UK government seeks additional surveillance powers, including overriding encryption

Barry Mason
20 May 2017

A recent leaked document highlights how the UK Conservative government intends to spy on thousands of internet and phone users in real-time.

Its proposed measures dramatically weaken the ability to protect privacy through the use of encryption.

The plans only became known due to the Open Rights Group, a UK digital campaigning organisation whose remit is to protect the right to privacy and free speech online, releasing the leaked government Home Office consultation document.

The document is a draft statutory instrument. Despite its dry title; "The Investigatory Powers (Technical Capability) Regulations 2017," the document spells out how Internet Service Providers (ISPs) and phone companies, at one day's notice, would be obliged to give real-time access to a named individual including any related "secondary data." It also puts a legal requirement on data providers to set up backdoor access to their systems to allow the UK state to override end-to-end encryption of data.

The draft proposals would build on the already draconian Investigatory Powers Act. The IPA, known as the "Snoopers' Charter", passed into law last December. It is an unprecedented attack on the rights and privacy of every UK citizen. The Open Democracy group described it as the "most sweeping surveillance powers ever seen, not just in the UK, but in any western European nation or in the United States."

The act began as the Investigatory Powers Bill (IPB), the flagship policy of then Home Secretary and now Prime Minister Theresa May, who introduced it to parliament in November 2015. The act brings together previously diverse sets of rules into one piece of legislation. It also provides a legal stamp to vast illegal spying operations against the entire UK population, has been carried out for years by the intelligence apparatus without legal authorisation—before being exposed by the US whistleblower Edward Snowden.

The act allows the state to monitor every web site visited by an individual as well as comments made and search terms used. It also compels tech companies to hack into customers' devices at the request of state spying agencies to override their security, enabling the bulk hacking of millions of people's electronic devices on the say-so of the home secretary. The IPA compels Internet Service Providers to keep Internet connection records for a 12-month period for access by the police and security services.

The nine-page document leaked by the Open Rights Group was produced and sent out for a four week consultation to six telecom companies, BT, O2, BskyB, Cable & Wireless, Vodafone and Virgin Media. These companies comprise the Technical Advisory Board, along with state spying agencies. It is presumed that a representative of one of the six telecom companies, concerned over the invasion of privacy implications decided to leak the document to the Open Rights Group. There is no mention of the consultation document on the Home Office web site or on the UK government information website, gov.uk.

Responses have to be made by May 19 to the Home Office. The Open Rights Group noted, "This is a 'targeted consultation'—and has not been publicised to the tech industry or public. The Secretary of State is in fact not under any obligation to consult the public, but must consult only a small selection of organisations listed in Section 253 (6) of the Investigatory Powers Act."

The leaked document spells out how telecommunication operators would be required to "provide and maintain the capability to ensure, where practicable, the transmission of communications and

secondary data in near real time to a hand-over point as agreed with the person to whom the warrant is addressed… To provide and maintain the capability to disclose, where practicable, the content of communications or secondary data in an intelligible form and to remove electronic protection… to permit the person to whom the warrant is addressed to remove such electronic protection."

The authorization to carry out such surveillance on an individual would come from a secretary of state (a cabinet minister in charge of a government department), overseen by a judge appointed by the prime minister.

The *Register*, a web site carrying IT related news, commented on the leaking of the consultation document, "In addition, comms providers will be required to make bulk surveillance possible by introducing systems that can provide real-time interception of 1 in 10,000 of its customers. Or in other words, the UK government will be able to simultaneously spy on 6,500 folks in Blighty [the UK] at any given moment."

Just in the case of BT, which has nine million British broadband customers, fully 900 people using its services could be, legally, monitored in real time, without their knowledge.

The *Register* concluded that the document would "effectively make strong and unbreakable encryption illegal. This act of stripping away safeguards on people's private data is also fantastic news for hackers, criminals, and anyone else who wants to snoop on Brits. The seals are finally coming off."

Writing on the techworld web site May 5, journalist Scott Carey commented, "Simply put, either a message is encrypted or it is not. If there is backdoor for security services, there is essentially a backdoor for anyone with the right skills to exploit it, it is a Pandora's box."

While the government is not under any legal obligation to inform the public about draft regulations under consideration, it would have to pass both Houses of Parliament to become law. Jim Killock, executive director of the Open Rights Group, told the BBC, "The public has a right to know about government powers that could put their privacy and security at risk."

The IPA was finally put on the statute books by the Conservative government elected in 2015, led first by Prime Minister David Cameron and now by May. Should the Conservatives win the June 8 snap election, they will extend its scope along the lines laid out in the leaked document.

However, workers cannot look to the Labour Party to oppose a further massive abrogation of democratic rights. In parliament, Labour ensured the Investigative Powers Bill became law—offering only a few, token and minor amendments. Most Labour MPs voted for the IPA at its final reading. Labour's general election manifesto makes no mention of state surveillance whatsoever, or of the IPA—despite it being introduced since the last election in 2015. If elected, Labour would use the vast powers now available to the state to monitor the entire population just as surely as will the Tories.