Electronic communications: personal data protection rules and availability of traffic data for anti-terrorism purposes

2005/0182(COD) - 18/04/2011 - Follow-up document

The Commission presents its evaluation report on Directive 2006/24/EC (the Data Retention Directive). The Directive requires Member States to oblige providers of publicly available electronic communications services or of public communications networks ('operators') to retain traffic and location data for between six months and two years for the purpose of the investigation, detection and prosecution of serious crime.

The report evaluates the application of the directive by Member States and its impact on economic operators and consumers. It aims to determine whether it is necessary to amend the provisions of the Directive, in particular with regard to its data coverage and retention periods. The report also examines the implications of the Directive for fundamental rights, in view of the criticisms which have been levelled in general at data retention, and examines whether measures are needed to address concerns associated with the use of anonymous SIM cards for criminal purposes.

The report highlights a number of benefits of and areas for improvement in the current data retention regime in the EU. The EU adopted the Directive at a time of heightened alert of imminent terrorist attacks. The Commission intends to conduct an **impact assessment** that will provide an opportunity to assess the data retention in the EU against the tests of necessity and proportionality, with regard to and in the interests of internal security, the smooth functioning of the internal market and reinforcing respect for privacy and the fundamental right to protection of personal data. The Commission's proposal for revising the data retention framework should build on its conclusions and recommendations.

The EU should support and regulate data retention as a security measure: most Member States take the view that EU rules on data retention remain necessary as a tool for law enforcement, the protection of victims and the criminal justice systems. The evidence, in the form of statistics and examples, provided by Member States is limited in some respects but nevertheless attests to the very important role of retained data for criminal investigation. These data provide valuable leads and evidence in the prevention and prosecution of crime. Their use has resulted in convictions for criminal offences which, without data retention, might never have been solved. It has also resulted in acquittals of innocent persons. Harmonised rules in this area should ensure that data retention is an effective tool in combating crime, that industry has legal certainty in a smoothly functioning internal market, and that the high levels of respect for privacy and the protection of personal data are applied consistently throughout the EU.

Transposition has been uneven: transposed legislation is in force in 22 Member States. The considerable leeway left to Member States to adopt data retention measures under the e-Privacy Directive (Directive 2002/58/EC) renders assessment of the Data Retention Directive highly problematic. There are considerable differences between transposed legislation in the areas of purpose limitation, access to data, periods of retention, data protection and data security and statistics. Three Member States (Czech Republic, Germany and Romania) have been in breach of the Directive since their transposing legislation was annulled by their respective constitutional courts. Two further Member States (Austria and Sweden) have yet to transpose. The Commission will continue to work with all Member States to help ensure effective implementation of the Directive. It will also continue in its role of enforcing EU law, ultimately using infringement proceedings if required.

The Directive has not fully harmonised the approach to data retention and has not created a level-playing field for operators: the Directive does not in itself guarantee that retained data are being stored, retrieved and used in full compliance with the right to privacy and protection of personal data. The responsibility for ensuring these rights are upheld lies with Member States. The Directive only sought partial harmonisation of approaches to data retention; therefore it is unsurprising that there is no common approach, whether in terms of specific provisions of the Directive, such as purpose limitation or retention periods, or in terms of aspects outside scope, such as cost reimbursement. However, beyond the degree of variation explicitly provided for by the Directive, differences in national application of data retention have presented considerable difficulties for operators.

Operators should be consistently reimbursed for the costs they incur: there continues to be a lack of legal certainty for industry. The obligation to retain and retrieve data represents a substantial cost to operators, especially smaller operators, and operators are affected and reimbursed to different degrees in some Member States compared with others, although there is no evidence that telecommunications sector overall has been adversely affected as a result of the Directive. The Commission will consider ways of providing consistent reimbursement for operators.

Ensuring proportionality in the end-to-end process of storage, retrieval and use: the Commission will ensure that any future data retention proposal respects the principle of proportionality and is appropriate for attaining the objective of combating serious crime and terrorism and does not go beyond what is necessary to achieve it. It will recognise that any exemptions or limitations in relation to the protection of personal data should only apply insofar as they are necessary. It will assess thoroughly the implications for the effectiveness and efficiency of the criminal justice system and of law enforcement, for privacy and for costs to public administration and operators, of more stringent regulation of storage, access to and use of traffic data. The following areas will be examined in the impact assessment:

- consistency in limitation of the purpose of data retention and types of crime for which retained data may be accessed and used;
- more harmonisation of, and possibly shortening, the periods of mandatory data retention;
- ensuring independent supervision of requests for access and of the overall data retention and access regime applied in all Member States;
- limiting the authorities authorised to access the data;
- reducing the data categories to be retained;
- guidance on technical and organisational security measures for access to data including handover procedures;
- guidance on use of data including the prevention of data mining; and
- developing feasible metrics and reporting procedures to facilitate comparisons of application and evaluation of a future instrument.

The Commission will also consider whether and if so how an EU approach to data preservation might complement data retention.

With reference to the fundamental rights ‘check-list’ and the approach to information management in the area of freedom, security and justice, the Commission will consider each of these areas according to the principles of proportionality and the requirement of foreseeability. It will also ensure consistency with the ongoing review of the EU data protection framework.

Next steps: the Commission will propose a revision of the current data retention framework, and devise a number of options in consultation with law enforcement, the judiciary, industry and consumer groups, data protection authorities and civil society organisations. It will research further public perceptions of data retention and its impact on behaviour. These findings will feed into an impact assessment of the policy options identified which will provide the basis for the Commission's proposal.