Liberty’s response to the Home Office consultation paper: Transposition of Directive 2006/24/EC
About Liberty

Liberty (The National Council for Civil Liberties) is one of the UK’s leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

Liberty Policy

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, Inquiries and other policy fora, and undertake independent, funded research.


Contact

Gareth Crossman  Isabella Sankey  Anita Coles
Director of Policy  Policy Officer  Policy Officer
Direct Line: 020 7378 3654  Direct Line 020 7378 5254  Direct Line: 020 7378 3659
Email: garethc@liberty-human-rights.org.uk  Email: bellas@liberty-human-rights.org.uk  Email: anitac@liberty-human-rights.org.uk
Introduction

1. The consultation paper on the transposition of Directive 2006/24/EC is understandably limited in scope. It simply invites comment on the transposition of the directive into domestic law by way of statutory instrument (SI). The consultation questions are primarily aimed at communications service providers and the implications that implementation of the directive will have on them. Consequently there is little comment that Liberty is able to make on the substance of the consultation as the proposed instrument closely reflects the directive.

2. The subject of communications data access, however, has become the subject of much wider political interest. The Communications Data bill, to be published following consultation in early 2009, may contain proposals for communications data to be placed on a centralised database. Data is currently held by individual communications service providers. Any public body wishing to access communications data has to request it from the service provider who has followed the appropriate authorisation process set out in the Regulation of Investigatory Powers Act 2000 (RIPA). The prospect of centralising all communications data entirely within the public sector is of huge concern. It will undermine the accountability of public sector agencies and could provide the basis for moves towards data mining. Data mining (or data profiling) has been identified by the Home Office as increasingly relevant to modern crime detection/prevention. We are extremely concerned by the prospect of allowing millions of communications to be sifted to identify potential criminality. Centralised retention of all communications would signify a significant shift in the relationship between the individual and state.

---

1 See, for example the consultation ‘New Powers New Powers Against Organised and Financial Crime. http://www.homeoffice.gov.uk/documents/cons-2006-new-powers-org-crime/cons-new-powers-paper?view=Binary which states (page 22) ‘We believe there may be greater scope for law enforcement to adopt this process of ‘profiling’ in order to check across a range of datasets to identify suspicious patterns of activity. As technology advances, and ever more information is stored electronically, there is a huge opportunity to use these sort of techniques, which hold out the opportunity to protect the public by picking up patterns and trends in criminal activity which might not be spotted when data is looked at individually.’
The consultation

3. The consultation gives a range of examples demonstrating the importance of communications data retention. We agree that communications data record can prove a valuable crime detection and prevention tool. It is exercisable by a wide range of public authorities and does not need to involve investigation into serious criminality. The most recent report of the Interceptions of Communications Commissioner gives an indication of the type of activity where communications data is used by local authorities and other public bodies. ‘Generally the trading standards services are the principal users of communications data within local authorities although the environmental health departments and housing benefit fraud investigators also occasionally make use of the powers. Local authorities enforce numerous statutes and Councils use communications data to identify criminals who persistently rip off consumers, cheat the taxpayer, deal in counterfeit goods, and prey on the elderly and vulnerable. The environmental health departments principally use communications data to identify fly-tippers whose activities cause damage to the environment and cost the taxpayers large sums to recover or otherwise deal with the waste’. Fly-tipping, counterfeiting and benefit fraud are criminal activities but they are not at the most serious end of criminality. However, the examples given in the consultation involve offences of child sex abuse; armed robbery; bomb threats; kidnap; rape; murder and blackmail. This could give the impression that communications data access relates only to the most serious forms of offending. The Government and Home Office have stated, with some justification, that it is a mistake to refer to RIPA powers as relating only to terrorism or organised crime. However, if this misconception is to be avoided it would assist if consultation papers gave a greater range of purpose for communications data access.

4. At paragraph 2.7 the consultation states that business will be able to retain data for periods over the minimum 12 months so long as the Data Protection Act 1998 (DPA) is complied with. While it is correct to refer to the DPA it is also necessary, we would also suggest that retention periods would also need to be compatible with the Human Rights Act 1998. Although communications data providers are not public authorities any

---

3 There are also two examples given of communications data being used to prevent or assist with attempted suicide
private body carrying out a public function is covered by the HRA. If the purpose of communications data retention is for national security, crime detection/prevention and so on then we suggest that those holding the data will be carrying out a public function. In practical terms there will not be a significant distinction between DPA compliance and HRA compliance. Many of the data protection principles, such as only processing data for legitimate purposes and not retaining data for longer than necessary, mirror HRA requirements for proportionality and necessity. However in terms of presentation, it is important to acknowledge that all those who hold communications data do so in accordance with human rights principles.

5. The transposition of the directive will take place by way of SI. The majority of the SI directly transposes the Directive. As a consequence, there is little comment that can be made. It is however worth noting part of the SI that is not contained in the Directive. Paragraph 13 states that ‘the regulations do not apply to a public communications provider if, or to the extent that, the communications data concerned are retained…by another public communications provider.’ This would seem a sensible measure intended to avoid unnecessary duplication. Indeed the impact assessment states that this is intended to ‘avoid duplicative storage of data’. However, it is worth considering paragraph 13 in the context of reported plans to allow black boxes to collect communications data. This would assist in allowing centralised retention as described in paragraph 2 above. It is not clear whether black box technology will copy or replace communication provider data. Similarly, it is not clear whether retention of this type would be ‘by another communications provider’. However, if black boxes are introduced it is possible to interpret paragraph 13 to mean that the SI’s protections relating to improper use of data do not apply. This includes paragraph 9 which states that ‘data must be subject to appropriate…measures to protect the data against…unauthorised or unlawful storage, processing, access or disclosure.’ This interpretation of Paragraph 13 is clearly not that envisaged by the impact assessment. However, it would be preferable if Paragraph 13 were to be amended so that it specifies that the purpose is to avoid duplicative storage of data.

Gareth Crossman, Liberty

---

4 See http://www.independent.co.uk/news/uk/home-news/government-black-boxes-will-collect-every-email-992268.html