



Foreign &
Commonwealth
Office

London SW1A 2AH

Minister for Europe

RECEIVED 10 FEB 2006

8 February 2006

Your reference: [REDACTED]

Our reference: 23843

Ben Chapman Esq MP
House of Commons
London
SW1A 0AA

Dear Ben -

Thank you for your letter of 23 January enclosing one from your constituent, Mr Simon Jones of 11a The Village, [REDACTED], about the data retention directive.

I am aware that the Creative and Media Business Alliance (CMBA) lobbied Members of the European Parliament (MEPs) to broaden the scope of the directive to cover piracy before its adoption last year. Their petition was in fact unsuccessful. The directive is designed to assist law enforcement in the fight against terrorism and serious crime, and the text reflects this. Nonetheless, the directive does not prevent individual Member States from continuing with established domestic practice. In the UK, police and intelligence agencies can access retained communications data for the purpose of investigating any crime, although any request to access data must be proportionate to the investigation.

There is no question of allowing the creative industries access to data retained under the terms of the directive. Only law enforcement agencies have the authority to access the data, and they must meet national standards to access private information. I should clarify that the data is limited to call records, location information and internet logs. This reveals who made the call, when and where. The actual content of calls or emails will not be retained and will remain private.

There is no doubt that communications data is a valuable law enforcement tool. In the UK, the availability of this data has already proven to be a vital asset in the investigation of countless offences, including the terrorist attacks in London. It can also help to prove alibis. In one recent case, unsuccessful call data was actually used to eliminate a suspect from a murder investigation. The directive will extend the obligation to retain communications data for at least six months to all EU Member States, helping to close loopholes that criminals seek to exploit.

As Mr Jones points out, in order to avoid detection terrorists and criminals may seek to acquire and use the same technologies that afford businesses and individuals legitimate security and privacy. The Home Office is considering domestic legislation to tackle this problem.

This Government regards communications data as an essential tool in combating terrorism and serious crime. Imposing requirements on service providers to retain data about innocent people is part of the difficult balance between protecting people from terrorism and serious crime, and respecting the civil liberties of the same individuals.

Yours ever,

DOUGLAS ALEXANDER