UNICE
THE VOICE OF BUSINESS IN EUROPE

COMMENTS

31 October 2005

PRELIMINARY UNICE COMMENTS ON DATA RETENTION

BACKGROUND

Over the past year, there has been a controversial discussion about imposing obligations on telecommunication operators and Internet Service Providers ("(ISP") to store end-user traffic data for possible use by Law Enforcement Agencies ("LEAs"). In the aftermath of the 11 March 2004 terrorist attack in Madrid the French Republic, the United Kingdom, Ireland and the Kingdom of Sweden presented a joint proposal for a "Framework decision on the retention of communications data" in April 2004 [1]. Such discussions are not new and follow from the first proposal for data retention which started more than five years ago in the context of the Cyber Crime Convention of the Council of Europe and the revision of the telecommunications data protection Directive.

The new Council-proposal aims to improve cross-border judicial cooperation between Member States to combat criminal offences, in particular organised crime and terrorism, by introducing European-wide harmonised rules on the retention of data that is generated, processed and stored by suppliers of public communication networks or publicly available communication services. Storage would apply to traffic and location data, including subscriber and user data generated in the areas of traditional telephony (fixed network and mobile communication), and Internet (including e-mail, Voice over Internet, etc.). The Council-proposal does not apply to the content of information communicated.

Retention periods are supposed to be 12 months in principle, but derogations have been provided for minimum periods of 6 months and maximum periods up to 48 months (to be re-viewed every 5 years). The proposal does not provide rules for compensation of expenses incurred, though it does say that Member States **may** provide compensation.

With regard to internal market and competition considerations, the European Parliament as well as the European Commission have indicated significant doubts concerning the Council's choice of the legal basis ("third pillar"; Art. 31(1)c, 34(2)b TEU). The European Commission is currently working on a draft directive based on Art. 95 TEC. An agreement between the institutions on the legal basis has not been reached yet.

[1] Council Document 8958 / 2004: Draft framework decision on retention of data processed and stored in connection with the provisions of publicly available electronic communications services or data on public communication networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism; Council Document 8864/1/05: amended Council proposal (24 May 2005)

AV. DE CORTENBERGH 168
B-1000 BRUSSELS
VAT BE 863 418 279

TEL +32(0)2 237 65 11
FAX +32(0)2 231 14 45
E-MAIL: MAIN@UNICE.BE
WWW.UNICE.ORG

Regardless of the unresolved controversy over the correct legal basis, the following fundamental concerns have been at the centre of the discussion for years and were highlighted in the EPs first opinion[2] as well:

(1) Lack of a proper impact assessment that would justify additional storage requirements beyond legitimate business purposes in terms of all the costs and benefits. While law enforcement agencies cite instances where access to communications data has proved useful in criminal or terrorist investigations, they have still not satisfactorily shown that there is really the need for a blanket data retention regime as wide-ranging and un-differentiated as they have proposed.

(2) Significant costs are involved in the hardware and software modifications needed to generate the proposed data types and to store and process large volumes of data (costs depend on the respective retention period and - to a large extent - on the scope of data types).

(3) An impact will be felt on the data protection and privacy rights of European citizens; damage to end-user confidence and increased security risks are also involved in the storing of large volumes of data.

ISSUE

UNICE would like to emphasise that industry supports effective methods to combat organised crime and terrorism. "Security" serves the common good and is a definite plus for any business. UNICE has always supported the EU and national governments in the fight against terror[3]. But fighting crime generally is not, and should not be, an integral element of the development, management and investment of communications' businesses.

UNICE has serious doubts as to whether the introduction of a (EU) mandatory and blanket data retention regime is proportionate. With regard to the Lisbon process, UNICE would like to recall once again, that all European institutions have committed themselves to carry out a proper impact assessment (cost and benefit analysis) before proposing any new regulations. However, to our knowledge, an impact assessment has not been undertaken yet.

(1) LEAs have not been able so far to demonstrate the concrete need and benefit of data retention with regard to the broad range of data types (like unsuccessful calls, mobile location data during a call or the full range of internet data) on the one hand and retention periods longer than 6 months on the other hand.

Concerning the storage period, it can be safely assumed that data of 6 months basically meet law enforcement requirements. For instance, a survey of the German Association for Information Technology, Telecommunications and New

[2] http://www2.europarl.eu.int/oeil/file.jsp?id=5215602
[3] See UNICE General remarks on security, 1 December 2004

Media of December 2004 shows that law enforcement authorities hardly ask for data that is older than 3-6 months. Retention periods longer than 6 months are therefore hard to justify. Risk-based principles of better regulation would suggest that data regulatory burdens are only justifiable (and practicable) where there is a strong likelihood of a problem occurring – not in all instances where a problem **might** occur (as these could be infinite).

Even "the European Confederation of Police (EuroCOP) has dismissed the [Council] measures, claming it would take to long to search the records and noting that criminals could circumvent the use of phone cards and unregistered mobile phones". At present, UNICE has the impression that the European LEAs were not able (or asked) to present their common position. But this would be the first and decisive presupposition for a discussion that reflects the official demands of LEAs and not the abstract ideas of politicians.

