GlobalResearch
Center for Research on Globalization

The UK Now Wields Unprecedented Surveillance Powers — Here's What it means

By James Vincent
Global Research, December 09, 2016
The Verge 29 November 2016

Region: Europe
Theme: Police State & Civil Rights

The UK is about to become one of the world's foremost surveillance states, allowing its police and intelligence agencies to spy on its own people to a degree that is unprecedented for a democracy. The UN's privacy chief has called the situation "worse than scary." Edward Snowden says it's simply "the most extreme surveillance in the history of western democracy."

The legislation in question is called the Investigatory Powers Bill. It's been cleared by politicians and granted royal assent on November 29th — officially becoming law. The bill will legalize the UK's global surveillance program, which scoops up communications data from around the world, but it will also introduce new domestic powers, including a government database that stores the web history of every citizen in the country. UK spies will be empowered to hack individuals, internet infrastructure, and even whole towns — if the government deems it necessary.

Although the UK's opposition Labour Party originally put forward strong objections to the bill, these never turned into real opposition. The combination of a civil war between different factions in Labour and the UK's shock decision to leave the European Unionmeans the bill was never given politicians' — or the country's — full attention. Instead, it will likely inspire similar surveillance laws in other countries. After all, if the UK can do it, why shouldn't everyone else? And there will be no moderating influence from the US, where the country's mostly intact surveillance apparatus will soon be handed over to president-elect Donald Trump.

With this global tide of surveillance rising, it's worth taking a closer look at what exactly is happening in the UK. Here's our overview of what the Investigatory Powers Bill entails:

A NATION'S BROWSER HISTORY AND A SEARCH ENGINE TO MATCH

The UK government will keep a record of every website every citizen visits for up to a year, with this information also including the apps they use on their phone, and the metadata of their calls. This information is known as internet connection records, or ICRs, and won't include the exact URL of each site someone visits, but the base domain. For this particular webpage, for example, the government would know you went to www.theverge.com, the time you visited, how long you stayed, your IP address, and some information about your computer — but no individual pages.

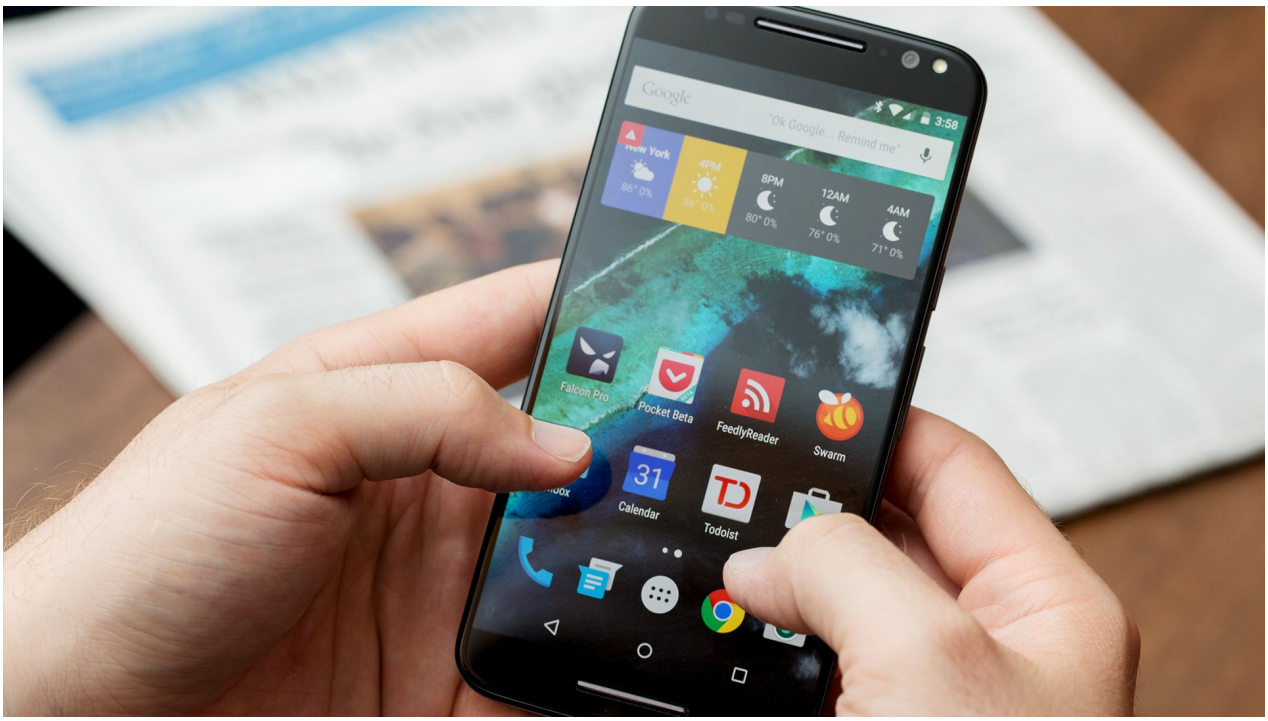
Each Internet Service Provider (ISP) and mobile carrier in the UK will have to store this data, which the government will pay them to do. Police officers will then be able to access a

central search engine known as the "request filter" to retrieve this information. Exactly how this request filter will work still isn't clear (will you be able to find every visitor to a certain website, for example, then filter that down to specific weeks or days?), but it will be easy to tie browsing data to individuals. If you sign a contract for your phone, for example, that can be linked to your web history.

