



translated from German (original version)

Demands of German Industry for the Debate About a European-Wide Compulsory Data Retention

BACKGROUND:

For more than a year now the issue as to whether and to what extent telecommunication operators and internet service providers should be obliged to store traffic and location data as well as subscriber and user data for possible use by Law Enforcement Agencies ("LEAs") has been discussed in a controversial debate. In the aftermath of the terrorist attacks in Madrid on 11 March 2004, France, Great Britain, Ireland and Sweden submitted a joint proposal for an EU framework decision on the retention of communication data in April 2004¹. As a consequence of the bomb attacks in London in July 2005, the Justice and Interior Ministers of the European Union recently announced to reach an agreement on regulations for the retention of communication data and their exchange between Member States by October 2005².

Besides general points of criticism, the European Parliament as well as the Commission have expressed considerable doubts concerning the Council's legal competence to regulate the matter (within the so-called "third pillar" based on Art. 31 Section 1 c, Art. 34 Section 2 b TEU). The European Commission is currently working on a draft directive based on Article 95 TEC. So far, an agreement among the institutions on the appropriate legal basis has not been achieved.

With regard to the parallel discussions about different legal instruments in different legislative proceedings, the present paper offers a contribution both for the current work in the Council of Ministers as well as in the Commission.

BASIC POSITION:

Industry strongly supports the endeavour to find adequate solutions to combat cross-border organised crime and terrorism. Internal security serves the common good and therefore benefits any industrial location. However, industry has considerable doubts whether the benefits of the intended storage requirements are in due proportion to the high cost burdens for industry and the affected basic rights of EU-citizens.

¹ Council Document 8958/2004: Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism.

² Press statement of the JI Council of 13 July 2005: http://ue.eu.int/ueDocs/cms_Data/docs/pressData/en/jha/85703.pdf .

Industry would like to point out that the European Union is confronted with a crisis of acceptance and a loss of confidence because politicians are too often unable to explain the purpose and benefits of European Union activities to citizens and industry. The concerns and uneasiness associated with data retention also result from the fact that a solid and adequate impact assessment has not been carried out, giving rise to the impression that neither the concerns of consumers nor those of industry seem to be addressed seriously.

The measures currently discussed in the Council and within the Commission by far exceed the demands of German LEAs as expressed in expert talks held at the beginning of this year, both with regard to the types of data to be retained and to retention periods. Even the European Confederation of Police (EuroCOP) has dismissed the draft of the Council, claiming it would take too long to search the presently expected records and noting that numerous possibilities to circumvent question the effectiveness of any data retention regime altogether (<http://www.enn.ie/news.html?code=9611167>). A study commissioned by the German Association for Information Technology, Telecommunications and New Media (BITKOM) likewise showed that LEAs hardly ask for data that are older than three months (http://www.bitkom.org/Default_28861.aspx).

Considering this, any obligation to retain data must in any case be limited to a minimum standard. It must not include data types currently not centrally processed and recorded within the networks. Apart from that, any retention period must not exceed six months.

In any case must the Member States bear 100 % of all initial investment and operational costs incurred by industry for the implementation and operation of any retention measures. For this very reason, it is in the interest of the Member States to scrutinize in detail every proposal (retention period as well as each specific data type) for its effectiveness and necessity as opposed to being a mere cost driver.

RECOMMENDATIONS OF INDUSTRY IN DETAIL:

1. Agreement on the legal basis

Disputes among the EU institutions about their competences and responsibilities will lead to legal uncertainty and possibly to “sunk investments“ for those concerned. Therefore, the EU institutions – also with regard to their credibility – are called upon to solve their dispute about the correct legal basis in the near future and only then continue with any further material discussion.

2. Performance of legal impact assessment

The Commission has committed itself to accomplishing a thorough impact assessment before adopting specific regulation. This is the only reliable means to evaluate the consequences for industry and consumers and to analyse if and to what degree a European data retention regime helps to ensure effective police and judicial co-operation. This preliminary work has not yet been done. In particular, LEAs have demonstrated neither the concrete need for a data retention regime nor the alleged lack of effectiveness of the current practice. This analysis must urgently be made up for if the promises of "better regulation" and "impact assessment" are to be taken seriously with regard to the issue of data retention.

