EUROPEAN COMMISSION

MEMO

Brussels, 8 April 2014

Frequently Asked Questions: The Data Retention Directive

Data concerning telecommunications traffic through telephone networks and through the internet is, to some extent, retained (stored) by telecommunication service providers for their own commercial purposes (e.g., for billing purposes). The Data Retention Directive seeks to harmonise certain aspects of national rules on such storage. It requires telecommunication service providers to store traffic and location data regarding fixed and mobile telephony, internet access, email and telephony, for a period of at least six months (and no more than two years), and to make it available on request to law enforcement authorities for the purpose of investigation, detection and prosecution of serious crime and terrorism.

Which types of data are being retained under the Directive?

The Directive requires telecommunications service providers to retain (store) traffic and location data generated or processed by service and network providers as a result of communications activities. It does not require or allow the retention of the content of the communications (it is therefore different from lawful interception or 'wiretapping'). The Data Retention Directive applies to the fields of fixed network telephony, mobile telephony, internet access, internet email and internet telephony. It requires service providers to retain those traffic data necessary for identifying the source (i.e. sender), destination (recipient), date, time and duration, type, equipment of communication, and, for mobile telephony, the location of the equipment.

How valuable is data retention for criminal justice systems and law enforcement?

Data retention takes place in most Member States. Member States have generally reported that retained data is very valuable, and in some cases indispensable, for preventing and combating crime, for protecting victims and for the acquittal of the innocent in criminal cases.

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. This data provides valuable leads and evidence in the prevention and prosecution of crime and ensuring criminal justice. Its 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.

Data retention enables the construction of trails of evidence leading up to an offence. It also helps to discern or corroborate other forms of evidence on the activities of and links between suspects and victims. In the absence of forensic or eye witness evidence, data retention is often the only way to start a criminal investigation. Generally, data retention appears to play a central role in criminal investigation even if it is not always possible to isolate and quantify the impact of a particular form of evidence in a given case.

How often do law enforcement authorities request access to retained data?

The volume of both telecommunications traffic and requests for access to retained data is increasing. The Commission received statistics on the volume of requests for access to retained data from 2008 to 2012. The volume of requests varies considerably from one Member State to the next[1]. Based on figures provided by 17 Member States, there were about 1.56 million requests for data in 2008 and, based on statistics from 12 Member States, there were about 2.66 million requests in 2012.. The most frequently requested type of data overall concerns mobile telephony.

What do national Constitutional Courts say about data retention and the Directive?

Constitutional courts in several Member States (Germany, Romania, the Czech Republic and to some extent Cyprus and Bulgaria) found national data retention laws to be unconstitutional. In no case did the courts rule that the Data Retention Directive is contrary to fundamental rights.

The German Constitutional Court did not consider data retention unconstitutional as such, but found the law transposing the Directive to be unconstitutional since it did not sufficiently limit the circumstances in which law enforcement authorities could access the data, and did not contain sufficient measures to protect retained data against breaches of confidentiality (data security).

The Romanian Court found the law transposing the Directive to be ambiguous in its scope and purpose, with insufficient safeguards, and found, against that background, the obligation to retain data for a period of six months to be unconstitutional.

The Czech Constitutional Court annulled the law transposing the Directive on the basis that, as a measure which interfered with fundamental rights, it was insufficiently precise and clear in its formulation.

Of these Member States only Germany so far has failed to transpose in a way that complies with its respective national court judgment.

[1] The statistics vary considerably in scope and detail. For instance, in the Czech Republic, Latvia and Poland the volumes included identical requests sent to each of the main mobile telephony operators.

What is the security and privacy impact of data retention?

Data retention constitutes a restriction of the right to privacy, and the Directive expressly states that national laws governing access to those data must respect fundamental rights as guaranteed by the European Convention of Human Rights (in particular Article 8 on the right to privacy). This means that this data cannot be accessed in an arbitrary manner without due reason (for instance, national rules on access to this data must comply with the principles of necessity and proportionality).

Telecommunications data are stored by companies for normal business purposes. They are not stored in police databases. Law enforcement authorities can only require access to data on a case-by-case basis and, in most Member States, only after a request has been made to a judge. Hence, there is no unlimited access to data by law enforcement authorities.

While no concrete examples of serious breaches of privacy have emerged under the Directive, data retention implies in itself a risk of a potential breach.

Is Data preservation (or quick freeze) an alternative to Data retention?

Data preservation and Data retention are two different criminal investigation tools. Data preservation, also known as 'quick freeze', is applied only from the moment a suspicion arises and a preservation order is issued with respect to a particular person. Data retention, on the other hand, is key to conducting investigations into events that took place prior to the moment a criminal suspicion arose. It guarantees the availability of historical data linked to the case under investigation.

Unlike data retention, data preservation does not guarantee the ability to establish evidence trails prior to the preservation order. For instance, it does not allow for evidence to be gathered on the movements of either victims of or witnesses to a crime.

Lawful interception, or 'wiretapping', is different from data preservation and data retention. Interception involves real time listening/reading into the content of conversations and exchanges between a target and his associates. It is not regulated by EU law.

What is the cost of data retention?

Operators have argued that the cost of complying with the Directive is very significant, although estimates provided by specific operators in terms of capital and operational expenditure vary considerably. There appears to have been no major impact on competition or retail prices for consumers.

A study carried out before the transposition of the Directive estimated the cost of setting up a system for retaining data for an internet service provider to be around €375 000 in the first year and about €10 000 in operational costs.

What happens to national legislation following the decision by the Court?

National legislation needs to be amended only with regard to aspects that become contrary to EU law after a judgment by the European Court of Justice. Furthermore, a finding of invalidity of the Directive does not cancel the ability for Member States under the e-Privacy Directive (2002/58/EC) to oblige retention of data.

For more information

Statement by Comissioner Malmström on the Data Retention Directive

http://europa.eu/rapid/press-release_STATEMENT-14-113_en.htm

2011 European Commission Evaluation Report on the Data Retention Directive:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF

Homepage of Cecilia Malmström, Commissioner for Home Affairs

http://ec.europa.eu/commission_2010-2014/malmstrom/index_en.htm

Homepage DG Home Affairs:

http://ec.europa.eu/dgs/home-affairs/index_en.htm