December 2015

Evidence given in a hearing brought against the Government Communications Headquarters (GCHQ), by Privacy International and seven international internet service providers has shed further light on its mass surveillance operations.

Privacy International is an international campaign group for private and unmonitored use of the Internet. The case is being heard at the Investigatory Powers Tribunal (IPT), which deals with complaints about the intelligence services and surveillance by government organisations. The four-day hearing in Central London is the result of American whistleblower Edward Snowden's exposure of illegal and widespread abuse of power by both the US-based National Security Agency (NSA) and GCHQ.

Snowden revealed GCHQ's use of computer network exploitation (CNE), also known as hacking, against whole sections of the population inside the UK and internationally. The programmes included ones with the following codenames: "Nosey Smurf, which involved implanting malware to activate the microphone on smartphones; Dreamy Smurf, which had the capability to switch on smartphones; Tracker Smurf, which had the capability to provide the location of a target's smartphone with high precision; and Paranoid Smurf, which ensured all malware remained hidden."

Snowden gave more details on these programs in a Panorama documentary aired on the BBC last October.

During the case, GCHQ admitted for the first time in court that it engages in computer hacking. Previously it had refused to confirm or deny whether it had such capabilities. In 2013, 20 percent of GCHQ intelligence reports were based on information from hacking, the tribunal heard. That proportion is likely to have increased since then, as the use of encryption has made it more difficult to listen in on communications.

Ben Jaffey, counsel for Privacy International, told the IPT, "GCHQ undertakes 'persistent' CNE operations where an implant 'resides' in a targeted computer for an extended period to transmit information or 'non-persistent operations' where an implant expires at the end of a user's internet session."

CNE is so effective that having a smartphone is like "carrying around a bug with you."

The intelligence services are accused of using generalised "thematic" warrants that do not refer to named individuals or addresses but instead refer to whole categories of people or places. These are an "exorbitant" extension of normal powers, Jaffey told the tribunal. Under Section 5 of the Intelligence Services Act, safeguards are bypassed allowing the targeting of groups as loosely defined as "all mobile telephones" in Birmingham, the UK's second largest city.

One instruction aimed at GCHQ staff states, "CNE involves gaining remote access to computers and networks and possibly modifying their software without the knowledge or consent of the owners and users with the aim of obtaining intelligence. ... CNE operations carry political risk. These risks are assessed by the relevant team—consult them at an early stage if you're considering a CNE operation."

Following a written response to the IPT by Ciaran Martin, director of cyber security at GCHQ, Privacy International concluded, "Previously secret documents, and witness statements produced by GCHQ now reveal and confirm:

"GCHQ confirmed that the Secretary of State does not individually sign off on most hacking operations abroad, but only when 'additional sensitivity' or 'political risk' are involved.

"Overseas hacking does not require authorisations to

name or describe a particular piece of equipment, or an individual user of the equipment…"

The response also acknowledged that the monitoring agency does most of its surveillance work based on Section 5 ("class" or "thematic") authorisations:

"GCHQ primarily operate under class authorisations and have very few specific section 7s [authorised targeting of named individuals]."

Lawyers representing GCHQ argued, "GCHQ and other intelligence agencies must develop innovative and agile technical capabilities to meet these serious national security challenges. Computer network exploitation is one such capability… CNE may, in some cases, be the only way to acquire intelligence coverage of a terrorist suspect or serious criminal in a foreign country."

The reality is that, in virtually every terrorist-related incident from 9/11 to the latest attacks in Paris, far from being the work of unknown quantities that would require generalised surveillance to detect, the perpetrators have been well-known to the security services. In some cases, they were seen as potential recruits.

The other argument used in justification of the intrusive spying activities of GCHQ and MI5 is that that they are merely asking for their powers to be kept up to date with modern methods of communication.

This argument is fraudulent. The scale of state surveillance revealed by Snowden has no precedent. The British state now reserves the right to treat the mobile phones, computers and networks of its own citizens and those of other countries as its own property, to be interfered with, controlled and vetted—even when their owners are not accused of any crime. Whereas in previous centuries the state had to at least formally treat "every Englishman's home as his castle" and not attempt to gain entry without a legal warrant, it now arrogates to itself the right to use all electronic devices as an extension of its own surveillance network.

The NSA and GCHQ have been engaged in large-scale and illegal surveillance of the world's population for a number of years, while lying to anyone who tried to ascertain what they were doing.

While the IPT poses as a neutral arbiter, ensuring fairness for UK citizens in their treatment by the secret services and police, it is an essential part of the state machine it purports to be regulating. Since being set up in 2000, the IPT has upheld only 10 of the 1,468 complaints brought to its attention (0.68 percent).

Whether or not the IPT finds in favour of a complainant, it does not disclose whether he or she has been the subject of investigation by the security services or what methods of investigation were used.

When the IPT decides that a complaint should be upheld, this leads to little more than a rewording of legislation to ensure that operations can continue. The governments' move to legislate what is dubbed the " Snoopers' Charter" is the most recent example of this. In response to Snowden's exposures, the legislation brings many of the formerly illegal practices within the remit of the law without any accounting for who was responsible for the prior abuse of power and law-breaking.

In December the IPT ruled, in another case brought by Privacy International and others, that mass surveillance under GCHQ's Tempora programme was legal.

Given this record and the ruling elite's increasing reliance on authoritarian methods to prolong its existence, it is likely that the IPT will find against Privacy International and the other complainants and allow the mass surveillance and hacking by GCHQ to continue.