# Looking through a legal PRISM at UK and US intelligence agency surveillance

blogs.lse.ac.uk/politicsandpolicy/looking-through-a-legal-prism-at-uk-and-us-intelligence-agency-surveillance/

6/13/2013

*The uncovering of the PRISM programme has concerned many that the UK authorities are circumventing the legal framework and gathering data on its own citizens via US surveillance agencies.* **Orla Lynskey** *describes the statutory controls that exist regarding data sharing with the US and explores whether they are adequate to protect UK citizens' privacy. She concludes that there are little safeguards and redress opportunities for non-US persons, and that EU Data Protection regulation is, at present, toothless once international data transfers have been made. On the bright side, the revelation has brought the issue of government surveillance to the fore.*

Following the revelation that US intelligence agencies are engaged in widespread surveillance of internet communications using the so-called 'PRISM' programme, President Obama's guarantees that PRISM 'does not apply to US citizens and it does not apply to people living in the US' is unlikely to reassure many on this side of the Atlantic.

PRISM gives the US National Security Agency (NSA) access to both communications content and traffic data held on servers of global internet communications heavyweights such as Google, Facebook and Apple. The PRISM revelation quickly led to the concern that the UK's Government Communications Head Quarters (GCHQ) was gathering data on UK citizens via PRISM thereby circumventing the protection offered by the UK legal framework. William Hague, appearing before the Commons, was quick to refute this claim describing it as 'baseless'. While refusing to comment on the details of PRISM, he expressly stated that any data obtained by the UK from the US involving UK nationals is subject to 'proper UK statutory controls and safeguards'. This begs the question: What are these statutory controls and are they adequate to protect UK residents from US surveillance?


The main statutory instrument governing data gathering and surveillance in the UK is the controversial Regulation of Investigatory Powers Act (RIPA) 2000. RIPA provides a legal basis for, amongst other things, the interception of communications in the UK and the acquisition and disclosure of communications traffic data. RIPA sets out a list of individuals and public bodies, including the Director of GCHQ, which can apply for both. It also sets out the conditions under which communications can be intercepted and communications data acquired. The interception of communications, which involves access to communications content, is more strictly regulated than the acquisition/disclosure of communications traffic data: communications can be intercepted for a more limited range of purposes and such interception can, in general, only be authorised by the Secretary of State.

These stricter requirements are needed to ensure compliance with the right to privacy in Article 8 ECHR. Interception of communications by government constitutes an interference with the right to privacy set out in Article 8(1) ECHR. However, this interference can be justified under Article 8(2) ECHR provided that it is in accordance with the law, necessary in a democratic society and proportionate. RIPA provides the necessary legal basis for interception to be deemed 'in accordance with the law'. Interception is considered 'necessary in a democratic society' provided it pursues one of the purposes set out in section 5(3) of RIPA. To be deemed proportionate, this interception should not go beyond what is necessary to achieve its stated purpose. RIPA puts in place a number of

safeguards to help ensure proportionality: for instance, warrants can only be issued by the Secretary of State; warrants are valid for a limited time period and the disclosure, copying and retention of intercept data should be kept to the minimum necessary. Compliance with these safeguards is overseen by an Interception of Communications Commissioner as well as an Investigatory Powers Tribunal. Therefore, on paper at least, the UK communications interception regime is Article 8 ECHR compliant. However, only a negligible number of cases are given judicial consideration. Furthermore, between 2000 and 2009 of the 956 complaints before the Tribunal only 4 were upheld. These figures have raised concerns regarding the practical effects of these legislative safeguards and the robustness of the oversight mechanisms in practice. Moreover, it should be emphasised that the safeguards in place for acquiring and disseminating traffic data are much lower thus giving rise to countless allegations of abuse since RIPA came into force.

However, the real crux of the problem lies elsewhere. While RIPA, in theory at least, provides UK residents with protection against surveillance conducted by UK agencies, it does nothing to protect UK residents against US surveillance under the Foreign Intelligence Surveillance Act (FISA). This Act allows the US to target 'persons reasonably believed to be located outside the United States to acquire foreign intelligence information'. All electronic communications companies conducting 'continuous and systematic business' in the US are subject to this Act. Therefore, traffic and content data relating to UK residents stored on the servers of companies such as Facebook and Google may be provided to US government agencies, such as the NSA, as a result of this legislation. The power to authorise this data collection rests jointly with the US Attorney General and the Director of National Intelligence and is subject to prior approval by the Foreign Intelligence Surveillance Court (FISC). What is notable about this legislation is that it provides no legal safeguards for non-US persons. The limitations and 'minimization' procedures it provides for seek only to ensure that data collection relating to 'US persons' is limited and minimised. Similarly, the review the FISC conducts focuses primarily on the impact the data collection will have on US citizens. The only substantive limitation imposed is that the acquisition of data must have the obtaining of foreign intelligence information as a 'significant' (not primary!) purpose. To make matters worse, non-US persons abroad are unable to invoke 4$^{th}$ Amendment Constitutional protection against unreasonable search and seizures. According to US Supreme Court jurisprudence, any such protection would need to be agreed through 'diplomatic understanding, treaty or legislation'.

What then does this mean for UK residents? Can UK authorities access data on UK residents gathered by US agencies in accordance with FISA? Former Foreign Secretary Malcolm Rifkind argues that the law applies equally whether the intercept is conducted by GCHQ or by another agency on its behalf and therefore ministerial approval is necessary under RIPA. However, Matthew Ryder QC and Simon McKay argue that when intelligence already in the hands of an agency such as the NSA is handed over to the GCHQ, 'there is little, if any, legal regulation or oversight in that situation' as the RIPA applies only when the GCHQ gathers the data itself. A possible distinction exists here between situations where the GCHQ asks the NSA for data and thus intercepts indirectly (hence RIPA applies) and one where the data is simply provided to the GCHQ by the NSA pursuant to The Security Service Act 1989 and the Intelligence Services Act 1994.

A number of conclusions can be drawn from this bleak picture. First, the current plea for transparency from technology giants regarding FISA requests will be of little consolation to non-US persons given the lack of ex ante safeguards and ex post redress options they have under the legislation. Second, EU Data Protection regulation is, at present, toothless once international data transfers have been made. Some are proposing a technical solution to this problem, a 'European Cloud' which would keep personal data out of the hands of US agencies from the outset. Finally, there is a potential silver lining to this problematic Cloud: this scandal has raised the prominence of problems associated with government surveillance. This will hopefully help put a nail in the coffin of the 'Snooper's Charter' once and for all.

*Note: This article gives the views of the author, and not the position of the British Politics and Policy blog, nor of the London School of Economics. Please read our comments policy before posting.*

**About the Author**

**Dr Orla Lynskey** *is a Lecturer in the law deparment at the LSE. She studied law at Trinity College, Dublin (LLB Law and French) before reading for a Masters in European Legal Studies at the College of Europe, Bruges. She was called to the Bar of England and Wales in 2008. She completed a PhD at the University of Cambridge focusing on European data protection law.*