



GSME POSITION ON DATA RETENTION – IMPLICATIONS FOR THE MOBILE INDUSTRY

23 August 2005

GSM Europe, representing 148 mobile operators in Europe, fully recognises the importance of the fight against terrorism. Our members already have a long track record of cooperating and working with law enforcement agencies (LEAs) to conduct this fight. However, while LEAs have voiced a need for mandatory data retention requirements across the EU, there is still a lack of a clear and in-depth analysis of the benefits and the costs these proposals would have on society and industry, as well as the consequences for citizens and personal integrity. In the interests of better regulation, GSME believes that existing legal measures and the possibilities there within for cooperation between industry and LEAs should be further examined before another layer of regulation is introduced.

Summary

- Data retention obligations have far reaching implications for citizens, industry and society. Any EU-initiative must therefore be preceded by a proper impact assessment of the costs and likely benefits to society to ensure that the correct balance is struck. Needs should be justified by clear evidence.
- To ensure a proportional policy in terms of the fundamental rights involved and the costs incurred to society, the application scope must – as originally provided for by the Council of Ministers – be clearly and strictly defined. This will provide legal certainty to the industry. In that respect, the European Commission ideas would seem more in line with these objectives.
- The cost of fighting crime should be borne by society, not private companies operating in a competitive market. Should there be a data retention instrument at EU-level it must be accompanied by a clear obligation on Member States to compensate operators fully for the additional costs incurred. Not only will this regulate demand, but it will also safeguard a level competition field for the whole industry.
- Any EU-wide data retention obligations must be based on the principle that only data already processed and stored for billing, commercial and any other legitimate purposes be retained. Any requirements that go beyond this will have severe technical and financial implications and result in legal uncertainty for the industry.

GSM Europe

Diamant Building, Bd A. Reyers Ln 80, B- 1030 Brussels
Tel: +32 2 706 81 04 Mobile: +32 472 29 38 58 Fax: +32 2 706 81 08
Email: kwalravens@gsm.org Web: www.gsmeurope.org



- In this respect, current discussions on types of data to be retained raise severe problems for the mobile industry, notably as regards location data, unsuccessful call attempts, information on the service used, identification of prepaid users and International Mobile Equipment Numbers (IMEIs). As GSM technologies are being rapidly enhanced, new types of communications are arising, some of which are difficult to generate records for and to store. Their value in a law enforcement investigation has yet to be assessed.

1. Data retention must be proportionate, effective and strictly scoped

GSME strongly recommends the undertaking of an impact assessment of data retention obligations imposed on industry and on their efficiency and effectiveness. To our knowledge, this has not been undertaken to date. This has been due in part to a considerable uncertainty as to what sorts of records were actually of value to investigating officers in all EU Member States. Such an impact assessment is key to ascertaining the proportionality and necessity of any measure taken. Particularly it is necessary to keep in mind that the value for crime prevention purposes of any records retained is likely to be limited by the fact that criminals are already able, through simple means, to reduce the risk of being associated with traffic data records. These means include switching to services where data are held in a jurisdiction over which a particular member state has no immediate control or using public telephone boxes.

The uncertainty is also a result of technological changes that are currently revolutionising the communications industry (GSM technologies being enhanced with GPRS, UMTS, WLAN and other advanced IP technologies). This is heralding the creation of new types of communications, for which records are difficult to generate and store. Their potential value in a law enforcement investigation has, moreover, yet to be assessed. The new flat-rate IP-based services are good examples of this enhancement.

To ensure a proportional policy in terms of the fundamental rights involved and the costs incurred to society, the application scope must – as originally provided for by the Council of Ministers – be clearly and strictly defined. This will ultimately provide legal certainty to the industry. In that respect, what we understand of the European Commission ideas seems more in line with these objectives.

2. Financing the demand for data regulation will regulate it

While cooperating to the fullest with LEAs and recognising society's need for adequate instruments in fighting terrorism, GSME and its members are of the firm view that the necessary costs to combat crime should be borne by society, not private companies operating in a competitive market. Not only will this regulate demand, but it will also safeguard a level playing field for the whole industry.

GSM Europe



Any data retention instrument on EU-level must be accompanied by a clear obligation on Member States to compensate operators fully for all the additional costs incurred, both for investment and running costs.

Merely stating that Member States should undertake appropriate contribution is not enough - this would only create uncertainty for market players while distorting competition as different companies will be subject to different national schemes.