In this context, basic rights as guaranteed by the constitutions of the Member States have to be taken into account. In Germany, the adjudication of the German Federal Constitutional Court (Bundesverfassungsgericht) sets extremely narrow limits for blanket data retention. Just recently, the Court³ has underlined the outstanding importance of both the secrecy of telecommunications as well as the right to informational self-determination. It pointed out that these civil rights could only be restricted under very limited premises.

3. Personal scope (obligated party): Limitation to the provider of the particular service

Any data retention legislation must explicitly clarify that a storage obligation can and may only be imposed upon the provider that offers the particular service employed by its user. Only this provider has the specific customer relationship and thus the authorisation over the data to be retained. Therefore, any obligation to make information available about the recipients of a call or a data transmission cannot be met by the provider of the person calling or sending data, because the recipient may be a customer of a different service provider. Such obligations must not be part of any data retention regime.

4. Material scope (types of data to be stored): Limitation to a minimum standard

Comprehensive mandatory data retention can lead to enormous investment and operational costs especially with certain types of data that are not – and, for legal reasons, must not be – stored at present and are therefore currently not even recorded and processed within the networks. Accordingly, generation and storage of these types of data would require costly technical upgrading. Clear limits are necessary, as only a carefully limited material scope can lead to an appropriate and adequate solution. This evaluation process must be guided by the actually proven need of LEAs.

The Council and the Commission have emphasised that only such data are to be retained that can be processed and stored without additional effort for the industry. In order to limit extra costs, the regulations would thus merely require companies to extend the retention period of data already processed and stored for other reasons. However, this approach is not in line with the types of data now discussed by the Council and the Commission. Many of the types of data discussed are

³ BVerfG, 1 BvR 668/04 vom 27.7.2005.

currently not recorded, let alone processed, in networks, e.g. because they are not necessary for service performance or billing purposes and their storage is therefore prohibited under present data protection law. The issue here is not simply to extend the retention period of data already processed and stored for other reasons, but extensive hardware and software upgrades would be required in order to generate and make these data available within the networks in the first place.

German industry therefore advocates the following specific limitations regarding the material scope. Discussions with German LEAs have made it clear that German LEAs themselves do not consider the following types of data necessary for an effective prevention and prosecution of crimes (see the “German List” submitted to the Council Working Group).

All types of communication:

- No storage of unsuccessful connection attempts
Reason: The storage of these data is prohibited under present data protection law because they are not necessary for billing purposes. These data are therefore currently not even processed or recorded by the networks. In order to make these data available on the networks, companies would have to rebuild all switching centres fundamentally. The resulting costs to the industry would be within the three-figure million Euro range exclusively for this type of data. To date, LEAs have not been able to prove the need for this information in light of these substantial costs.
- No storage of the type of communication used (e.g. voice, fax etc.)
Reason: This information is recorded within the network only if it is relevant for billing purposes (e.g. in the case of an SMS). In most cases (e.g. whether a connection was used for voice or fax transmission), the data are not available within the network. Making them available would require substantial technical upgrading.

Mobile communications:

- No storage of cell ID during or at the end of a call
Reason: These data, as well, are currently not recorded or processed within the networks because they are not necessary for billing purposes. Recording these data would also require substantial technical upgrading. LEAs have not yet proven an added value, as the retention of the cell ID at the beginning of every call already suffices to establish a movement profile. Apart from that, there is no justification to oblige companies to supply “data mapping”, i.e. a specified geographic description of the cell, with each cell ID. Instead, it suffices that LEAs are enabled to gather this information from a pre-submitted list.
- No storage of the IMEI (communication device number)
Reason: The added value of IMEI retention in addition to the telephone number in order to identify a user clearly is questionable and has not been demonstrated. For this very reason, German LEAs departed from requesting IMEI data during expert discussions held in Germany.