There are a few ways this data could be muddied. For a start, services like VPNs and Tor, that bounce your internet traffic around the world, will be difficult to follow. And when it comes to tracking activity on your phone — for an app like Facebook Messenger, for example — this information will be fairly useless, as most of these apps maintain regular connections to the internet throughout the day. "The government won't be able to get all of the data all of the time," Jim Killock, executive director of the UK's Open Rights Group tells *The Verge*. "But they're not expecting most people to bother to protect their privacy."

The key point about this power, though, is that it has no judicial oversight. Access to citizens' web history will be solely at the discretion of the police, with a specially trained supervising officer approving or denying requests. "It makes this kind of surveillance a simple, routine activity," says Killock, adding that without oversight, it'll be impossible to know when police target specific groups disproportionately. That's definitely a problem in a country where even senior law enforcement officers admit that claims that the police force is institutionally racist have "some justification."

Although this power sounds almost farcical in its reach ("The police will know what porn you look at! They'll know how much time you waste on Facebook!"), it's no laughing matter. It's not as intrusive as other measures, but it establishes a dangerous new norm, where surveillance of all citizens' online activity is seen as the baseline for a peaceful society. Collect evidence first, the government is saying, and find the criminals later. The country has a surprising tolerance for this, embracing the use of surveillance cameras more than most. Now, though, it has CCTV for the nation's online life.



Other parts of the bill don't introduce new powers, but establish surveillance and hacking activities revealed by the Snowden revelations. These include the collection of metadata from around the world, and targeted hacking of individuals' computers — bugging their phone calls, reading texts, and so on. Unlike access to browser history, these latter powers will require a warrant from both the Secretary of State and a panel of judges.

The government has given hacking the deceptively understated description of "equipment interference," and splits it into two camps: targeted and bulk. Targeted equipment interference allows law enforcement and security agencies to hack specific devices, phones or computers, while bulk hacking can cover larger groups. The only difference between the two powers is that bulk hacking is only authorized for foreign targets.

We already know quite a bit about these capabilities thanks to Snowden's leaks, and they cover the sort of malware and spyware you might expect any hacker to use. GCHQ's toolkit, for example, includes a collection of programs named after smurfs: "Nosey Smurf" activates a device's microphone to record conversations; "Tracker Smurf" hijacks its GPS to track location in real time; while "Dreamy Smurf" allows a phone that appears to be off to secretly turn itself on.

The headquarters of GCHQ, the UK's signals intelligence agency.

Out of all the new legislation, targeted hacking has probably been objected to the least. This is because it will require a warrant approved by both government ministers and a specially appointed panel of seven judicial commissioners — the so-called double lock procedure — and will be reserved for "serious crimes" and threats to national security. This sort of interception also takes place on a much smaller scale. The UK police made more than half a

million requests for metadata last year, but there were only around 2,700 warrants for directly intercepting communications in the same period.

However, what is new is the authorization of "bulk equipment interference" or the hacking of large groups of people. This power will be limited to the security agencies and can only be used outside of the UK, but the government is clear about its potential scope. It's said that if it needs to hack every phone and laptop in a "major town" to stop a terrorist attack, it will; and it's suggested that it might be used to take over the entire internal email system of a "hypothetical totalitarian state," if it's developing biological weapons.

There's also the worry that the targeted hacking laws could be used to hack multiple people under the use of something called a "thematic warrant." Ross Anderson, a professor of security engineering at Cambridge University who gave testimony about the IP bill to the government, gives the example of the police chief of a UK city wanting to stem knife crime, and asking the government to force Google to get data from Android smartphones. "The point is that it's possible," Anderson tells *The Verge*. "Perhaps the government has given some private assurances to these companies [that it won't happen], but we know from long experience that such private assurances are not worth the paper they're not written on."

In addition to bulk hacking, the IP bill legalizes the bulk collection of communication data from around the world, activity that Snowden first revealed in 2013. The UK courts judged that this activity was in breach of human rights law earlier this year, but once the IP bill passes, it'll be absolutely legal. Although the government claims that this sort of information is treated respectfully, its own internal memos have shown staff abusing their powers; using bulk datasets for things like finding addresses to send birthday cards, and "checking details of family members for personal convenience."

