GlobalResearch
Center for Research on Globalization

Britain's "Snooper Charter": U.K. Parliament Approves Unprecedented Hacking and Surveillance Powers

By Ryan Gallagher
Global Research, November 26, 2016

Region: Europe
Theme: Law and Justice, Police State & Civil Rights

A few years ago, it would have been unthinkable for the British government to admit that it was hacking into people's computers and collecting private data on a massive scale. But now, these controversial tactics are about to be explicitly sanctioned in an unprecedented new surveillance law.

Last week, the U.K.'s Parliament approved the Investigatory Powers Bill, dubbed the "Snoopers' Charter" by critics. The law, which is expected to come into force before the end of the year, was introduced in November 2015 after the fallout from revelations by National Security Agency whistleblower Edward Snowden about extensive British mass surveillance. The Investigatory Powers Bill essentially retroactively legalizes the electronic spying programs exposed in the Snowden documents — and also expands some of the government's surveillance powers.

Perhaps the most controversial aspect of the new law is that it will give the British government the authority to serve internet service providers with a "data retention notice," forcing them to record and store for up to 12 months logs showing websites visited by all of their customers. Law enforcement agencies will then be able to obtain access to this data without any court order or warrant. In addition, the new powers will hand police and tax investigators the ability to, with the approval of a government minister, hack into targeted phones and computers. The law will also permit intelligence agencies to sift through "bulk personal datasets" that contain millions of records about people's phone calls, travel habits, internet activity, and financial transactions; and it will make it legal for British spies to carry out "foreign-focused" large-scale hacks of computers or phones in order to identify potential "targets of interest."

"Every citizen will have their internet activity — the apps they use, the communications they send, and to who — logged for 12 months," says Eric King, a privacy expert and former director of Don't Spy On Us, a coalition of leading British human rights groups that campaigns against mass surveillance. "There is no other democracy in the world, possibly no other country in the world, doing this."

> There is no other democracy in the world, possibly no other country in the world, doing this.

King argues that the new law will cause a chilling effect, resulting in fewer people feeling

comfortable communicating freely with one another. He cites a Pew surveypublished in March 2015 that found that 30 percent of American adults had altered their phone or internet habits due to concerns about government surveillance. “It’s going to change how people communicate and express their thoughts,” King says. “For a society that’s supposed to be progressive, that encourages open debate and dialogue, it’s awful.”

Other civil liberties advocates are concerned that the new law will be viewed by governments across the world as a green light to launch similar sweeping surveillance regimes. “The passing of the IP Bill will have an impact that goes beyond the U.K.’s shores,” says Jim Killock, executive director of the London-based Open Rights Group. “It is likely that other countries, including authoritarian regimes with poor human rights records, will use this law to justify their own intrusive surveillance powers.”

Despite the broad scope of the Investigatory Powers Bill, it generated little public debate in the U.K., and did not receive a great deal of coverage in the mainstream press. One reason for this was undoubtedly the U.K.’s shock vote in June to leave European Union — known as Brexit — which has dominated news and discussion in recent months. But there was another major factor for the swift passage of the law in the face of little backlash. The Labour Party, the U.K.’s leading opposition political party, had pledged to fight back against “unwarranted snooping,” but ended up supporting the government and voting in favor of the new surveillance law. “Blame has to be fixed on the Labour Party,” says Killock. “They asked for far too little and weren’t prepared to strongly challenge many of the central tenets of the bill.”

In an effort to placate some of its critics, the government has agreed to strengthen oversight of the surveillance. The Investigatory Powers Bill introduces for the first time a “judicial commissioner” — likely a former senior judge — who will have the authority to review spying warrants authorized by a government minister. It also bolsters provisions relating to how police and spy agencies can target journalists in a bid to identify their confidential sources. New safeguards will mean the authorities will have to seek approval from the judicial commissioner before obtaining a journalist’s phone or email records; previously they could obtain this data without any independent scrutiny.

The U.K.’s National Union of Journalists, however, believes that the law does not go far enough in protecting press freedom. The union is particularly alarmed that any potential surveillance of media organizations will be kept completely secret, meaning they will not be afforded the chance to challenge or appeal any decisions relating to them or their sources. “The bill is an attack on democracy and on the public’s right to know and it enables unjustified, secret, state interference in the press,” the union blasted in a statement last week, adding that “the lack of protection for sources has an impact on journalists working in war zones or those investigating organized crime or state misconduct.”

Other issues relating to how the law will be applied remain unclear. It contains a provision, for instance, allowing the government to serve a company with a “technical capability notice,” which can include “obligations relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data.” Earlier this year, technology giants Apple, Facebook, Google, Microsoft, Twitter, and Yahoo criticized this power, expressing concerns that it could be used by the government to force companies to weaken or circumvent encryption technology used to protect the privacy of communications and data.

In practice, if the law is used to undermine encryption, it may never come to light. The government included a section in the law that criminalizes “unauthorized disclosures” of any information related to its surveillance orders, which could potentially deter any whistleblowers or leakers from coming forward. The punishment for breaches is a prison sentence of up to 12 months, a fine, or both.

Though the Investigatory Powers Bill will soon to come into force, it is likely to face several lawsuits. There are at least three ongoing cases that could result in changes to some of its provisions. One of these cases is a major challenge in the European Court of Human Rights, which could potentially rule the government’s mass collection and retention of data to be illegal. (Judgments from the European Court of Human Rights remain binding in the U.K., despite its vote to leave the European Union.)

Either way, some are not willing to leave it up to the courts to determine how much of their data the government can vacuum up. One recently established British nonprofit company, calling itself Brass Horn Communications, says it is planning to build a new internet provider that is based on Tor — a tool used to browse the internet anonymously — in an effort to help people protect themselves from the spying. “We should be able to research an embarrassing medical condition, or ask questions on Google, without having to worry about it being stored on a permanent internet record somewhere,” says a spokesperson for the company. “The government has decided that everyone is a suspect, but you can’t treat an entire society as criminal.”

Articles by: Ryan Gallagher