



All Party Parliamentary Group on Privacy

Providing Early Warning Protection on Privacy Issues to Parliament



Enquiry Terms

Interception Modernisation Programme

ABOUT THE APPG

Purpose

- Promote interest in and protection of the right to privacy;
- Address key emerging privacy issues in public policy; and
- Promote debate and discussion of privacy related issues throughout Parliament.

Officers of the group

Edward Garnier QC MP
(Conservative) – Chair

Lord Peston (Labour) – Vice
Chair

The Earl of Northesk
(Conservative) – Vice Chair

David Heath MP (Liberal
Democrat) – Vice Chair

Secretariat

Privacy International
privacyint@privacy.org
<http://privacyappg.org.uk>

The APPG on Privacy is enquiring into the implications of the Home Office proposals for its Interception Modernisation Programme.

On 27 April 2009 the Government published a consultation document Protecting the Public in a Changing Communications Environment which calls for telephone companies and internet service providers to substantially increase the amount of material they retain about their customers' internet usage and to analyse it against demands for disclosure from law enforcement and the Agencies. The document explicitly rejects the notion that this data should be held in a centralised database.

A meeting will be held in Committee Room 16 of the House on Wednesday July 1st between 10.00 and 11.45. A number of experts have been invited to present evidence on the implications of these proposals. The government will also be invited to present its case.

The Chairman of the meeting will be Edward Garnier QC.

The main terms of reference are:

- Given that Communications Service Providers (CSPs) are already compelled to retain customer data for a period of 12 months, what detailed risk analysis has been carried out to justify requiring them to collect a great deal more and to carry out preliminary analyses?
- Given the nature of the new ways in which people communicate across the Internet such as web-mail, social networking and online gaming, is it feasible to maintain the distinction between “communications data” and “intercepted content”? What are the implications for investigations and trials if intercept material remains inadmissible?
- Is it still reasonable that interception warrants are issued by the Secretary of State and that communications data disclosures are self-authorised by the organisations seeking them? Should these powers be exercised by the judiciary? Does the office of the Interception Commissioner provide a realistic safeguard against abuse? What Parliamentary oversight of the activities covered in the scheme is envisaged?
- Is the Home Office estimate of the costs of its programme at £2bn realistic and likely to be value for money?
- Given that a new and heavy financial burden is to be placed on CSPs, what will be the implications for the provision of universal Internet access throughout the United Kingdom?

- What other routes are available to the police and Agencies to investigate the threats that they argue are faced by the UK?
- What steps have been taken by the Home Office to ensure that other government departments and agencies are content with the way the scheme is intended to operate?
- What protocols have the Home Office agreed to with regard to data sharing within and outside government and what protections or procedures are available to the individual citizen or subject of the collected information to audit its content and movement between government departments and agencies or private operators?