Home Office

Office for Security and Counter-Terrorism
2 Marsham Street, London
SW1P 4DF
OSCTFOI@homeoffice.x.gsi.gov.uk
Website: www.homeoffice.gov.uk

Tel: 020 7035 4848
Fax: 020 7035 4745
www.homeoffice.gov.uk

TJ McIntyre
request-160774-01ef71ec@whatdotheyknow.com

FOI Ref: 27471
Date: 28 June 2013

Dear TJ McIntyre

Thank you for your correspondence of 9 May 2013 in which you request information about URL filtering. Your request has been handled as a request for information under the Freedom of Information Act (2000).

You have asked a series of questions about the operation of a URL filtering list. Some questions seek disclosure of recorded information, others an explanation of the basis on which the filtering mechanism operates. We have set out at the enclosed annex a detailed explanation of how URL filtering presently operates. This explanation should address all of the points you have raised. You requested disclosure of specific risk assessment and consultation documents. These documents do not exist and are therefore not enclosed.

If you are dissatisfied with this response you may request an independent internal review of our handling of your request by submitting a complaint within two months to the address below, quoting reference 27471. If you ask for an internal review, it would be helpful if you could say why you are dissatisfied with the response.

If you have further questions based on the content of this response, or seek other recorded information on this subject, these questions should be submitted as a new FOI request.

Information Access Team
Home Office
Ground Floor, Seacole Building
2 Marsham Street
London SW1P 4DF
e-mail: info.access@homeoffice.gsi.gov.uk

As part of any internal review the Department's handling of your information request will be reassessed by staff who were not involved in providing you with this response. If you remain dissatisfied after this internal review, you would have a right of complaint to the Information Commissioner as established by section 50 of the Freedom of Information Act.

Yours sincerely,

J. Fanshaw

Annex

The Home Office do currently provide a list of URLs which breach UK terrorism legislation to filtering companies that supply some coverage across the public estate, mainly schools and libraries, with a view to safeguarding vulnerable people.

This forms the policy referred to in our response to your previous request on this issue (FOI 20529) which was then under development and took effect shortly after the Prevent Strategy was published. We made this clear on publication of the strategy (2011):

> *"internet filtering across the public estate is essential. We want to ensure that users in schools, libraries, colleges and Immigration Removal Centres are unable to access unlawful material. We will continue to work closely with DfE, BIS, the CTIRU, Regional Broadband Consortia and the filtering industry."*

There are a number of statutory provisions that allow the prosecution of individuals who publish terrorist or related extremist material on the internet or elsewhere. In particular these provisions criminalise the encouragement of terrorism (s.1 Terrorism Act 2006) and the dissemination of terrorist publications (s.2 Terrorism Act 2006).

The assessment of whether material hosted or distributed from abroad would make the host/distributor liable to prosecution if they were apprehended in the UK is a decision made by specialist prosecutors at the Special Crime and Counter Terrorism Division of the CPS. As the unit of the CPS responsible for advising on and prosecuting all terrorism cases within England and Wales they have a considerable wealth of experience on which to draw. The specialist prosecutors who review the material referred to them by CTIRU therefore apply their understanding of the law to the particular content of the material submitted.

By way of background, the Counter Terrorism Internet Referral Unit (CTIRU) is a dedicated police unit which assesses and investigates internet-based content which may breach the Terrorism Act 2006 (TACT).

If content breaches TACT, CTIRU takes appropriate action through the criminal justice system and/or by contacting internet service providers. Members of the public concerned about online material can make referrals to the CTIRU through the gov.uk website: www.gov.uk/terrorism-national-emergency/reporting-suspected-terrorism.The website also highlights how to find out which company hosts the unlawful or offensive material. The intention is that content can be referred directly to the company which hosts the relevant site and whose contractual terms of use may be breached by it.

Where material is hosted overseas and CTIRU are unable to take it down due to jurisdictional issues, the focus has been on voluntary end-user filtering. Unlike blocking, which occurs at the network level and over which users have no choice, filtering software allows end users to choose to apply filtering at the desk top level.

CTIRU have developed and are updating a list of URLs that are hosted abroad and which it is assessed the distribution or hosting of which would (in the absence of any statutory defence) give rise to criminal liability under the provisions of the Terrorism Act 2006. All material filtered from the public estate is therefore considered to be illegal under the Terrorism Act 2006, as assessed by the Crown Prosecution Service (CPS),.

The filtering list is provided to companies who supply filtering products across the public estate, including schools and libraries. This means that the URLs on the list can still be accessed on private computers or devices outside the public estate. There is no formal appeal process but if

there is concern regarding the filtering of a specific URL containing illegal material, contact should be made with Home Office.

Yours sincerely

J Fanshaw