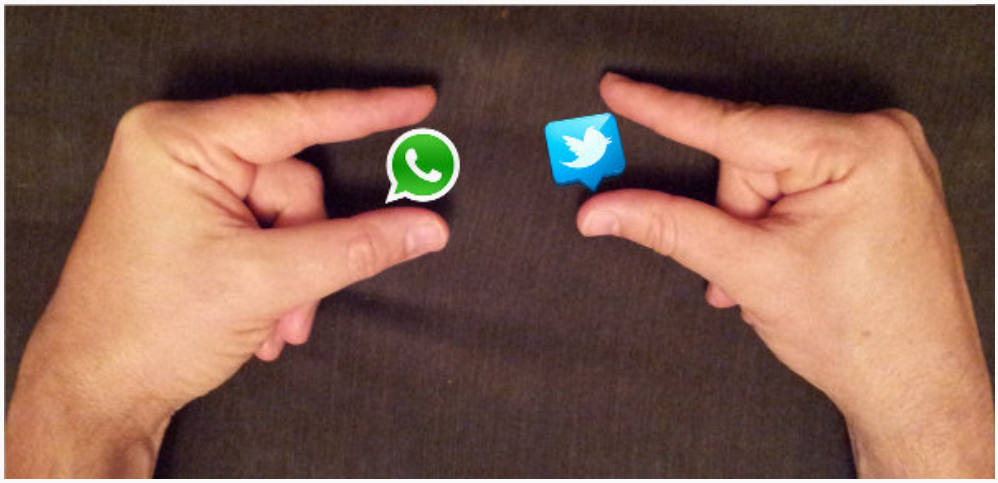
Time for the media shadow boxing to end, and for the democratic deficit in the expansion of the UK's surveillance powers to be tackled

democraticaudit.com /2015/07/16/time-for-the-media-shadow-boxing-to-end-and-for-the-democratic-deficit-in-the-expansion-of-the-uks-surveillance-pwoers-to-be-tackled/

By Democratic Audit UK 2015-7-16

Since the Snowden revelations, the extent of the UK's surveillance powers has come into sharp focus. This has been justified by the government and the security agencies themselves as being the necessary cost of freedom in an age of grave uncertainty and risk. Andrew Murray argues that the media 'shadow boxing' that has gone on about the latest proposed increase in security powers must come to an end, and that we now have an opportunity to tackle the yawning democratic deficit.



Criminal Activity (Credit: Thahi Levent-Levi, CC BY 2.0)

The topical debate over the scope and extent of the yet to be published Investigatory Powers Bill is a textbook example of the modern form of shadow political debate formulated in the echo chamber of news and social media, rather than in the debating chamber. The current public discourse on mass surveillance capability and the wider role of the security and intelligence services is almost laughably lacking in solid contextualisation. At least it would be a laughing matter were it not so deadly serious and were it not also in danger of becoming the textbook example of democratic deficit.

The starting point of this debate does much further back than most people realise. At its heart are three pieces of legislation and a court case. The first piece of legislation was the Computer Misuse Act 1990. It was passed to ensure that new forms of criminal activity involving computers were properly policed. Its ostensible targets were computer hacking and the creation of viruses. It had a small exception to the hacking provision in s.10 for law enforcement organisations. It allowed, "a constable or other person charged with the duty of investigating offences" to gain access to a computer without the permission of the owner. We all knew what that was for; it was to ensure that someone arrested for say possession of child abuse images would not escape prosecution because police forensic officers would be committing an offence in accessing his computer without his permission (which one would assume would be refused).

The second was the Regulation of Investigatory Powers Act 2000. Again we thought we knew what this was all about. This was an attempt to formalise and regulate interception powers in the emergent digital society. It required ISPs and others to maintain an interception capability and it created a regime for lawful interception. Interception of

communications within the United Kingdom would be carried out only following the issuance of a warrant from the Secretary of State as allowed by s.5 and in accordance with ss.6-11. Communications which were external to the UK were subject to less rigorous safeguards should the Secretary of State issue a s.8(4) certificate, certifying that the warrant did not relate to a domestic communication, and in the event the communication related to a UK resident was subject to further safeguards in s.16. The third piece of legislation was the Data Retention Directive (now invalidated).

Passed in 2006 in the aftermath of the terrorist attacks in Madrid in 2004 and London in 2005 it stands as the archetypal "knee jerk" response to a shadow threat. It required Member States to implement laws requiring telecommunications and information society service providers to retain large amounts of customer metadata for between six months and two years to allow law enforcement authorities access to this data. There was much disquiet at the time about this, yet the law was passed against the backdrop of these two atrocities. Two observations should be made on the policy-making process of the Directive. Firstly, in a tactic which has become standard for the UK Home Office, a deadline was set which cut off democratic debate on the provision, and secondly the UK Government used its position as EU Council President to push through a legislative change which it had been warned was probably unlawful in UK Law by the Parliamentary All Party Internet Group. In the event we know now that not only was this unlawful at UK Law it was also unlawful at the European level. On 8 April 2014, the Court of Justice of the European Union declared the Data Retention Directive invalid. The Court took the view that the Directive failed to meet the principle of proportionality and should have provided more safeguards to protect the fundamental rights to respect for private life and to the protection of personal data.

