Volume 3 Issue 1 January 2006

Data Retention: Data Retention Directive: scope and obligation

The controversial Data Retention Directive received support from the European Parliament in December 2005. Karin Retzer, Of Counsel, in the Brussels office of international law firm, Morrison & Foerster LLP, summarises the most controversial issues of the Directive, namely the scope of the new obligations, the purposes of retention and access, retention periods, data storage obligations, and reimbursement of associated costs.

On December 14, 2005, the European Parliament adopted a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (Directive). Once formally approved by the Council, the Directive would require European Union Member States to introduce a data retention scheme compelling communications service providers to indiscriminately store and retain their clients’ communications data. This would include data necessary to follow and identify the source and the destination of every communication, the time the communication was made, the duration, the subscriber name and the communication device and equipment involved, including information on unsuccessful call attempts. The minimum storage period agreed by the Parliament is six months from the date of the communication; individual Member States may extend the time period up to twenty-four months. The data would subsequently be made available as needed to law enforcement agencies in the course of the investigation and prosecution of "serious criminal offences."

The Directive was strongly opposed by privacy advocates and service providers alike. Currently, communication data generated through communication services such as landline, mobile, and internet telephony, data text messaging, voicemail, call forwarding, instant messaging, paging, electronic mail, and other multi-media services, must be erased or made anonymous at the time the communication is completed, unless the information is needed for subscriber billing, interconnection payments, marketing, etc., or where national law requires the retention of certain information.

Due to the sheer magnitude of the data that must be retained under the new regime, the investment in equipment and technological expertise for retaining and accessing the data would be significant, and may result in increased communication costs for consumers. The Parliament's plenary session decided to strike out the provision in the
earlier Commission proposal requiring Member States to compensate providers for their increased costs, leaving it to the Member States' discretion to reimburse providers (or not). Also there are serious concerns about the invasion of privacy and data security. The Parliament's plenary session, however, decided to ignore these concerns and agreed with Member States that broad retention obligations were (supposedly) necessary for law enforcement and anti-terrorism investigations across Europe.

After briefly explaining the legislative context, the following summarizes the salient points, focusing on the most controversial issues of the Directive, namely the scope of the new obligations, the purposes of retention and access, retention periods, data storage obligations, and reimbursement of associated costs.

Background: the changing legal landscape

Data retention rules have evolved over the past decade, resulting in wide variations among the EU Member States. Some States do not provide for retention obligations, while others require telecom and Internet service providers (ISPs) to retain communications data for periods ranging from a few months to four years.

Formation of a Legal Framework.

The issue of communications data retention was first raised in the 1997 Telecommunications Privacy Directive which permitted but did not require Member States to impose retention obligations on telecom operators for law enforcement purposes. The rise of the Internet then prompted the Commission to replace the Directive with the 2002 Electronic Communications Directive, covering the entire electronic communications sector. The new Directive explicitly allowed EU countries to compel ISPs to record traffic and location data when "appropriate and proportionate within a democratic society to safeguard national security, public security, prevention of criminal offences etc or of unauthorized use of an electronic communications system."

Since then, EU law enforcement agencies have lobbied for broader and more harmonized retention schemes, particularly because mobile phone records were instrumental in tracking down the perpetrators of the Madrid bombings which killed 191 and injured approximately 1,800 people on 11 March 2004. In the aftermath of those bombings, the European Council issued the Declaration on Combating Terrorism (the Declaration) which among other things recommended the introduction of traffic data retention rules. The Council also updated the EU Plan of Action on Combating Terrorism (the Action Plan), which was first introduced in the wake of the terrorist attacks of 11 September 2001.
Member State Proposal for Framework Decision

In April 2004, France, Ireland, Sweden, and the UK put forward a joint proposal on data retention that sought to ensure that an extremely wide variety of communications data were retained by communication service providers for a period of time between 12 and 36 months in order to enable both the subsequent investigation of the communications data and to facilitate judicial co-operation "for the purpose of prevention, investigation, detection and prosecution of crime or criminal offences including terrorism." Essentially, any communications data required to identify and trace the identity, source, destination, routing, date/time, location, device used, etc. of a communication would have been covered. Content of the communication, however, would not have been covered by the proposal. Moreover, each Member State would be able to request another Member State to grant access to the retained data in accordance with the established procedures on judicial cooperation in criminal matters.

Rejection by Parliament

After reviewing the proposal by these four Member States, Parliament issued a resolution in September 2005 rejecting the proposed Framework Decision and calling on them to withdraw their initiative. According to a report issued by the Parliament's Committee on Civil Liberties, Justice, and Home Affairs (Civil Liberties Committee), the Member State proposal was flawed for three key reasons:

- The proposed regime derogated from both the Data Protection Directive and the Electronic Communications Directive, and amendments must be made via a directive (as opposed to a Framework Decision);

- The proposed measures were neither appropriate nor necessary and were unreasonably harsh towards those who must bear the burden of data retention; and

- The proposed blanket retention was incompatible with Article 8 of the European Convention of Human Rights (ECHR) as it was neither consistent with the rule of law nor necessary in a democratic society, Member States did not have unlimited discretion to subject individuals within their territory to clandestine surveillance."