Internet:

- No storage of communication data of the internet services used

Reason: Communication data of the internet services used (e.g. who retrieved whose website or sent whom an email?) are not available for most services. Technical facilities to record, retain, and analyze these data would first have to be created and would lead to a tremendous rise in the volume of data to be stored. This is true even with a limitation to the two services email and VOIP (Voice Over Internet Protocol).

Storage of websites retrieved would also reveal the content of the communication (because it reveals what the user has looked at). This conflicts with the assertion by the EU institutions that an interception of the content of communication should not be part of any data retention scheme.

Since LEAs have so far always emphasized the fact that internet access data (who participated when and with what IP address in internet traffic) are their most important information, a data list should be limited to the retention of this type of data.

- No storage of MAC or any other device number

Reason: The device numbers of the network card of a computer (MAC) are, in contrast, e.g., to an IP address, not even transmitted to the service provider. In order to change this, it would be necessary to reform the internet protocol and the entire infrastructure. At the same time, the added value of a MAC, in addition to an IP address, with regard to a clear identification of the user is questionable and has not been demonstrated.

5. No storage period over six months

A legal framework that takes into account the requirements of LEAs and the costs involved requires a restrictive approach to storage periods. Specific research in this area (see the above-mentioned study, accessible from http://www.bitkom.org/Default_28861.aspx) has shown that retention periods of over six months are not necessary. Any retention period exceeding six months would therefore be clearly disproportionate.

6. Comprehensive financial compensation of industry by Member States necessary

Ensuring internal security is a core state function which the state has to finance with public budget funds. Therefore, the state must also bear the cost of any data retention. A legal regulation at the European Union level must oblige the Member States to compensate industry for these costs. To this end, a demand for "appropriate" compensation is not sufficient. Instead, it requires a clear wording that expressly mandates full and complete (100%) compensation both for the investment and the operational costs. Inadequate and non-uniform compensation systems within the European Union would otherwise distort competition, endanger long-term competition structures, and prevent the creation of a uniform European internal market. This is especially true in light of the fact that some Member States have already established or announced compensation schemes while others have not.

7. No additional obligation for companies to provide statistics

New mandatory data retention would considerably burden the industry even if the necessary limitations – described above – are implemented. Companies would have to adapt numerous operational processes that would involve substantial investment and operational costs. Under no circumstances must there be additional obligations such as the obligation also discussed to provide statistics on the information required by LEAs. Tasks like this can be performed just as well by the competent authorities themselves. Only they can demonstrate in which cases the information gathered from data retention actually led to successful investigation, an insight that is necessary to assess the effectiveness of any data retention. There is absolutely no justification here to call on the private sector to carry out state tasks.

Apart from that, a post-evaluation is not suitable to correct any misjudgement by the legislator as to the effectiveness and proportionality of a data retention regime, because the necessary investments will already have been made at that point in time.

Berlin, 4th August 2005

Contact details:

Bundesverband der Deutschen Industrie e.V. (BDI)
(Federation of German Industries)
Christiane Eichele, Dept. Energy Policy and Telecommunications Policy
Breite Straße 29, 10178 Berlin, Germany
Tel.: +49 - 30 - 2028 1419
Fax: +49 - 30 - 2028 2419
E-Mail: C.Eichele@bdi-online.de

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM)
(German Association for Information Technology, Telecommunications and New Media)
Dr. Volker Kitz LL.M. (NYU), Head of Dept., Telecommunications and Media Policy
Albrechtstraße 10, 10117 Berlin, Germany
Tel.: +49 - 30 - 27576 221
Fax: +49 - 30 - 27576 222
E-Mail: V.Kitz@bitkom.org

Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e.V. (VATM)
(Association of Telecommunications and Value-Added Service Providers)
Harald Geywitz, Head of Berlin Office
Albrechtstraße 12, 10117 Berlin, Germany
Tel.: +49 - 30 - 50 56 15 38
Fax: +49 - 30 - 50 56 15 39
E-Mail: berlin@vatm.de