Proposed snooping law: what you need to know
Michael Dalder

IFEX's guide to the government's plan to introduce more monitoring of people's emails, phone calls and web usage in the U.K. - and what it means for free expression.

Under new U.K. government proposals, the authorities could have the right to monitor what websites you visit - in real time and on demand

What's the plan?

Under new government proposals, the police and security services could soon have the right to monitor the calls, emails, texts and website visits of everyone in the U.K. - in real time and on demand, and entirely unfettered by the courts.

While it would not allow the U.K. intelligence agency, Government Communications Headquarters (GCHQ), to access the actual content of emails, calls or messages without a warrant, it would let intelligence officers identify who an individual or group is in contact with - including every friend they've had on Facebook - how often and for how long. They would also be able to see which websites someone had visited.

And all this info could be authorised and obtained by a slew of government agencies, ranging from local councils to environmental regulators.

Basically, Privacy International sums up, "[communications data] represents a list of all your interactions in a modern world… [It] can reveal all your interests, relationships and habits. Google and other Internet companies reliant on targeted advertising can only dream of having access to this amount of data."

Why are they doing this?

The Home Office says the bill would let the authorities combat "serious crime and terrorism" and "protect the public."

Plus, in the era of Google, Facebook and Twitter, it is now more difficult to monitor who's

talking to whom. In a statement, the Home Office said action was needed to "maintain the continued availability of communications data as technology changes."

When will we find out the details?

Initially, the proposed legislation was going to be featured in the Queen's Speech on 9 May. But a backlash by civil rights groups and, notably, Liberal Democrat MPs who are part of the coalition government, has led to a much-welcome pause for thorough examination of the data surveillance proposals.

Deputy Prime Minister Nick Clegg is now promising open parliamentary hearings about the measures. The draft clauses of the new bill will be published in early May, he says, and will be scrutinised by the Commons Home Affairs Select Committee in public.

How would it work?

Internet service providers, phone operators, website hosting companies and even the likes of Google and Facebook would have to install data-collecting equipment that would allow the GCHQ real-time, on-demand access to any person's communication records and browsing history, says Reporters Without Borders (RSF).

The move raises major legal, technical and financial questions, says RSF, like: who will be responsible for managing the data gathered by the surveillance system? How long would data be kept? Who would pay for it? How will it be stored securely? Details of the plan have yet to be revealed.

What do critics say?

The proposal has encountered widespread criticism from civil liberties groups in the U.K. that say it is a gross invasion of privacy. IFEX members too, have joined the outcry.

Privacy International says the system being proposed is the kind "favoured by al-Assad, Mubarak and Gaddafi" and "has no place in a country that would call itself free and democratic."

Privacy adds that if the plan goes ahead, "There's basically no limit on future actions… The government will have enormous scope to monitor and control the Internet," from tracking file-sharing to restricting access to services.

Plus, once the information is collected, "it can never be 100 percent secure and is always vulnerable to exposure by human error or corruption," says Privacy.

RSF also worries about the system being open for misuse. "By placing all of its citizens under surveillance, it would have the effect of encouraging its targets to use easily accessible anonymisation methods," says RSF. "And its implementation without reference to the courts could open the way to all kinds of abuses."

Internet advocacy expert Danny O'Brien of the Committee to Protect Journalists (CPJ) observes that "state surveillance has a long history of being misused against reporters," as evidenced by Colombia's phone-tapping scandal, and last year's case of a "Le Monde" reporter whose phone records were obtained by French intelligence services in violation of press freedom laws.

O'Brien also warns that communications data nowadays "can reveal far more about you than simply an address on an envelope." For instance, the address of a webpage could include some of the content on the page, just as searches in Google are reflected in web addresses it returns, he notes.

Index on Censorship's Padraig Reidy says the move "severely undermines [the U.K.'s] power

to criticise states that would use the same legislation to watch activists and dissidents… Have no doubt, this is a bad idea and Index will campaign against it should it go any further."

Even the UN has expressed reservations about this kind of surveillance. In a June 2011 report, UN special rapporteur for free expression Frank La Rue voiced alarm at the tendency of some governments to monitor the activities of Internet users without providing sufficient guarantees against abuses and without data protection laws. He also stressed that the right to privacy should only be curtailed in "exceptional circumstances" and never systematically.

Isn't this déjà-vu?

The previous Labour government tried to introduce a similar system using a central database tracking all phone, text, email and Internet use in 2009. But that was dropped because of an outcry from civil society - including the opposition parties, who are in power now.

Isabella Sankey, director of policy at the campaign group Liberty, says, "The coalition agreement explicitly promised to 'end unnecessary data retention' and restore our civil liberties. At the very least we need less secret briefing and more public consultation if this promise is to be abandoned."

I'm not from the U.K. Why should I care?

Any proposed changes to how surveillance is regulated "need to be closely examined for how they could affect press freedom worldwide," O'Brien cautions.

If the British government is permitted to obtain access to international companies like Facebook and Skype, "what would prevent other governments from demanding, and getting, the same access?" asks O'Brien.

Sadly, the U.K. is not the only democracy to have communications surveillance plans in the works. "We are shocked to hear more and more supposedly democratic countries such as India, France, Australia and now the United Kingdom expressing a desire to adopt the kind of systematic monitoring of communications used by the planet's most repressive regimes," says RSF.

RSF argues that Australia's crackdown on child porn sites would lead to innocent websites being unfairly blocked. Meanwhile, France is aspiring to make visiting websites that advocate terrorism or violence a crime.

And newsmagazine "India Today" just announced that BlackBerry maker Research In Motion has given into the Indian government, granting security forces in that country access to private instant messages.

Then there's the U.S. The Internet has been abuzz about a new bill in Congress called CISPA, or the Cyber Intelligence Sharing and Protection Act of 2011. According to RSF, it would allow the government and private companies to deploy draconian measures to monitor, even censor, the web in the name of the war on cybercrime. It might even be used to close down sites that publish classified files or information, such as WikiLeaks or "The New York Times".

Ultimately, though, Privacy International says, to date, no democratic country has pursued as sweeping a policy as the U.K. "The U.K. will find itself aligned with China and Iran if this proposal goes ahead," it warns.

Fonte: IFEX, 11 Apr. 2012. [Portal]. Disponível em: <http://www.ifex.org>. Acesso em: 13 Apr. 2012.