



International Chamber of Commerce

*The world business organization*

## Policy statement

### **EU Proposals for Data Retention for Law Enforcement Purposes**

*Prepared by ICC's Commission on E-Business, IT & Telecoms*

#### **Background**

For more than a year, the issue as to whether and to what extent communication service providers (CSPs) 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. This debate has included the release of several draft Framework Decisions by the Council of Ministers since April 2004 and the most recent effort by the European Commission to broker a compromise proposal in the form of the Commission's draft Directive. We recognize that the most recent terrorist events and threats in London have accelerated debate of both the retention issue and the drive for a Europe-wide legislated framework. This present paper reaffirms ICC's past statements on the issue of mandatory data retention in Europe and contributes to the work before all European institutions as they consider the proposed Directive.

As we stated in our 18 November 2002 position on Storage of Traffic Data for Law Enforcement Purposes<sup>1</sup>, business remains committed to cooperating with law enforcement to effectively combat crime in a manner consistent with business realities in a competitive, dynamic market and according to legal requirements. However, ICC continues to be concerned that differing national policies on mandatory data retention within Europe will create disadvantages for CSPs operating in countries with more far-reaching requirements and an impossible compliance burden for CSPs with operations in many different countries. A harmonised approach has to balance the needs of LEAs with business and user interests in an adequate, effective and fair way. ICC's comments in this context do not mean to interfere with the ability of CSPs to respond to requests from judicial authorities to release or preserve information for other purposes.

ICC welcomes the vote of the Parliament's Civil Liberties, Justice and Home Affairs Committee on Mr Alvaro Report which considerably improves the initial Commission proposal. Nonetheless, ICC remains concerned that further important clarifications are still needed, particularly regarding the scope of data retention measures. Too long retention periods have also been introduced, particularly for data related to Internet traffic. Retaining traffic data for longer periods will only produce more data volumes, without increasing the quality of information.

---

<sup>1</sup> <http://www.iccwbo.org/policy/ebitt/id2341/index.html>

International Chamber of Commerce

38, Cours Albert 1er, 75008 Paris, France

Telephone +33 1 49 53 28 28 Fax +33 1 49 53 28 59

Web site [www.iccwbo.org](http://www.iccwbo.org) E-mail [icc@iccwbo.org](mailto:icc@iccwbo.org)

ICC also welcomes the recognition by the members of the Civil Liberties Committee of the need for cost reimbursement for obligations through a data retention regime.

At the same time, ICC is concerned that EU Ministers of Justice last week, while improving the Commission's proposal on some of the technical aspects, did not acknowledge the specificities of the online world and underestimated the technical, social and economic consequences of retention of Internet data. In addition, Ministers failed to recognize the need for cost reimbursement which is vital to the European competitiveness.

### **Recommendations**

ICC urges that the EU Institutions, in their review of the Commission proposal, continue to engage industry in recommending a framework that recognizes the following key points:

- The Council has emphasised that only such data types are to be retained that can be processed and stored without additional effort for industry. However, this approach is not in line with the types of data now discussed by the Council and the Commission. As telecommunications operators already collect and disclose a multitude of the data demanded by LEAs, this raises the fundamental question whether the demand for 'new' types of data – not at any specific point of time and beyond what is needed for business purposes recorded for billing purposes - is reasonable. Comprehensive mandatory data retention can lead to enormous investment and operational costs especially with certain types of data. The issue here is not simply to extend the retention period of data 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. For instance, the proposed retention of email traffic data (subject header, sender/recipient) would represent a major departure from existing business practices. Many CSPs do not presently retain even a week's worth of email traffic data originating on their network for business cases. Industry therefore additionally advocates the following specific limitations regarding the scope of any legislation:

All types of communication:

- No storage of unsuccessful connection attempts
- No storage of the type of communication used (e.g. voice, fax etc.)

