'Proposed US and UK Laws Will Entrench Surveillance Powers Across the Atlantic'

The Conversation

Eliza Watt

Important changes relating to surveillance powers are afoot on both sides of the Atlantic. A new Investigatory Powers Bill (IPB) was introduced to the UK Parliament by the Home Secretary, Theresa May, on 4 November 2015, whilst the US Senate Intelligence Committee has already voted in favour of Cybesecurity Information Sharing Act (CISA). Both of these new pieces of legislation follow in the footsteps of Edward Snowden 2013 revelations relating to the National Security Agency (NSA) and Government Telecommunications Headquarters (GCHQ) interception and collection of telephone and digital communications en mass and, we are told, are an attempt to address the significant privacy and security concerns. The US and the UK governments advocate that these new measures represent much needed surveillance powers reform. But what do they really allow for? What safeguards do they create and most importantly, how do they relate to the obligations of privacy protection under Article 8 of the European Convention on Human Rights and Article 17 the International Covenant of Civil and Political Rights (ICCPR) of the countries concerned?

CISA's aim is to enable companies and federal agencies to coordinate responses to cyber attacks. To that end, the Act grants new, sweeping powers to private enterprises. First, it allows them to voluntarily share 'cybersecurity threat data', including personal information about individuals, with the Department of Homeland Security (DHS), who could then pass it on in real time to other agencies, such as the NSA and the Federal Bureau of Investigation (FBI). Secondly, it authorises companies to deploy 'defensive measures' for 'cybersecurity purposes' and allows them to monitor information systems to protect their hardware and software. Critics agree that the CISA dresses new government surveillance mechanisms in a cloak of security protection. Their unease and concern centres around both what the Act allows for and what it does not address. As far as sharing cybersecurity data is concerned, the CISA authorises passing on information that falls within the rubric of 'cyber threat indicators' 'notwithstanding any other provision of the law', whilst also obliging companies to remove some personal information before sharing it with the government. 'Threat indicators' are broadly defined and therefore allow any information to be construed as such. Consequently, not only does CISA authorise vast amounts of personal data to be shared without adequate privacy protections, but also permits the federal, state and local governments to use the 'indicators' for criminal investigations that may be completely unrelated to cybersecurity and since all other laws are subordinated to CISA, avoid due process protection. The defenders of CISA, such as Richard Burr, the Chairman of the Senate Select Committee, dismisses these worries pointing to the voluntary nature of the information sharing, but disregarding the fact that companies will receive incentives in a form of protection from any liability that may arise as a result of sharing private information directly with the

DHS. Then, there is the problem of vetting data in order to remove personal information before it is shared, which is hard to reconcile with the government's duty under Article 17 ICCPR to ensure in law confidentiality of correspondence. In addition, companies may leave personal and identifying information in the indictors they share, unless they know that the information is not directly related to a threat. According to the letter from 55 civil society organizations of 20 April 2015 to the Senate, 'this allows companies to share virtually all personal and identifying information in indicators by default'. Yet, the Act does not address what it was set out to do, namely it does nothing to prevent intrusion into networks and leaks out of them, therefore does not deliver on the promise that it will help protect personal information from being hacked and stolen. The net result of the CISA is the carte blanche given to the private sector to collect, vet and pass on private data disregarding other laws, including human rights protection and cast a wide surveillance net for the intelligence community and domestic law enforcement, without setting out any remedies, transparency, or independent oversights.

The UK Investigatory Powers Bill, does not seem to be faring any better. Ostensibly, it aims to give the police and security agencies tools to keep us safe. In reality, it requires web and phone companies to store records of the websites visited by every individual for 12 months to allow access and for the first time confirms in writing the continued bulk collection and interception of vast volumes of personal communications, both content and metadata. According to the IPB, interception of the content of communications, such as a telephone call, email or social media messages will be allowed, provided a warrant is obtained from the Secretary of State and signed off by a panel of independent judges with a power of a veto. The judges will review warrants issued by ministers taking into account the criteria of necessity and proportionality. Theresa May referred to these new powers of oversight as a 'double lock' system. However, in circumstances of exceptional urgency the judges will not need to be involved. Metadata, including website browsing history, will be made available without a warrant, which arguably reinforces indiscriminate mass surveillance, as this type of data is in many cases more telling and valuable than content of communications. This provision seems at odds with the Court of Justice of the European Union 2015 decision in *Digital Rights Ireland* where it was unequivocally stated that the requirement placed on internet and telecommunication service providers mandating bulk retention of metadata of all individuals, even those not suspected of having a remote connection to any crime, interfered in particularly serious manner with the right to privacy. In addition, the Investigatory Powers Bill gives explicit powers to both the security agencies and the police to hack into and bug computers and phones. It also obliges companies to assist them to bypass encryption. Mrs May, introducing the new draft Act, stated that it will provide a modern legal framework, having openness, transparency and oversight, whilst giving the intelligence services their licence to operate. Human rights organizations, such as Liberty disagree, calling this new legislative effort 'an astonishing assault on all of our Internet security'.

The conclusion that can be drawn from these new American and British legislative efforts is a convergence in aggressive policy aimed at strengthening powers of surveillance, whilst sacrificing privacy of their citizens. Both countries seem to aim at introducing more intrusive measures, which disregard privacy considerations-the CISA by tramping any other laws, whilst the IPB by expressly authorising bulk collection and retention of all data with very little meaningful independent oversights. Bearing in mind that the 2014 United Nations General

Assembly Resolution, *The Right to Privacy in Digital Age*, identified an urgent need to bring the already existing legal frameworks in line with the human rights treaties, it is hard to see that the CISA and IPB is even a 'nod in the right direction'. Rather, it seems 'business as usual' for the likes of NSA and GCHQ. Will the other three members of the Five Eyes follow suit?