Evaluation of Directive 2006/24/EC; reply from Sweden

General

The issue of data retention is politically sensitive in Sweden because of its implications on the protection of privacy. This has meant that there is a delay in the timetable for transposition of Directive 2006/24/EC. At present work is under way in the Ministry of Justice on the drafting of a bill to the Parliament. It is not clear at this moment when the bill will be submitted to the Parliament.

1. Application of Directive 2006/24/EC

Due to the situation described above, Sweden will unfortunately not be able to contribute to this evaluation with qualitative or quantitative answers regarding the application of Directive 2006/24/EC.

The current Swedish system (legislation enclosed) regarding access to traffic data is as follows:

There is today no obligation for telecommunication companies to store traffic data. In line with Directive 2002/58/EG, the principal rule is that traffic data shall be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. However, the telecommunication companies are allowed to store traffic data for other purposes such as for example subscriber billing and interconnection payments (see chapter 6, Law (2003:389) on electronic communication). When such data is stored, crime fighting authorities can gain access to the data by using two different channels:

1) By a court decision issued under the Swedish Code of Judicial Proceeding (chapter 27). The qualifications for such a decision is that someone is reasonably suspected of an offence for which a less severe
sentence than six months imprisonment is not prescribed, and the measure is of exceptional importance to the inquiry.

2) By asking the telecommunication company according to the Law on electronic communication (chapter 6, section 22). The telecommunication company storing the data will be obliged to hand out the information if the offence being investigated does not prescribe a less severe sentence than two years imprisonment. If the authorities ask only for data necessary to identify the subscriber, the offence being investigated has to prescribe a sentence of imprisonment and the authority has to estimate that a sentence other than a fine will be imposed.

During 2007, approximately 1300 decisions described in 1) were made and around 9500 requests described in 2) were issued.

With the current system, the telecommunication companies are compensated for their costs relating to each demand from the authorities, but are not compensated for costs related to storing, security etc.

1.B Measures on identifying buyers of prepaid SIM-cards

There is no work ongoing within the law enforcement services with a view to register persons that buy prepaid SIM-cards. The experience of the National Police Board is that criminals use prepaid cards in order to make it difficult or impossible for the Police to establish the identity of the user.

Establishing the identity of a user requires a series of measures such as applying the Law on electronic communication (see above), control of communication at connection points, and IMEI-searches. On the basis of this information, the user may be identified. This type of work is carried out in connection with criminal investigations and in co-operation with criminal intelligence units in which analysts have the capacity to analyse and compare a large amount of information.

The added value of introducing mandatory registration of buyers of prepaid SIM cards is questioned particularly since such a registration is very easy to circumvent.