Commission Initiative

After the Member State proposal was rejected by the Parliament, the Commission decided to develop in close collaboration with the Parliament a directive that would harmonize Member State data retention rules to ensure that the data is available to investigate, detect, and prosecute serious crimes under Member State law. The proposed Directive was then submitted to the Council and to the
Parliament for approval.

In October 2005, the Article 29 Data Protection Working Party, a body created by the Data Protection Directive (95/46/EC) to examine and provide rather critical opinions to the EC on issues relating to data protection law at EU and national levels, issued Opinion 113/2005, criticizing the draft Directive.

After considerable debate and compromise between the socialist PES and the conservative EPP parliament groups, Parliament approved multiple amendments to the proposed Directive on December 14, 2005 at first reading by 387 votes in favor to 204 against.

To become law, the draft Directive is now awaiting approval by the Council. The Council must decide with a qualified majority. However, as the final text approved by the Parliament was negotiated beforehand with the Council in informal meetings prior to the Parliament's plenary vote, approval by the Council is likely. Member States must adapt national laws within eighteen months after the publication of the final text in the Official Journal.

The scope

The Directive, in its final version covers "...providers of publicly available electronic communications service or of a public communications network..." (Article 3.1). As a result, all telecommunication and Internet service providers within Member States' jurisdiction as well as, arguably, employers providing employees with internet access, must store communication data.

While a new amendment to the Directive clarifies that the Directive is not applicable to data revealing the content of communications, the Directive does cover a wide variety of data, including data required to identify and trace the identity, source, destination, routing, date/time, location, device used, etc. of a communication. The categories of data that must be retained should be revised on a regular basis.

The Directive as amended by the Parliament also requires retention of data on unsuccessful calls, defined as "a communication where a telephone call has been successfully connected but is unanswered or there has been a network management intervention." (Article 2(2)). This was a controversial provision because providers do not currently register lost calls for billing purposes and so to do this will require using new technologies and will be expensive. The Civil Liberties Committee had suggested making it optional for organizations to keep data about incomplete calls.

Internet related data to be retained is limited to email and IPtelephony data - which means that no data on web pages visited will need to be
Circumstances for access to retained data

The aim of the Directive is to ensure that the data is available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The Civil Liberties Committee commenting on the draft had suggested a specific list of serious crimes in the investigation of which retained data could be used. The Parliamentary plenary session, however, voted against a definite catalogue to allow for greater Member State flexibility. In this respect it is interesting to note that content owners have unsuccessfully lobbied hard to have the Directive require retention of data for criminal offenses other than "serious" crimes, presumably so that law enforcement agencies could use retained data to prosecute violators of intellectual property law. Those requests were rejected, but, depending on the scope of Member States' definition of "serious crime," the distinction in the wording of the directive may be irrelevant.

Further, Member States must ensure that data retained in accordance with the Directive are only provided to the competent national authorities, in specific cases and in accordance with national legislation (push-system).

Retention period

The Directive obliges each Member State to ensure that the relevant data is retained "...for a period of not less than 6 months and for a maximum of two years from the date of communication" (Article 7). A new clause has been introduced by the Parliament permitting derogation from the time period for particular circumstances warranting an extension for a limited period of the maximum retention period.

Data storage

A new provision introduced by the Parliament states that each Member State shall ensure that communication service providers respect, as a minimum, certain prescribed data security principles with respect to data retained. There is a provision for "effective, proportionate and dissuasive" penal sanctions for companies who fail to store the data or misuse the retained information, and Member States must designate an independent supervisory authority to ensure compliance with the Directive, which "may be the same authorities as those referred to in Article 28 of Directive 95/46/C." Hence, the data protection authorities may assume supervisory authority for compliance with the implementation legislation of this Directive as well.
Storage should allow for sharing with law enforcement authorities without delay. However the technical implications will need to be defined in the implementation legislation. Data must be destroyed after the period of retention, except for those data that have been accessed and preserved.

Reimbursement of costs

The Parliament decided to delete the provision in the Commission proposal that mandated Member States reimburse providers for additional costs of retention, storage and transmission of data, stating in recital 13: "Given the fact that retention of data generates significant additional costs for electronic communication providers, whilst the benefits in terms of public security impact on society in general, it is appropriate to foresee that Member States reimburse demonstrated additional costs incurred in order to comply with the obligations imposed on them as a consequence of this Directive."

The Parliament's Civil Liberties Committee had also called for full reimbursement of all costs. Communications service providers are disappointed by the Parliament's attitude to cost reimbursement, as the cost of implementing a data retention capability is estimated to run to millions of euros.

Karin Retzer Of Counsel
Morrison & Foerster LLP
kretzer@mofo.com


2. The 25 Member States of the European Union currently are: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, the Netherlands, and the United Kingdom.