British government prepares further draconian legislation to censor Internet

Steve James
10 October 2017

British Home Secretary Amber Rudd's speech at last week's Conservative Party conference elaborated on the government's proposal for a Commission on Countering Extremism, announced in the aftermath of the Manchester Arena bombing in May.

The measures being put together to expose "extremism and division" amount to a fundamental attack on democratic rights, free speech and privacy.

Rudd described "extremism" in sweeping terms, underscoring that the government is seizing on recent attacks as the pretext for all-embracing Internet censorship and the criminalisation of free speech. Besides "warped Islamist ideologies," Rudd insisted, "violent and non-violent extremism in all its forms—anti-Semitism, neo-Nazism, Islamophobia, intolerance of women's rights—these, and others, cannot be permitted to fester."

Rudd and her government's view of extremism could be extended *ad infinitum* to all forms of political dissent and criticism . "The safer Britain I want to build is a united one," she said.

The home secretary asserted that recent attacks "include an element of online radicalisation." She complained that "extremist and terrorist material can still be published online, and is then too easily accessible on some devices within seconds."

Following last month's bombing at Parsons Green Underground station in London, calls for further Internet censorship were being made before the bomber's identity had even been established.

Contrary to Rudd's assertions, the main and only proven common element between the recent terroristic attacks on innocent concertgoers and tube travellers is that the perpetrators have been known to the police and security forces for an extended period.

Nevertheless, the government intends to change the law "so that people who repeatedly view content deemed terroristic online could face up to 15 years in prison."

Currently, material falling foul of section 58 of the Terrorism Act 2000 has to be saved locally to a computer drive or printed to be deemed criminal. In future, if the government gets its way, the mere act of repeatedly viewing a video stream of a site deemed extremist without "reasonable excuse" could be enough to merit a jail sentence. According to the Home Office, "reasonable excuse" will be restricted to academics, journalists and others who may have what the Home Office view as a legitimate reason.

Rudd also harangued the giants of social media, Facebook, Google, Twitter and Microsoft, with whom she is already collaborating closely, to "bring forward technology solutions to rid your platforms of this vile terrorist material." "Act now," Rudd went on. "Honour your moral obligations."

Under the guise of clamping down on images of child abuse, Rudd made clear that she wanted widespread deployment of crawler technology, described as Project Arachnid, to rapidly identify offensive images and automate their instant removal. "Our investment," Rudd continued, "will also enable internet companies to proactively search for, and destroy, illegal images in their systems."

A technology that can identify images of child abuse can target images of anything else and, in the hands of the Home Office and the Web giants, would be used to suppress alternative opinions, and consolidate the immense worldwide program of Web censorship already being developed.

Rudd used the same hysterical technique to propagandise for the government's attack on encryption, the basis of most secure data transmission on the Internet. "We also know that end to end encryption services like Whatsapp, are being used by paedophiles. … I do not accept it is right to allow them and other criminals to operate beyond the reach of law enforcement."

According to this logic, all means of communication and transport, not to mention public utilities, should be suppressed because paedophiles and other criminals use them.

Under powers contained in the Investigatory Powers Act, which came into force last year, Rudd can already issue a technical capability notice (TCN) to demand companies undermine the security of their own technology. Any organisation with over 10,000 users in the UK can be instructed to alter their product to allow interception of communications and metadata collection.

In practice, the government confronts major problems in pushing through its attack on encryption because so much of modern finance and industry depends on it. Moreover, by the nature of encryption, which involves the exchange of keys generated at each end of a communication session, and which are then used to encrypt traffic during that session, the very notion of a "back door" is fraudulent.

Encryption either works, or it has been broken. Once an exploit exists, it is only a matter of time before its use becomes widespread, with potentially catastrophic consequences, as was shown with the Wannacrypt ransomware outbreak earlier this year, which brought much of the National Health Service to a standstill but was based on the Eternal Blue exploit developed by the US government's National Security Agency (NSA).

Rudd has been repeatedly advised, including by industrial and technical commentators by no means otherwise hostile to her government's agenda, where this might lead. Speaking in the House of Lords last month, Baroness Martha Lane Fox, founder of LastMinute.com, criticised earlier comments from Rudd banging the drum against encryption. Fox described Rudd's approach as "asinine" and "alarmist and a disservice to the people we serve."

None of this bothers Rudd, however, who is one of the candidates to replace Theresa May when her premiership finally disintegrates. Rudd declared that she doesn't "need to understand how encryption works to understand how it's helping the criminals."

More than mere ignorance is on ostentatious show here. Nor should one rely on a scenario where the "voice of sanity" within ruling circles somehow acts as a counter to the sharp turn to state repression. For Rudd, the target is neither potential terrorists nor sex criminals but the entire working population at a time of acute and growing social and political tensions.

Rudd's initial focus is on clamping down on opposition to British imperialism's predatory wars in the Middle East, but this will inevitably be extended to cover all anti-war sentiment and commentary at a time when Britain and its major ally, US imperialism, are threatening North Korea with military intervention as part of a general patter of threats and aggression against Both China and Russia.

The same concerns inform proposals for a new Espionage Act to replace the Official Secrets Acts of 1911, 1929 and 1939. Still at the level of proposals with the Law Commission, the statutory body that reviews and updates legislation in line with government demands, the Espionage Act proposals, "Protection of Official Data: A Consultation Paper," include measures that would, according to the British-based Open Rights Group (ORG):

- Make persons who are not British subjects or citizens, and who have never been on British territory, potentially chargeable and subject to extradition;
- Eliminate the requirement to prove that any alleged release of information actually caused damage;
- Prohibit a defence of prior disclosure unless information was already "lawfully in the public domain";
- Include economic information as a punishable disclosure;
- Prohibit any form of public interest defence.

The ORG noted that the proposals are in part a reaction to the efforts by Julian Assange, WikiLeaks, and former NSA agent turned whistle-blower Edward Snowden to expose imperialist war crimes and secret electronic surveillance of the population, although neither Assange nor Snowden is mentioned in the Law Commission documents.

In 2013, Snowden exposed the extent of Internet surveillance organised by the British and US intelligence agencies. WikiLeaks continues to reveal numerous vast data troves exposing the machinations of the rich and powerful to the world's working population, despite Assange's incarceration in the Ecuadorean Embassy in London. Seeking to guard against future such exposures, the Law Commission insists it is "necessary to ensure sensitive information is safeguarded against those whose goal is to obtain it contrary to the national interest."