EUROPEAN COMMISSION

DIRECTORATE-GENERAL INFORMATION SOCIETY
Directorate B: Communication services: policy and regulation framework

DIRECTORATE-GENERAL JUSTICE AND HOME AFFAIRS
Directorate D : Internal Security and Criminal Justice

Brussels, 30 July 2004

DG INFSO – DG JAI CONSULTATION DOCUMENT

ON

TRAFFIC DATA RETENTION

This is a joint working document of DG Information Society and DG Justice and Home Affairs which does not necessarily reflect the official position of the Commission. No inferences should be drawn from this document as to the precise form or content of future measures to be submitted by the Commission. The Commission accepts no responsibility or liability whatsoever with regard to any information or data referred to in this document.

DG INFSO - DG JAI consultation document on traffic data retention

Summary

Citizens increasingly perform daily activities and transactions using electronic communications networks and services. These communications generate so-called 'traffic data' possibly including details about time, place and numbers used for fixed and mobile voice services, faxes, e-mails, SMS and other use of the Internet.

Because of changes in technologies, business models and service offerings (e.g. flat rate tariffs, prepaid and free electronic communications services, email services, SMS and MMS), law enforcement authorities are concerned that some data may not always be stored by all electronic communications operators to the same extent as they were in recent years. These traffic data would hence not be available for these public authorities when needed.

A certain number of Member States have therefore adopted, or plan to adopt, national measures requiring some or all operators to retain given types of traffic data so that they can be used for certain 'public order' purposes when necessary.

In its recent **Declaration on combating terrorism of 25 March 2004**, the European Council instructed the Council to examine 'proposals for establishing rules on the retention of communications traffic data by service providers'. The Declaration also stated that priority should be given to these with a view to adoption by June 2005.

In response, four Member States (UK, IE, FR, and SW) tabled a proposal for a Council Framework Decision on Data Retention under Title VI of the Treaty on European Union, which is being discussed in the Council[1].

The Commission services would welcome written contributions on the issues raised in the present consultation document.

Contributions should be addressed to INFSO B.1 and JAI D.2 at the following addresses: infso-b1@cec.eu.int and jai-eu-forum-organised-crime@cec.eu.int

The deadline for sending contributions is 15 September 2004.

Contributions received will not be made public.

[1] Draft Council Framework Decision on the Retention of Data Processed and Stored in Connection With the Provision Of Publicly Available Electronic Communications Services or Data on Public Communications Networks for the Purpose Of Prevention, Investigation, Detection And Prosecution of Crime and Criminal Offences Including Terrorism (document 8958/04 CRIMORG 49, TELECOM 82). This document is available at: http://register.consilium.eu.int/pdf/en/04/st08/st08958.en04.pdf

Purpose of the consultation

DG Information Society and DG Justice and Home Affairs are seeking input from a broad spectrum of stakeholders on a number of questions raised by the issue of traffic data retention, as set out hereafter.

On previous occasions the Council has explicitly called for a dialogue at national and EU level aimed at finding solutions to the issue of traffic data retention[2]. An open and transparent debate has also been asked by the European Parliament, as well as by industry[3].

The contributions of all interested parties, including Member States, law enforcement authorities, data protection authorities, industry and consumers/citizens are most welcome. The Commission services plan to hold a public workshop on this subject in September 2004.

No inferences should however be drawn from this document as to any position that may be taken by the Commission on this issue or any related initiative.

Background

To contribute to the protection of citizens' fundamental rights and freedoms, and in particular their privacy and personal data, Community law provides for the deletion of traffic data once it is no longer needed for the purpose of the transmission of the communication. However, some data may be kept and further processed by service and network providers, for their own business purposes such as billing or simply because consumers have consented to this[4].

Beyond these business purposes, 'public order' purposes can also be invoked to justify the further storage and processing of traffic data[5]. The availability of traffic data can indeed be important for certain 'public order' purposes.

---

[2] JAI Council Conclusions 'on information technology and the investigation and prosecution of organised crime' of 19 December 2002 have explicitly called upon a dialogue at national and EU level aimed at finding solutions to the issue of traffic data retention that satisfies both the need for effective tools for prevention, detection, investigation and prosecution of criminal offences and the protection of fundamental rights and freedoms of natural persons, and in particular their right to privacy, data protection and secrecy of correspondence.