Mobile communications:

- No storage of cell ID during or at the end of a call
- No storage of the IMEI (communication device number)

Internet:

- No storage of communication data of the internet services used
- No storage of MAC number (device numbers of the network card of a computer)

- A legal framework that takes into account the requirements of LEAs and the costs involved requires a restrictive approach to storage periods. Telecommunications operators collect and disclose a multitude of the data presently demanded by LEAs. Therewith longer retention periods for these types of data would already lead to an additional financial burden for operators as, for example, existing databases (storage and searching tools) would need to be expanded and adapted. In addition, research in this area has shown that a 3-6 month retention period already covers the majority of public authorities' current requests. Any retention period exceeding six months would therefore be clearly disproportionate.
- Laws which already exist in some Member States differ greatly both in the durations and definitions of data to be retained, and a European framework should harmonize national laws on both key issues. Therefore, the main object should be to harmonize legislation at the lowest level (shortest retention duration, limited data types). If this is not possible, sufficient flexibility is needed for Member States to implement less restrictive legislation. EU legislation in this case should serve as a limitation to the top. Any duration established should act as a ceiling supported by the demonstrable need of law enforcement, and a harmonized data definition must be sufficiently flexible to assimilate next generation communications services.
- A pan-European cost reimbursement scheme is a necessary component to any retention framework, to cover investment and operational (retention and search) costs beyond industry business cases and to safeguard the privacy rights of individuals. Without full reimbursement, the costs of retention to industry will drive up the costs of services, affecting the global competitiveness of the European CSP sector and the Single Market.
- Access by law enforcement agencies to data retained must continue to be limited to criminal investigative, prosecution and enforcement purposes, under a clear process to achieve the requisite authority. CSPs acting in conformance with a valid request for access to retained data should not be subject to liability for provision of such information.
- Recommendation for the EU to continue to permit data preservation – the retention of data for a specific case and for a finite period – to be favoured by national governments as the preferred method for investigative cooperation. Targeted data preservation is not only less costly and burdensome to business and less damaging to public confidence in communication networks, but it also serves law enforcement's investigative objectives in a more straightforward and efficient way, as accorded in the Council of Europe Convention on Cybercrime.

Although many technical and legal questions still remain unclear with regard to the demands and specifications received from the Council and Commission, we can now see that the cost consequences of the proposals are very important. It can, after a first assessment, note that the proposed data retention procedures would lead to a tremendous increase in data volumes that have to be handled by telecom operators. Such volumes are estimated in the best case to be equal to or in excess of the volumes handled by the largest known data warehouses in the world, and in the worst case over 50 times more data than what is being stored at the present time. (It is estimated that, for a medium sized operator, the investments required would amount to more

than EUR 100 Mln, with the yearly running cost of EUR 30-40 Mln. Therefore, governments must ensure full cost compensation to the operators).

It is also to be noted that the proposals have wide-spread consequences for personal privacy for all users of electronic communication services. This risks hurting customers' confidence and reduce their willingness to use new e-services.

### **A more thorough analysis is needed**

ICC wishes to point out that the present data retention proposals lack a deeper and more comprehensive analysis of the consequences and ICC therefore welcomes a dialogue between the European authorities and the European industries. Information needs to be exchanged for a more thorough analysis of the advantages and disadvantages and the political decision-making process needs to clearly understand the consequences for society and industry. To safeguard commercial operations ICC calls for clarification regarding:

- LEA requirements and technical issues
- What responsibility operators have for the quality of processed data
- What value this data will have in terms of evidence; high value means high backwards traceability
- If processed data was proven to be false – who is to blame
- Quality assurance and integrity of data
- Cost compensations and harmonisation of obligations
- How easy is it, especially with regard to IP-communications, to evade the proposed data retention measures by those who wish to do so?

### **Conclusion**

ICC is horrified at recent terrorist attacks in London, which echo the terror of the Madrid and 9/11 attacks in the United States. However, in the context of this debate, we again counsel caution. As in 2002, our comments on mandatory data retention in Europe are not an endorsement of mandatory retention as a concept, but recognition that there is a way to safeguard business and consumer interests while continuing effective investigative co-operation with LEAs. As we stated in 2002, any traffic data storage requirements imposed by governments should be focused, narrow, publicly funded, limited to the measures absolutely necessary to protect society, and balance the interests of government, business and users. We commend these comments to your review and look forward to a continued public dialogue as the Parliament considers the current Commission proposal.

\* \* \* \* \*

12 December 2005  
Doc. 373/468