3. Scope, types of data retained: technical and administrative issues

In our understanding, the current discussions in the Council on the types of data to be retained go beyond the earlier idea that retention obligations should only apply to such data that can be generated and processed without additional investment for industry, i.e. data necessary for business and billing purposes. Any obligation to retain data must in any case be limited to a minimum. It must not include data types currently not centrally processed and recorded within the networks – i.e. data already processed and stored for billing, commercial and any other legitimate purposes. In this respect it is worth mentioning that there are about 366 million mobile subscribers across the EU Member States generating billions and billions of records every day. Only in the UK in March 2005, 2.75 billion SMS were sent person-to-person and more than 1.6 billion WAP pages were viewed.

Retaining data not used for legitimate business purposes is governed by the very narrow provisions of Article 15 of the Directive on privacy in electronic communications. There are also important technical, financial and administrative issues to be considered and GSME feels that many aspects have not been sufficiently addressed:

- Unsuccessful call attempts

Call Data Records (CDR) are usually only generated and retained for successful call set-ups. If mobile operators were required to retain data also for unsuccessful call set-ups (which comprise about 40% of the total amount of call set-ups) as currently discussed in the Council, this would have a significant impact on costs due to the extensive technical upgrades of the network and the storage hardware.

- Information on the service used

GSME is also concerned about the requirements to store the type of communication used. For the majority of cases such as voice and fax services, information on which service that was used is not retained in the operator's network. This type of data is only recorded if needed for billing purposes, e.g. when a subscriber sends an SMS. Again, making this data available would require many operators to make significant investments in hardware and software, and huge volumes of data would have to be stored and evaluated

GSM Europe



It should also be pointed out that as operators move to IP-based services, the type of communication becomes even more difficult to identify and trace – services will consist of ‘anonymous’ packets of data going through the IP-network without the operator keeping track of the service used. Retaining information on the type of communication used in these cases will be close to impossible.

- Cell ID and location data during and at the end of a call

The draft Framework Decision does not distinguish between traffic data and location data. This is in contrast to the Directive on privacy in electronic communications which applies a stricter regime to location data. For example, operators are required to block any processing of location data for each connection to the network or for each transmission of a communication. GSME finds that the discrepancy between the Directive on privacy and the data retention discussions creates legal uncertainty, as mobile operators could be required to retain location data despite the fact that our customers have requested to block the processing for privacy reasons.

We must also draw attention to the fact that data on Cell ID during and at the end of a call are not retained or processed when they are not necessary for billing purposes. Again, starting to record this information would entail considerable investments in mobile operators’ networks to upgrade the switching units necessary to record each individual Cell-ID throughout and at the end of a call and to transmit them to the data center as well as the costs for storage and evaluation

LEAs have not yet proven Cell-ID data provides any added value: the retention of the cell ID at the beginning and – if available - at the end of every call already suffices to establish a movement profile. It is doubtful whether the potential added value of the information obtained can justify the financial burden imposed on industry investment costs that would be required

- International Mobile Equipment Number (IMEI)

Given that operators would be required to retain the telephone number in order to identify the user, retention of the IMEI would seem unnecessary. Many operators do not retain such data and so a future requirement to retain them would incur further investment costs. It is also doubtful whether IMEIs can be used to noticeably improve the fight against crime, since these are IDs that can be multiply assigned by manufacturers and can be manipulated by users with the result that subscribers cannot be clearly identified by means of an IMEI. This is also the reason why network operators/service providers do not identify a subscriber at login using the IMEI.

GSM Europe



- Parties obliged to perform data retention

Any proposal for data retention requirements must make it clear that only the party offering the respective service can be subject to the data retention obligation. This party is the only one in a direct relationship with the customer and with sovereignty over the data. Besides, it cannot be the duty of one company to collect data even from other providers for the LEAs.

As regards security, if more stringent requirements are introduced than are currently applied by operators as part of their regular business processes, this will have a cost increasing effect. In some countries, specific requirements already apply to data that is generated by providers under lawful interception obligations.

GSM Europe

Diamant Building, Bd A. Reyers Ln 80, B- 1030 Brussels
Tel: +32 2 706 81 04 Mobile: +32 472 29 38 58 Fax: +32 2 706 81 08
Email: kwalravens@gsm.org Web: www.gsmeurope.org