Introduction

The Communications Data Bill, referred to as the 'Snooper’s Charter’, grants extensive powers of surveillance to police and security services. Theresa May originally introduced it in 2012–13 but it was blocked by the Liberal Democrats.

In April 2014 the Court of Justice of the EU struck down previously existing rules brought in in 2009 that placed obligations on UK service providers to retain communications data for 12 months through a blanket regime. The court ruled that these were a violation of our basic rights and set out the parameters of a proportionate data retention regime, tied to the investigation of serious crime.

This led the Government to rush through emergency legislation – the Data Retention and Investigatory Powers Act 2014 (DRIPA) – in the remaining days before recess.

DRIPA ignores the judgement of the Court of Justice by re-legislating for blanket retention of communications data and also granting the Government new powers to reintroduce the Communications Data Bill now that they have a parliamentary majority.

Theresa May has vowed to reintroduce the Communications Data Bill in this parliament.

What is proposed?

The new Communications Data Bill has still not yet been published, however it is understood to contain substantial expansion of current powers. The Bill is expected to include requirements on internet service providers and mobile phone companies to maintain blanket records of each user's internet browsing activity (including social media), email correspondence, voice calls, internet gaming, and mobile phone messaging services and store the records for 12 months. Retention of email and telephone contact data for this time is already required by DRIPA 2014. There are also proposals for the outlawing of encryption software.

The Government has argued that these powers are necessary due to increasing threats of terrorism, both international and domestic, as well as organised crime and child abuse. They argue that criminal groups have developed growing sophistication in using internet and communication activities.

Civil liberties under threat

The Government's proposals have received strong criticism from a variety of organisations including Open Rights Group and Liberty who have worked with cross party opposition (David Davies MP and Tom Watson MP) to take joint legal action to challenge the laws. These groups argue that such surveillance strongly breaches people's right to privacy, personal and political freedoms.

They argue that surveillance should only happen to people suspected of crimes not a blanket approach to every citizen. They also point out that such an approach did not stop atrocities like the attacks on Charlie Hebdo, the Boston marathon or the murder of Lee Rigby despite the perpetrators being known to the authorities.

Most recently David Anderson QC, the independent reviewer of terrorism legislation, condemned snooping laws as “undemocratic, unnecessary and – in the long run – intolerable”. His report did not reject the need for powers but called for a fundamental overhaul of the laws governing state surveillance with a new law that could be understood by the public and parliament. Such a new law must comply with international human rights standards and require prior judicial authorisation and
that covert spying methods should be brought clearly under law. He also questioned the justification for such extensive powers given the limited scale of threat that has in reality emerged.

Alongside other proposed legislation such as abolishing the Human Rights Act, anti-union legislation and reductions to other safeguards, such as judicial review and legal aid these proposals form a very worrying extension of the arbitrary enforcement powers of the state.

New risk from technology

Revelations from US whistle-blower Edward Snowden have shown how extensively state surveillance is taking place, often illegally, with developments in communication technology creating the capacity to carry out surveillance far in excess of the powers of the Stasi:

- **Spying on a global scale**: The USA and other allied countries have developed software that is harvesting, as standard, data from billions of people around the world (known as PRISM). This has been used to spy on world leaders such as Angela Merkel, Dilma Rousseff and Vladimir Putin along with huge numbers of ordinary internet users.

- **Complete data harvesting**: The software brings together data from a range of sources including mobile phones, internet, telephones, social media, bank transactions, travel services, and satellite GPS systems. Crucially the computing capacity and software now allows the data to be simultaneously tracked to produce a near complete picture of an individual’s life in real time.

- **Orwellian nightmare**: Security services have the ability to activate mobile and laptop cameras remotely, track people with wifi and mobile signals and use land-line phones as listening devices even when the receiver is down.

- **UK role**: Snowden reported that the UK's GCHQ has a more extensive surveillance system with far fewer controls or accountability than the NSA. Snowden highlights that the US outsources controversial surveillance activities to the UK to circumvent their own controls.

Can we trust the state?

The long history of spying on trade unionists in the UK suggests that this is a major threat:

- **Blacklisting**: Extensive revelations of blacklisting of trade union activists for the past 30 years by employers with collaboration from the police. Metropolitan police, Special Demonstration Squad (SDS) whistle-blowers have admitted spending years undercover infiltrating political activists including trade unionists.

- **Wapping and the Miners’ strike**: The official biography of the MI5 - The Defence of the Realm (2009) - shows that Margaret Thatcher encouraged MI5 to monitor union leaders' activities and communications during both the miners' strike and the Wapping dispute.

- **Defence of the Realm** also details how the secret service was spying on numerous trade union leaders (e.g. Jack Jones from the T&G) throughout the Cold War and beyond as well as senior Labour politicians such as Harriet Harman and Patricia Hewitt.

- **International**: The UK security services have a vile history of union busting and collaboration with brutal regimes to repress political activism and workers’ rights, e.g. the Egyptian military dictatorship, the Saudi Arabian and Bahrain royal family and Colombia. In many of these countries trade unionists are routinely under threat from imprisonment, torture and murder. UK surveillance sends a green light to other regimes around the world and would potentially place activists in those countries at risk through information shared, including about solidarity efforts here in the UK (e.g the Anti-apartheid movement).