This is the prehistory of the current debate: life before Snowden if you like. Today the wheel turns again. A number of legislative developments in the last year have re-raised concerns of a democratic deficit. Firstly on 10 July 2014 the then Coalition Government announced the need for emergency legislation to replace the now invalidated Data Retention Directive. The legislation would be debated in Parliament in three days while party political leaders lined up to support an unpublished Bill. A group of 15 legal academics, myself included, signed an open letter to Parliamentarians urging the government not to fast track the Bill but to ensure full and proper parliamentary scrutiny was applied. Of course the Bill was fast-tracked and became law seven days after it was first announced. It was denounced by Parliamentarians and two of them David Davis MP and Tom Watson MP have gone on to Judicially Review the actions of the very Parliament they are members of. In February this year, the Home Office published the draft Equipment Interference Code of Practice.

The draft Code was the first time the intelligence services openly sought specific authorisation to hack computers both within and outside the UK. Hacking is a much more intrusive form of surveillance than any previously authorised by Parliament. The Government, though, sought to authorise its hacking, not through primary legislation and full Parliamentary consideration, but via a Code of Practice. A final amendment to the legal settlement (thus far) may be found in the Serious Crimes Act 2015. Although subject to full Parliamentary scrutiny the relevant section, s.44, was described in the explanatory notes to the Bill as a 'clarifying amendment'. The amendment effectively exempts the police and intelligence services from criminal liability for hacking. This had an immediate impact on the on-going litigation of civil society organisations who were suing the Government based in part on the law amended, s.10 of the Computer Misuse Act 1990.

Knowing the so-called Snooper's Charter was about to be resurrected by the newly elected Conservative Government thirty-nine legal academics, including myself, signed a subsequent open letter calling upon the Government to ensure "Parliamentary scrutiny is applied to all developments in UK surveillance laws and powers as proposed by the current Government". The Snooper's Charter is now called the Investigatory Powers Bill. It was announced in the Queen's Speech. We still do not know what it will contain as it has yet to be published. The debate on the Bill (not yet in existence) is though vibrant. In his report the Independent Reviewer of Terrorism Legislation reported that the capability of the security and intelligence agencies to practise bulk collection of intercepted material and associated data should be retained but used only subject to strict additional safeguards concerning judicial authorisation of warrants, a tighter definition of purposes [for collection], targeting of external communications and

the need for judicially authorised warrants within the UK.

In reply the Prime Minister indicated that government would resist calls for judicial warrants. Just last week reports emerged in the media that popular apps such as Snapchat, WhatsApp and Facebook messenger could be banned "within weeks" under the Bill (which remember no one has seen) as they allow for end-to-end encryption of messages. These reports all mention the Prime Minister's statement made after the Charlie Hebdo attacks:

> *"In our country, do we want to allow a means of communication between people which we cannot read? My answer to that question is: 'No, we must not'"*

However, they fail to give details of where the possible ban comes from, except to discuss the assumed general terms of the Bill (from Home Office briefings) which suggest systems which do not allow the UK government access to sessional data will be banned. Again there is much debate, but still a clear Parliamentary democratic deficit. We are all discussing something not yet in existence.

Earlier this week, the latest piece of the jigsaw arrived. The RUSI report A Democratic License to Operate commissioned in 2013 by the then Deputy Prime Minister was published. Currently we debate the implications of this report and determine how it fits into the jigsaw. Privacy campaigners are claiming it supports their position. They cite the report's finding that "Privacy is an essential prerequisite to the exercise of individual freedom, and its erosion weakens the constitutional foundations on which democracy and good governance have traditionally been based in this country" and record that it also recommends the introduction of judicial warrants as proposed by the Independent Reviewer of Terrorism. Others highlight that the report records that police and intelligence agencies face a significant challenge from encryption in monitoring individuals who pose a risk to collective security while proposing what seems to be an impossible balance: police and intelligence agencies should not have blanket access to all encrypted data, but material should not be beyond the reach of law enforcement.

All this debate is merely the *hors d'oeuvres* for the main course to come, the publication and (hopefully) consultation and debate on the Regulatory Powers Bill. I am pleased to say that in his response to the drafters of the open letter on surveillance powers the Minister of State for Security has pledged that "new legislation will be published for pre-legislative scrutiny later this year and we do intend this to be a very consultative process, subject to full parliamentary scrutiny". This is to be welcomed. There has been for too long an overwhelming democratic deficit in the scrutiny and review of UK surveillance powers: at times to make sense of them has felt like trying to do a jigsaw in the dark and with some of the pieces hidden from us. We will hold the Minister to his pledge. It is time for a full parliamentary review of the law and time for the shadow boxing in the media to end.

—

This post represents the views of the author only, and not those of Democratic Audit UK, the LSE Public Policy Group, or the LSE. Please read our comments policy before posting.

—

Andrew Murray is Professor of Law at the London School of Economics, a Fellow of the Royal Society of Arts (FRSA) and a member of the Executive Board of Creative Commons UK (CCUK). In Autumn 2014 he was a visiting Professor at the Computer Law Institute, VU Amsterdam, and was in Spring 2015 a visiting Professor at the Paris Institute of Political Science (Sciences Po).