Expanding state power in times of 'surveillance realism': how the UK got a 'world-leading' surveillance law

Arne Hintz and Lina Dencik 23 December 2016

A fragmented opposition, public resignation in the face of omnipresent data collection, and a dominant security discourse has created a social context for the Investigatory Powers Act to be passed largely unhindered.

Yui Mok/PA Archive/PA Images. All rights reserved.With the fallout of the Brexit referendum and the Trump election dominating the news, one important story of 2016 did not receive the attention it deserved: in late November, the British parliament adopted a law with an obscure name but far-reaching implications for citizens in the UK and, potentially, beyond. The 'Investigatory Powers Act' is a comprehensive legislative framework that regulates the surveillance powers of intelligence agencies and other public authorities.

While the government has maintained that the new law is "world-leading", critics have pointed out that it allows for some of the most extensive and intrusive surveillance practices in the world, and have asked: "What part of the world are we leading exactly: North Korea, Cuba, China and Saudi Arabia?"

The development of what was initially the Investigatory Powers (IP) Bill took over a year, was preceded by several other attempts to create what has been called a "Snooper's charter", and was accompanied by strong opposition from civil society, industry and several parliamentary commissions. Yet it survived all this largely unchanged and eventually became law "with barely a whimper" and a largely muted response from the British public. How did this happen?

As part of an ESRC-funded research project at Cardiff University, we explored the dynamics that led to the adoption of the Bill. The research included interviews with politicians as well as representatives of industry,

security agencies, and campaign groups during the development phase of the Bill, as well as focus groups with the British public and a content analysis of media coverage.

The Bill was an outcome of contradictory developments. On the one hand, the Snowden revelations triggered widespread public criticism, court cases against the British government, and official reviews such as the Anderson Report. All these demanded significant revisions to British surveillance practices and policies. On the other hand, the Conservative majority in the coalition government of 2010-15 had advanced plans for a Communications Data Bill – nicknamed the "Snooper's charter" – that would expand surveillance capabilities. Those were halted by the junior party in the coalition, the Liberal Democrats, but re-emerged after the Tory election victory in 2015.

This time around, there was neither a coalition partner, nor any viable parliamentary opposition, to moderate the Tory plans. The lack of detailed technical knowledge by most parliamentarians did not help, nor did – as we were told in our interviews – a traditional "deference to the agencies". As a result, both the Commons and the Lords were ineffective in serving as spaces of governmental control.

This role was occupied in part by civil society. Digital rights and civil liberties organisations were vocal throughout the process and were increasingly recognized as a legitimate actor with relevant expertise. Involvement in some of the more detailed debates on policy reform allowed them to engage with the process and develop specific proposals for improving the Bill. However this also meant that fundamental opposition to surveillance was less pronounced, as was public awareness-raising and protest. And while a number of organisations worked hard on developing detailed and thorough contributions throughout the policy process, most of them were eventually ignored by government.

The technology business sector served as another voice of strong criticism against an expansion of surveillance capabilities, and this was underlined by high-profile cases such as the conflict between Apple and the FBI as the Bill was being developed. In part, the more dissident position of internet businesses was a strategic effort by industry to re-gain consumer trust, but it led to a further source of opposition. Business largely joined the overwhelming majority of technology experts and other policy stakeholders who were critical of the Bill or rejected it outright.

An avalanche of written submissions at every stage of the process questioned the feasibility, costs, legality, intrusiveness, and democratic nature of the Bill, as well as its implications for basic human rights. Yet this opposition had little effect on the successive drafts of the Bill. Even recommendations by the Intelligence and Security Committee of Parliament to make privacy protection "the backbone of the draft legislation" merely led to minor cosmetic changes.

In this conflict between government and a (mostly non-parliamentary) opposition, which side did public opinion support? Neither one, it turns out. To understand public perceptions of surveillance, it is important to look at how people receive the majority of their information about the subject. And while a small portion of the public will consult specialist online publications, the main information sources remain traditional media (or rather, their stories which are shared across a variety of platforms).

However media coverage was limited, and reporting on surveillance typically legitimized, rather than questioned, state surveillance practices. Our research found that newspapers such as *The Mirror* and *The Times* quoted views in favour of increased surveillance twice as often as the opposing viewpoint. Foreign politicians and terrorists were highlighted as the prime targets of surveillance, while data collection of the general public received less attention. Partly, this was due to the predominance of political sources – with politicians and their spokespersons appearing the most frequently, at 40.8% of all sources.

Our research found that newspapers such as *The Mirror* and *The Times* quoted views in favour of increased surveillance twice as often as the opposing viewpoint.

Dominant opinions from the political establishment in the reporting of revelations of mass surveillance therefore firmly situated these practices as a necessary part of maintaining state security as the primary objective. The implications for citizens' rights and their interests in secure and unimpeded communication remained mute, in comparison. Reporting on the IP Bill followed this pattern and very little of it scrutinized its effects on citizens. The bill was processed without much public awareness.

