Home Office

James Brokenshire MP
Immigration and Security Minister

2 Marsham Street,
London SW1P 4DF
www.homeoffice.gov.uk

Caroline Lucas MP
House of Commons
London
SW1A 0AA

07 APR 2014

CTS Reference: M2659/14
Your Reference: ML.C0011.AR.24.02.14

Dear Caroline,

Thank you for your letter of 24 February on behalf of a number of constituents, raising the six principles of the "Don't Spy on Us" campaign. I am sorry for the delay in replying.

Our law enforcement and intelligence agencies undertake their work within a strict legal and policy framework. They must sometimes undertake intrusive activities in order to save lives and keep the public safe from the threat of terrorism and crime. When they do so, they are regulated by statute specifically to ensure that their activities are lawfully authorised, necessary for specified lawful purposes and proportionate, and subject to rigorous independent oversight.

The Regulation of Investigatory Powers Act 2000 (RIPA) sets out a transparent legal framework, approved by Parliament, for the regulation of the interception of communications and acquisition of communications data. RIPA contains a full range of robust safeguards, specifically designed to meet in full our obligations under the European Convention on Human Rights.

Requests for communications data must be authorised on a case-by-case basis by a senior officer or official in the applying agency at a rank and for purposes stipulated by Parliament. In 2012 the Joint Committee that scrutinised the Draft Communications Data Bill took a wide range of public evidence on this issue and concluded: "it is our view that the current internal authorisation procedure is the right model." For the interception of communications, the relevant Secretary of State must sign a warrant, and consideration must be given to the degree of collateral intrusion that might arise and where the communications might affect religious, medical or journalistic confidentiality or legal privilege. Authorisation takes place on a case-by-case basis, for limited and specified purposes and only when the test of necessity and proportionality is met.

Lawful interception and communications data acquisition powers are already subject to vigorous, independent oversight. RIPA provides for independent oversight by the Interception of Communications Commissioner who reports to the Prime Minister and whose annual report is published and laid before Parliament. The Commissioner must previously have held high judicial office. He has teams of inspectors who examine intelligence gathering activities, ensuring that required, statutory processes are followed and that requests are necessary and proportionate. They have access to any information that they believe is necessary to carry out their functions.

The Security and Intelligence Agencies are also subject to oversight by the Intelligence and Security Committee (ISC) of Parliament. The powers of the ISC have recently been strengthened by The Justice and Security Act 2013. The power for the agency heads to withhold information from the Committee on the grounds of sensitivity has been withdrawn. This has formalised the ISC's role in overseeing the wider intelligence community and enabled the ISC to oversee operational activities on matters of significant national interest retrospectively. The ISC is committed to ensuring oversight of the intelligence agencies becomes more transparent and accordingly held its first public evidence session on 7 November 2013. It is currently conducting a review into the balance between public privacy and national security, details of which can be found on the Intelligence and Security Committee website (http://isc.independent.gov.uk).

The independent Investigatory Powers Tribunal (IPT) provides an effective right of redress to any individual who thinks that surveillance powers have been used against them unlawfully. Members of the IPT must be senior members of the legal profession and both the president and vice president must have held high judicial office.

The Government remains committed to ensuring that the internet is a safe and secure environment for those who use it lawfully. The recently launched Cyber Streetwise campaign aims to change the way people view online safety, and provide the public and businesses with the skills and knowledge they need to take control of their cyber security. However, for those that would seek to use the internet for illegal purposes we are robust in disrupting their activities. We cannot allow cyberspace to become a haven for criminals.

Our current intelligence oversight arrangements are robust, fit for purpose, and wholly compatible with our obligations under the European Convention on Human Rights. Any intrusion into the lives of individuals must be shown to be necessary and proportionate, and a comprehensive regulatory framework has been put in place to oversee these procedures. Indeed, the UK has one of the strongest systems of checks and balances for its use of intelligence anywhere in the world.

I hope this reply addresses your constituents' concerns.

Yours ever,

James Brokenshire