

**Invest in experts. Donate now and help share their message
with a global audience.**

Donate now

THE CONVERSATION

Academic rigour, journalistic flair

Proposed powers in surveillance bill will dictate the shape of society to come

November 2, 2015 3.41pm GMT

asharkyu

Proposed powers in surveillance bill will dictate the shape of society to come

November 2, 2015 3.41pm GMT

If the feverish discussion in the press and the sudden appearance of spokesmen from the secret services and police are anything to go by, it seems that the UK government's Investigatory Powers bill, announced in the 2015 Queens Speech, is due to appear soon.

Of course, Britain has been here before.

Under the previous Conservative-Liberal Democrat coalition government, the Tories tried to enact the **Communications Data bill** – the so-called “snoopers charter” – only for it to be vetoed by the Lib Dems on the grounds that the mass surveillance powers it contained were disproportionate. In fact several subsequent attempts to pass the bill or elements of it were **tried and failed**.

What's different this time around is that the Conservative government is unshackled by coalition partners and has a Commons majority, albeit a slim one. In theory the government should be able to force through the legislation, but in practice – as the recent debacle over reform of tax credits has shown – much of the government's current legislative programme has been delayed, amended and rejected by the House of Lords.

Nor is there universal support for mass electronic state surveillance of UK citizens within the Conservative Party, with **high profile dissenting voices** including former Tory leadership candidate

<https://theconversation.com/proposed-powers-in-surveillance-bill-will-dictate-the-shape-of-society-to-come-49972>

Author



William Webster

Professor and Director, Centre for Research into Information, Surveillance and Privacy, University of Stirling

David Davies MP. The legislation proposed for the current parliamentary cycle is bound to be controversial. Mass surveillance strikes at the very heart of a modern digital society – expect a bumpy ride.

More than one way to squeeze a lemon

In an effort to ensure the bill's safe passage through parliament, the process is being closely managed this time. First, it has been reshaped so that electronic mass surveillance, its most concerning aspect, is no longer the focus as it was in its previous incarnation as the Communications Data bill. Instead the focus is “investigatory powers”, with the emphasis on the police, public safety, and the fight against terror.

This is a subtle but significant shift – who doesn't want to be safe and secure? Cynics argue that this is a diversion intended to head off public debate about the need for mass surveillance, with national security typically trumping an individual's right to privacy. This is the same approach which led to Britain having the most CCTV cameras per capita than anywhere else in the world.

Second, the government has mobilised the professional surveillance lobby, with a procession of spooks and police chiefs stepping in to support the government by framing the discussion in the run up to the bill's arrival. Notably Andrew Parker, director general of MI5, spoke about the need for a “modern MI5” – an unusual move for a usually secretive agency. That this has happened now is no coincidence. This is a preemptive strike by the bill's supporters, highlighting the public's loss of trust in the intelligence services following the Snowden revelations into the extent of government surveillance, and the need for these services to justify their actions.

Battle lines are drawn

Although the bill has yet to be published its core elements have been well trailed as legislation that “will modernise the law on communications data”, with the core purpose of addressing “ongoing capability gaps that are severely degrading the ability of law enforcement and intelligence agencies ability to combat terrorism and other serious crime”. At the same time we are promised “appropriate oversight and safeguard arrangements”. The devil will be in the detail, of course.

Targeted electronic surveillance of suspects and criminals has universal public support, and there is no question that intelligence services and law enforcement agencies should have access to the latest technologies to ensure this is available to them. But appropriate safeguards should be in place for all public services, not just for the most potentially invasive security agencies. Again this would have widespread political and public support. The sticking point is likely to be the “known unknowns” – that in practice the legislation could provide the basis for indiscriminate electronic mass surveillance, as opposed to targeted surveillance, and that arrangements for oversight and redress will prove unsatisfactory.

A seismic shift



When your thoughts, plans and opinions are stored digitally they can be found. VLADGRIN

It cannot be overemphasised that the implications for society of such legislation are immense. Routinely collecting communications and internet use data, and automatically profiling citizens based on their behaviour as assessed and predicted could become an automated process irrespective of whether an individual warrants this level of intrusive inspection.

This offers the potential to move away from skilled, informed, targeted surveillance towards the “fishing expeditions” of mass surveillance where everyone is a potential suspect. More, it represents a shift in the relationship between the citizen and the state, to a situation where individuals should have no expectation of electronic privacy nor control over their personal data.

The proposed Investigatory Powers bill is likely to lead to a wide range of hotly contested surveillance powers, powers that without proper and open debate will lead to levels of surveillance in our society that will not be acceptable to the majority and will be open to misuse.

Let battle commence.



[Online privacy](#) [Surveillance](#) [Digital privacy](#) [Mass surveillance](#)