(2) On the other hand, a blanket (EU) data regime will result in high cost burdens for industry. At present, companies generate, process and store data for billing, commercial and other legitimate purposes. Supplementary requirements (additional types of data; longer retention periods) would create extra costs that have to be covered. Costs are driven not primarily by the required storage capacities but mostly by the costs of adapting system technology for generating and storing the data, adapting the operational processes for safe archiving, and for handling and analysing enquiries from security authorities. At the Council meeting in June 2005, Finland's Minister of the Interior, Kari Rajamäki, announced, that the current proposal would amount for his country to a three-digit million figure.

As security is clearly a state responsibility - which has to be funded by the state – the Member States would have to bear the cost of data retention by compensating the ITC companies. Besides, LEAs seem to be swamped already today with the complexity and diversity of the ITC industry and communication processes. This often results in nonconforming requests and burdens for CSPs. The possibility of access requests for stored data by other Member States would intensify the complexity (language, contact persons etc.) and therefore involve very extensive and intensive training requirements.

(3) In weighing up whether cross-border combating of crime can and should actually be improved by legally stipulated data retention, the basic rights of EU citizens should be given sufficient consideration (right to informal self-determination and confidentiality of personal data; principle of data minimisation). Protected, confidential communication plays an important role in the use of innovative telecommunication services and for the further development of new media (internet, broadband, DSL, UMTS). The fear that one's own communications data is necessarily being recorded and analysed can inhibit the use and requests for information. This loss of consumer confidence holds the danger that the further development of the information society could be inhibited in the long term and thus the Lisbon Strategy could also be endangered. It would also not help law enforcement agencies get data that they might find useful.

Finally, UNICE cannot really agree with the assumption in the Council-document (8864/1/05 (COPEN 91)) that already "many Member States have passed legislation concerning a prior retention of data […]" and that "work is under way in other member States". The German ICT Industry has released an independent study. The findings showed that in the examined countries (France, Italy, the Netherlands, Austria, Sweden, Spain, UK and the US) data retention as requested in the initial Council document is hardly implemented in any country. There has been little if any systematic evaluation of the usefulness of legislation in relation to actual law enforcement needs and data requests. The US government even stated repeatedly that they do not use data retention in the US but give preference to a data "preservation" regime, which is also foreseen in the Cyber Crime Convention of the Council of Europe.[4]

Advocates of a European data retention regime often assume that industry would also benefit from harmonised requirements. However, mandatory data retention regimes do not exist in many European countries at present. European requirements would therefore largely result in new obligations. As a consequence, and with a view to proportionality, any "harmonised" data retention regime should be limited to minimum requirements and should be as specifically targeted as possible.

RECOMMENDATIONS

The European Union is confronted with a crisis and lack of trust because politicians are too often unable to explain the benefits of European activities. The concerns over data retention proposals also arise from this fact: a solid impact assessment is missing and neither the concerns of consumers nor those of industry seem to have been evaluated seriously.

⇒ **Impact Assessment:**
The EU institutions are obliged to carry out a proper impact assessment (cost and benefit analysis) in order to justify any concrete regulation. This is the only reliable and trustworthy way to evaluate the consequences of possible requirements for industry and consumers, and to analyse if and to what degree a (harmonised) European data regime helps to ensure effective police and judicial co-operation.

As EU institutions continue to discuss concrete proposals for a harmonised EU data regime, UNICE suggests the following specific guidelines:

⇒ **Agreement on the legal basis:**
Disputes about the legal basis will lead to legal uncertainty and have negative effects for industry since telecommunication operators and internet service providers may face a situation in which they would be obliged to implement a decision of the Council that may still be challenged by the EU-Commission and Parliament and therefore lead to "sunk investments" Thus, the EU institutions must find a solution to this question – also with regard to their credibility - before they go on with any further discussion.

[4] See for example the recent statement by Mark M. Richard , Counselor for Justice Affairs at the U.S. Mission to the EU, at a meeting of the EU's Article 29 Working party in Brussels on April 14, 2005

⇒ **Restriction of data types:**
Costs depend to a high degree on the specific data types at stake (the most critical being e.g. location data during a call, unsuccessful calls, range of internet data). With regard to proportionality, the data catalogue must be limited to a strict minimum.

⇒ **Limitation of retention period:**
Information available so far suggests that data older than 3-6 months is only infrequently requested by LEAs. Therefore, mandatory retention or reservation periods should be limited to 6 month as a maximum – not as a minimum.

⇒ **Cost compensation:**
As security is clearly a state responsibility - and state responsibilities have to be funded by the state – any EU requirements should oblige Member States to bear the cost of data retention or preservation by compensating ITC companies. Compensation should cover (1) incremental infrastructure costs and annual operational expenses.

Non-standardised or insufficient systems of compensation will lead to distortions in competition, in the long-term endanger the feasibility of competitive structures and thus prevent the evolution of a uniform European internal market. Therefore, European legislation also has to provide harmonised cost re-imbursement regimes.

The comparability of cost surveys will very much depend on standardised, well structured questionnaires based on concrete data types and scenarios keeping in mind that the processes and network structures may vary considerably between companies. UNICE welcomes all initiatives to conduct business impact assessments to assess the expected costs of data requirements.

⇒ **Scope of application:**
The scope of application must strictly be limited (to severe crimes). Otherwise, numerous requests by LEAs (for any kind of offence) will lead to additional operational costs for industry. Proportionality with regard to privacy and data protection rights will also be observed by this limitation.

UNICE looks forward to pursuing the debate on this issue with the interested parties.
These comments are preliminary and might be supplemented as the debate develops.

* * *