[3] See e.g. EP Recommendation for second reading on the Council common position for adopting a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector , A5-0130/2002, 22 April 2002. See also the EP report of 24 February 2004 on the First Report on the implementation of the Data Protection Directive (95/46/EC), A5 0104 -2004.

[4] See Article 6 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications), OJ L 201, 31 July 2002.

[5] 'Public order' purposes are understood in the present document as referring to the public order interests mentioned in Article 15 of Directive 2002/58/EC: national security (i.e. State security), defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system. For the sake of this document, law

Legitimate requests for the "preservation" of specific data (i.e. onwards storage of data, as from the date of the request) are allowed when necessary for specific purposes, such as investigations and prosecutions.

In Community law, the 2002 Directive on Privacy and Electronic Communications, adopted after 11 September 2001, has set out[6] conditions under which Member States may adopt legislative measures for law enforcement purposes, including data retention measures, which derogate from the obligation to erase traffic data when these are not longer necessary for the provision of the service or the billing of that service.

Directive 2002/58/EC on Privacy and Electronic Communications requires the following conditions to be respected by national data retention measures:

– be legislative in nature;

– ensure that the data is only retained for a limited period of time;

– aim to achieve specific, listed 'public order' purposes;

– be necessary, appropriate and proportionate within a democratic society for achieving these specific purposes.

Moreover, the conformity of data retention measures with the provisions of this Directive must be interpreted in the light of fundamental rights which form an integral part of the general principles of Community law including the right to respect for private life as laid down in Article 8 of the European Convention on Human Rights.

Directive 2002/58/EC on Privacy and Electronic Communications does however not fully harmonise the conditions under which traffic data might be retained or otherwise processed for 'public order' purposes.

Discussion points

From a European single market point of view, a proportionate and consistent approach in all Member States is desirable. Consistency would avoid the situation where the providers of electronic communications services are confronted with a patchwork of diverse technical and legal environments. From this perspective, it is desirable that any data retention measures taken by Member States differ as little as possible, in particular in terms of the types of data concerned, the periods of data retention, the technical feasibility of any requirements and the sharing of costs.

Determining what would be proportionate and consistent implies an assessment of both existing practices and the actual needs and capabilities.

The Commission services are therefore particularly keen to solicit contributions from interested parties on the issues below.

---

enforcement purposes are understood as restricted to the prevention, investigation, detection and prosecution of criminal offences.

[6] See in particular Article 15 (1) of Directive 2002/58/EC.

1. Existing practices

The Commission services are seeking input and comments from interested parties on the following issues:

- the current practices of traffic data storage for business purposes, including how long the traffic data are stored, according to services concerned (e.g. fixed telephony, mobile telephony, SMS, MMS, email and internet-related usage) and types of offerings (e.g. flat rate services, prepaid services);

- the current practices for public authorities to access and/or preserve the data stored, according to services concerned (e.g. fixed telephony, mobile telephony, SMS, MMS, email and internet-related usage) and types of offerings (e.g. flat rate services, prepaid services), and in particular:

  - the nature and the age of the data requested by law enforcement authorities;

  - the number and frequency at which requests for given types of data are made;

  - the procedures to which such requests are submitted;

  - if and how additional costs are taken into account or reimbursed;

  - the effectiveness of current access regimes.

2. Data retention for law enforcement purposes at EU level

The Commission services are seeking input and comments from interested parties on the following issues:

- the extent of the need for a common data retention regime at EU level for law enforcement purposes, and its scope, including for what types of traffic data (e.g. covering fixed and/or mobile telephony, or covering also SMS/MMS, email and other internet related services);

- the features of such a common data retention regime at EU level for law enforcement purposes, including :

  - the types of data that should be retained by operators for each service (for e.g. fixed telephony, voice telephony, SMS, MMS, email, internet-related data etc.);

  - the period of time, according to the services and to the data concerned;

  - the financial implications of data retention.

- the technical feasibility of specific data retention requirements, in relation to the cost of data retention requirements in specific services (e.g. fixed telephony, voice telephony, SMS, MMS, email, internet-related data etc.) or offerings.

As much as possible, responses should not only look at current, well established technologies but should also take into account technology developments in e.g. VoIP, broadband.