Our research with the general British public, which included 10 focus groups with 3-8 people in each group, emphasizing ethnic, socio-economic, age, and geographic diversity, demonstrated how this limited discussion has translated into muted and confused attitudes to state surveillance practices. We found that members of the public do have concerns about the monitoring of online communication but opinions are marred by a lack of knowledge about how exactly it works, for what purpose it is conducted, and how we can protect our privacy. Whilst there is prominent unease with ubiquitous data collection and a concern with how data is used, there is also a sense that this has become a contemporary inevitability and part of everyday life.

The sheer ubiquity of surveillance infrastructures and their embeddedness in ordinary aspects of social, political and cultural participation make it difficult to think they can be challenged. The consequence of this is a widespread resignation (rather than consent) to the status quo, exemplified in part by internalised justifications such as the much-used mantra of 'if you have nothing to hide, you have nothing to fear.' We refer to this condition as surveillance realism in which the active normalisation of surveillance infrastructures limits the possibilities of imagining another way of organising society, despite widespread unease with the current system.

Opposition against the bill failed to transform this context of surveillance realism. Digital rights campaigners were busy with advocacy efforts and reform debates at the governmental level and had fewer time, energy and resources to spend on public education and awareness. Civil society groups dealing with issues other than digital rights focused on their core remits and were not engaged with debates around surveillance and the IP Bill. Our interviews with environmental, anti-war, labour, community, and economic justice activists pointed to a 'disconnect' in this regard, between technology activists on the one hand, and social justice activists on the other.

When debates on resisting surveillance did reach a broader public, they often came in the shape of technological solutions to protect individual privacy. While encryption and anonymization tools have been important means of secure and responsible online communication, the broader debate on what social justice means in the era of datafication and digital citizenship has remained underdeveloped. As a starting-point for this necessary discussion, we have proposed the concept of "data justice" as a way to also broaden the parameters for understanding and debating surveillance beyond technological solutionism and a focus on individual privacy. Data justice is intended to guide a framework of debate that engages with the politics of data and the intricate relationship between mass data collection and substantive social justice claims.

A fragmented opposition, public resignation in the face of omnipresent surveillance, and a dominant security discourse that has prioritized a narrow set of national security concerns over a wider range of human security issues, have all contributed to a social context in which the agenda of security services and certain parts of governments could now be implemented in a largely unhindered way.

Security and intelligence agencies were involved in policy reform discussions early on and enjoyed the closest access to decision-makers. The Home Office (which is responsible for domestic security) was at the centre of the policy reform process, while interests that may have offered a counterbalance were based at other government departments. A combination of specific interests, political and institutional settings, and public discourses enabled the government to sideline significant expert opposition and push through the planned Bill.

Just before the IP Bill was adopted, the Investigatory Powers Tribunal (IPT) ruled that intelligence agencies had been unlawfully collecting personal data for 17 years. This was the latest in a series of court rulings which had criticised British surveillance policy. It demonstrated once more that the government had two options for how to respond to the post-Snowden critique: review and reduce surveillance powers, or legalise and expand them. With the new Investigatory Powers Act, it chose the latter.

But court challenges against the British surveillance regime are unlikely to subside with the adoption of the new law. Civil liberties and digital rights groups have criticised the IP Act as "more suited to a dictatorship than a democracy" and have declared they believe it is incompatible with human rights law. The legal route has already proved successful in forcing the government to revise surveillance policy in the immediate aftermath of the Snowden revelations. One of the main messages from civil society organisations after the adoption of the new Act was: see you in court.

Full research findings will be available on www.dcssproject.net soon.

About the authors

Dr Arne Hintz is Senior Lecturer at the School of Journalism, Media and Cultural Studies at Cardiff University and was Principal Investigator on the project "Digital Citizenship and Surveillance Society: UK State-Media-Citizen relations after the Snowden leaks". Follow on Twitter: @arne_hz.

Dr Lina Dencik is Senior Lecturer at the School of Journalism, Media and Cultural Studies at Cardiff University and was Co-Investigator on the project "Digital Citizenship and Surveillance Society: UK State-Media-Citizen relations after the Snowden leaks". Follow on Twitter: @LinaDencik.

Related Articles
Waking up to the UK's Investigatory Powers Act
Phoebe Braithwaite
The UK's Investigatory Powers Bill is about to become law – here's why that should terrify us
Julian Huppert
The Court of Justice of the European Union has ruled against the UK government, but will they listen?
Nik Williams
Related Articles
Waking up to the UK's Investigatory Powers Act

Phoebe Braithwaite

The UK's Investigatory Powers Bill is about to become law – here's why that should terrify us

Julian Huppert

The Court of Justice of the European Union has ruled against the UK government, but will they listen?

Nik Williams

Interview: William Binney, ex-NSA

Setting the critical agenda