

EU consults member states on data retention

By Eugene Oscapella

A NEW EU REPORT reveals that member state governments are not having an easy time trying to persuade Internet service providers to retain data on their customers.

The need for telecommunications providers and other such companies to retain "traffic data" for government investigative agencies has become a recurring concern (See *PL&B Int*, Sept 2002, p.2, 24).

On August 14th 2002, the EU Council sent to all Member States' governments a questionnaire on the retention of data traffic. The objective was in part to advance efforts to combat cybercrime. The questionnaire also aimed to provide greater knowledge about the impact of data retention on industry. The answers were examined at an EU Council expert group meeting (the Multidisciplinary Group on Organised Crime) on September 16th 2002 and made available to the public in early October.

Among other questions, the survey asked whether data traffic retention was covered by existing legislation. It asked about the specific periods of time for the retention of traffic data, and what kinds of traffic data should be retained.

The survey also asked about procedures for law enforcement authorities to obtain traffic data from a service provider, and whether the procedure has been efficient and effective. It also sought to determine whether law enforcement authorities felt their work was being obstructed by the "non-existence of appropriate legal instruments" concerning traffic data retention.

The survey sought to determine the impact of traffic data retention on industry. It asked whether countries had entered into a permanent dialogue with their telecommunications indus-

try about traffic data retention, and about the general willingness of the telecommunications industry to retain traffic data. Finally, it asked how the respondents would rate the solution of creating a legal instrument on traffic data retention for law enforcement purposes at a European level.

German associations
and service providers
"tend" to be critical of
obligations to retain
traffic data "on
economic grounds and
for reasons of data
protection."

SURVEY RESULTS

Of the countries surveyed, Greece, Luxembourg and Portugal did not provide answers because their governments are currently considering the issue. The preliminary French response was not included in the September 16th report because it still required verification by the various ministries involved in answering the questionnaire.

There were mixed answers to questions about the telecommunications industry's general willingness to retain

traffic data. The Austrian response indicated service providers' general readiness to retain traffic data. Similarly, the Belgian response noted a "fairly high willingness" in initial contacts with the telecommunications industry. Irish providers were also seen as cooperative. The report from the UK noted initial industry support for "voluntary" arrangements during the development of the Anti-Terrorism Act. Industry now appears to favour a mandatory system since this would protect it from corporate liability litigation. Still, the report indicated that the UK industry was willing to work with the government on data retention issues.

However, recent reports in the UK press have revealed a split between service providers and the government, which is currently trying to implement a voluntary code of practice on data retention. The Internet Service Providers' Association has said that it will not recommend that its members comply with the code (see p.3).

The Swedish report stated that it was not possible to judge the opinion of the whole industry concerned, while the Finnish telecommunications industry was described as being reluctant to retain traffic data other than for business purposes. German associations and service providers "tend" to be critical of obligations to retain traffic data "on economic grounds and for reasons of data protection". The Netherlands report notes that, in general, the willingness of the industry to retain traffic data "cannot be judged as entirely positive". Like some of their counterparts

elsewhere, Spanish service providers expressed concern about the possible cost of storing and processing such data. The Spanish report also noted that an overly costly obligation could constitute a barrier for smaller service providers to enter the market.

INCREASED SURVEILLANCE OF COMMUNICATIONS

At the same time as the EU survey was being completed, US-based Electronic Privacy Information Center (EPIC) and UK-based Privacy International released their 2002 edition of Privacy and Human Rights. This year's report documents increased communications surveillance in the wake of the terrorist attacks in the US. It expresses concern over the number of countries enacting laws requiring Internet service providers and other telecommunications operators to retain the traffic and location data of all people using mobile phones, text messaging, land-line telephones, faxes, e-mails, chat rooms, the Internet, or any other electronic communication devices.

Commenting on the *2002 Privacy and Human Rights Report* to UK broadcaster the BBC, Simon Davies, Director of Privacy International, warned that the Internet is being turned into a surveillance device and that surveillance will eventually be a core design component of computers.



Further information on the EU report and data retention issues:

General Secretariat of the Council,
Mr Peter Nath, 175 rue de la Loi, B-1048 Brussels, tel.: +32-2-285-6677,
facsimile: +32-2-285-8832, email:
peter.nath@consilium.eu.int;

For a copy of the "2002 Privacy and Human Rights Report," see the Privacy International website:
www.privacyinternational.org

EU pushes ahead with directive on workers' data

By Alan Pedersen

On October 31st, the European Commission launched the second stage of its consultation into a proposal for a directive on the protection of workers' personal data. The six-week consultation period with the social partners (including representatives from trade unions and the business community) will seek comments on areas relating to sensitive data, drugs and genetics testing, and workplace monitoring.

According to Anna Diamantopoulou, Commissioner for Employment and Social Affairs, the "EU needs clearer, simpler rules on protection of workers' personal data, which take better account of the employer/worker relationship." The Commission notes that workplace privacy across the EU is addressed through a varied and complex mix of data protection legislation, codes of practice and labour laws. This, it says, could create barriers to the internal market and affect the free movement of workers within the EU.

The social partners, understandably, are split in their opinions of the directive. The European Trade Union Confederation (ETUC) supports a harmonised data protection law specifically addressed to workers. However, the business community has stated that workers' data is sufficiently protected by existing data protection and labour laws. The Union of National Industrial and Employers' Confederation of Europe (UNICE) wants the Commission to wait until the results of the current EU Data Protection Directive (95/46/EC) review are published before deciding whether to embark on a new directive. A Commission-funded study into workplace privacy, published in July this year, has backed some of the business community's claims, indicating that there is a lack of evidence to suggest the need for an additional directive (see *PL&B Int*, Sept 2002, p.5).

The comments and proposals contained in the Commission's consultation paper are based on analysis from the first consultation stage. They include:

Consent – Due to the subordinate relationship between workers' and their employers, it is difficult for workers to refuse, withdraw or modify consent for processing data, especially in the case of sensitive personal data.

Health data – Health data should be processed only where necessary (ie. to meet occupational health and safety guidelines, or to assess ability to carry out duties), any examinations should be performed by healthcare professionals only, and only relevant information should be disclosed to employers.

Drug and genetics testing – According to the Commission, the use of drug testing is becoming a commonplace practice in some member states. There are also fears that employers may increasingly look towards the use of genetics testing when deciding whether to employ or promote staff. The Commission, therefore, intends to place limitations on the amount of information employers are allowed to collect, and the circumstances in which they can collect data.

Monitoring and surveillance – The Commission proposes that trade unions be consulted before monitoring and surveillance systems are implemented. Monitoring of individuals should be carried out only where there are reasonable grounds for suspicion of criminal activity or misconduct. Blanket monitoring of all staff should be prohibited, and employers should not be allowed to look at private e-mails.

The full text of the Commission's consultation can be found at:
www.europe.eu.int/comm/employment_social/news/2002/oct/data_prot_en.html