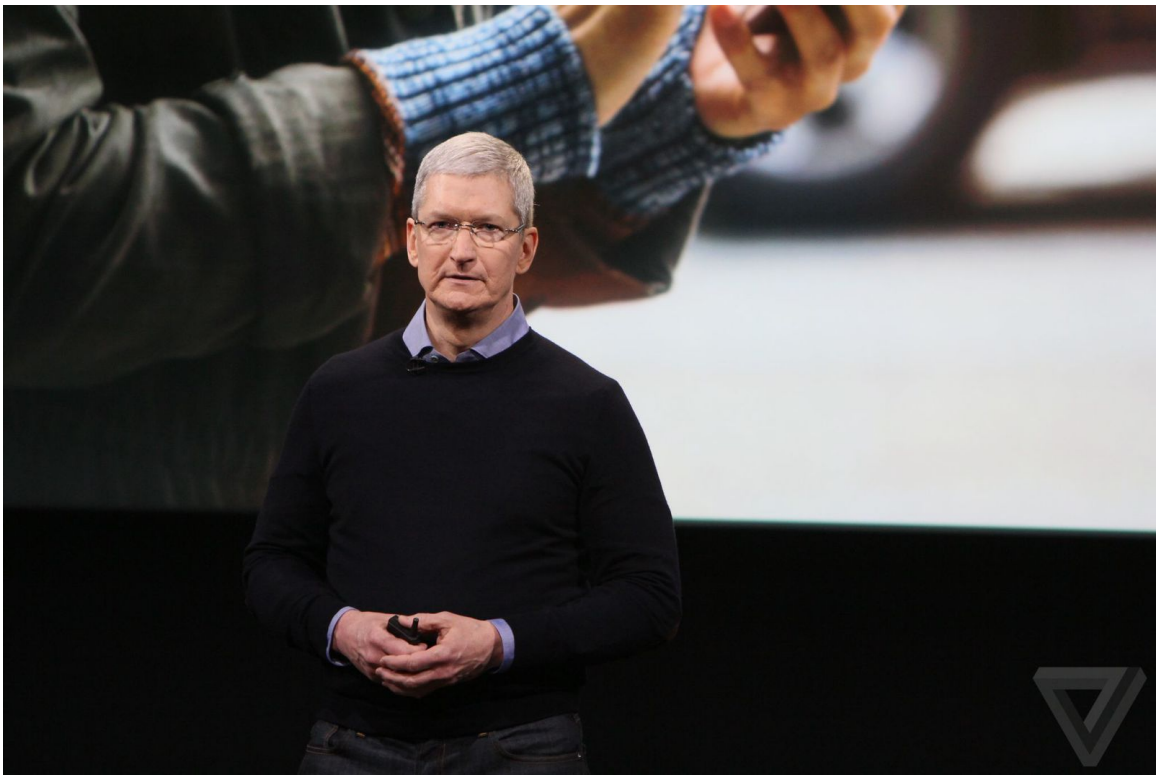
THE UK WILL BREAK ENCRYPTION — IF IT DARES

One of the biggest trouble spots for the bill, though, isn't so much an explicit power as an assumption by the government — namely, that it can force tech companies to decrypt user data on demand.

Now, there are a lot of caveats to this statement. Firstly, requests for this data will be on a small scale, like targeted hacking. Secondly, the wording of the bill is ambiguous. It doesn't explicitly force companies to install backdoors in their products, but it does say they should

be able to remove encryption on users' data whenever "practicable." What exactly "practicable" means is never explained. The UK might argue that it's "practicable" for a company to undermine its own encryption; that company might respond that doing so would endanger its business around the world.

Earlier this year, big tech companies including Facebook, Microsoft, and Google lined up to denounce this part of the legislation. Apple CEO Tim Cook was particularly critical, noting that the law would have "dire consequences" if introduced. "If you halt or weaken encryption, the people that you hurt are not the folks that want to do bad things. It's the good people," said Cook in 2015. "The other people know where to go."



Apple CEO Tim Cook says the law could have "dire consequences."

What exactly will happen if the UK government demands that a company like Apple decrypt its data isn't clear. However, it won't be straightforward replay of San Bernardino, when Apple battled the FBI over the decryption of a terrorist's iPhone. The UK has the legal authority to penalize companies that don't comply, but experts aren't sure whether they would bother. "A lot of this is about setting a precedent of how you think things ought to function, rather than necessarily expecting to be able to enforce the laws against overseas companies," says Killock. In many cases, he suggests, the issue will come down to leverage. Tech companies without any UK presence will be able to shrug off demands (what's the government going to do to them?), but big firms like Apple and Facebook, which have thousands of staff in the UK, may feel more at risk. Alternatively, this might give them an advantage against the government; allowing them to threaten to withdraw jobs, for example.

Experts say what is even more dangerous, is the fact that any such battles between tech companies and the UK government will take place in private. Any warrants issued to a company to decrypt users' data will come with a gagging order, forbidding the firm from discussing it. "There wouldn't be any public debate about it," Harmit Kambo, campaigns director at Privacy International, tells *The Verge*. "Apple vs. the FBI just wouldn't happen in the UK." The first we might know of a battle over encryption could be a company simply withdrawing its services from the UK. "The invisibility of it is the biggest trick they've pulled," says Kambo. "It's sad that the Snowden revelations backfired so spectacularly here. Rather than rolling back powers, they've been used to legitimize these practices."

The scope of the law reaches far beyond the UK's borders, and the knock-on effects will likely be felt in countries around the world. Taken as a whole, it's hard to see the Investigatory Powers Bill as anything other than a reshaping of the concept of private civil society.

Update November 29th: The story has been updated to note that the Bill has now received royal assent and is officially law.

Articles by: James Vincent